

CERTIFICATE OF AVAILABILITY OF A CERTIFIED PATENT DOCUMENT IN A DIGITAL LIBRARY

The International Bureau certifies that a copy of the patent application indicated below has been available to the WIPO Digital Access Service since the date of availability indicated, and that the patent application has been available to the indicated Office(s) as of the date specified following the relevant Office code:

Document details: Country/Office: EP

Filing date: 18 Oct 2019 (18.10.2019)

Application number: 19306357

Date of availability of document: 15 Jan 2020 (15.01.2020)

The following Offices can retrieve this document by using the access code:

AR, AU, BR, CA, CL, CN, DK, EA, EE, EP, ES, FI, GB, GE, IB, IL, IN,
JP, KR, MA, NL, NO, NZ, SE, US

Date of issue of this certificate: 30 Sep 2020 (30.09.2020)

Bescheinigung

Die angehefteten
Unterlagen stimmen mit der
als ursprünglich eingereicht
geltenden Fassung der auf
dem nächsten Blatt
bezeichneten europäischen
Patentanmeldung überein.

Certificate

The attached documents are
exact copies of the text in
which the European patent
application described on the
following page is deemed to
have been filed.

Attestation

Les documents joints à la
présente attestation sont
conformes au texte,
considéré comme
initialement déposé, de la
demande de brevet
européen qui est spécifiée à
la page suivante.

Patentanmeldung Nr.

Patent application No.

Demande de brevet n°

19306357.5 / EP19306357

The organisation code and number of your priority application, to be used for filing abroad under the Paris Convention, is EP19306357.

Der Präsident des Europäischen Patentamts,
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.



V. Joseph

Anmeldung Nr.: 19306357.5
Application no.:
Demande no.:

Anmeldetag: 18.10.19
Date of filing:
Date de dépôt:

Anmelder / Applicant(s) / Demandeur(s):

THALES DIS FRANCE SA
6, Rue de la Verrerie
92190 Meudon/FR

Bezeichnung der Erfindung / Title of the invention / Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, oder falls die Anmeldung in einer Nicht-Amtssprache des EPA eingereicht wurde, siehe Beschreibung bezüglich ursprünglicher Bezeichnung.
If no title is shown, or if the application has been filed in a non-EPO language, please refer to the description for the original title.
Si aucun titre n'est indiqué, ou si la demande a été déposée dans une langue autre qu'une langue officielle de l'OEB, se référer à la description pour le titre original.)

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

In Anspruch genommene Priorität(en) / Priority(Priorities) claimed / Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen / State/Date/File no. / Pays/Date/Numéro de dépôt:

Am Anmeldetag benannte Vertragsstaaten / Contracting States designated at date of filing / Etats contractants désignés lors du dépôt:

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL
PT RO RS SE SI SK SM TR

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

BACKGROUND OF THE INVENTION

[0001] The present invention relates, generally, mobile devices operating electronic identification (eID) wallet applications, and, more particularly, to security mechanisms for namespaces used to access data in eID wallet applications.

[0002] Mobile devices such as telephones and tablets provide users with many benefits that have allowed them to eliminate other devices and cards. For example, electronic wallets have allowed users to dispense with carrying many credit cards and enable users to load travel boarding passes and other tickets onto their mobile phones. Another emerging technology, known as electronic identification (eID), provides the ability to use mobile devices to store identification documents such as driver licenses, passports, national ID cards, university ID cards, and club membership cards.

[0003] At least one standard proposal for eID specifies the use of *namespaces* for accessing data stored in mobile Driving License application. ISO/IEC CD2 18013-5:2019, *Personal Identification — ISO-Compliant Driving Licence — Part 5: Mobile Driving Licence (mDL) application*. A namespace is a symbolic mechanism for organizing and identifying pieces of data. To access a piece of data a requestor specifies namespace identifier and a local name (unique within the namespace but not necessarily unique with respect to other namespaces).

[0004] Thus, using namespaces, within an eID wallet one or more eID applications may each have its own namespace that specifies the names of data managed by the eID application.

[0005] While multiple eID applications and associated namespaces managed by a mobile device can satisfy the same identification task, e.g., providing the age of a user, the level of confidence that a verifier associates with these multiple applications and namespaces may not be the same. For example, a government issued eID would typically provide a higher level of confidence than a club associated with a leisure activity.

[0006] Furthermore, eID applications may have security policy requirements before the eWallet allows access to the particular eID application and the information that it manages. Some such security policy requirements, e.g.,

cryptographic signatures of access requests, may be deemed overly cumbersome by certain attribute verifiers or a verifier may not be able to satisfy the requirements.

[0007] To allow a verifier to determine which namespace from which to request access, it is desirable to have a technology which allows uniform communication of namespaces available from a mobile device and namespace security policy access rules associated with such namespaces.

SUMMARY

[0008] A technology for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device provides for associating security policies with each of a plurality of supported namespaces on a mobile device and operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device. In an aspect, technology for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device includes transmitting a list of supported namespaces to the verifier module executing on the verifier and selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.

[0009] In a further aspect, a list of supported namespaces is transmitted to the verifier module and the verifier module selects at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace. In an aspect, prior to transmitting a list of supported namespaces to a verifier terminal via the reader, the mobile device filters out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

[0010] The security policy of each of the plurality of supported namespaces maybe transmitted from the mobile device to the reader, for examples, as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options. The required authentication may be selected from one or more of digital signature, reader

authentication, certificate verification, secure messaging, role authentication, and user consent.

[0011] In an aspect, the reader operates to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier associates with each namespace in the plurality of supported namespaces, for example, by selecting a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

[0012] In an aspect, the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory, the technology further including operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.

To achieve those and other advantages, and in accordance with the purpose of the invention as embodied and broadly described, the invention proposes a method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device, comprises the following steps:

- associating security policies with each of a plurality of supported namespaces on a mobile device; and

- operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device comprises the following steps:

- transmitting a list of supported namespaces to the verifier module executing on the verifier; and

- selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device, comprising the following steps:

transmitting a list of supported namespaces to the verifier module; and
selecting, by the verifier module, at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprising the following steps:

prior to transmitting a list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprising the following step of transmitting the security policy of each of the plurality of supported namespaces from the mobile device to the reader.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device wherein the required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprises operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier associates with each namespace in the plurality of supported namespaces.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprises

operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device wherein the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory, the method further comprising operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.

Another aspect of the invention is a mobile device comprising:

a processor; and

a memory for storing instructions executable by the processor and for storing electronic identity eID data, the memory including an eID wallet application having instructions to cause the processor to:

receive a list of selected namespaces from a reader;

in response to receiving the list of selected namespaces from the reader, transmitting security rules associated with each selected namespace according to a defined bytestring template.

In an aspect, the eID wallet application further comprises instruction to cause the processor to:

receive a request for supported namespaces from a reader;

transmit a list of supported name spaces to the reader.

In an aspect, the eID wallet application further comprises instruction to cause the processor to:

prior transmitting a list of supported namespaces to a reader, filter out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the reader.

In an aspect, the eID wallet application further comprises instruction to cause the processor to:

transmit the security policy of each of the plurality of supported namespaces to a reader connected to a verifier.

In an aspect, the eID wallet application wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

In an aspect, the present relates to a method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

- associating a security policy with each of a plurality of supported namespaces on a mobile device;

- transmitting the security policy of each of the plurality of supported namespaces to a reader connected to a verifier;

- selecting, by the reader, at least one of the namespaces as candidate namespaces, and transmitting from the reader to the mobile device, a list containing the candidate namespaces;

- transmitting to the reader by the mobile device, the security policy associated with each of the selected candidate namespaces;

- operating the reader to:

- determine for which of the candidate namespaces the reader can satisfy the security policy of the namespace, and

- if the verifier can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the verifier terminal can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the mobile device;

- if the verifier cannot satisfy the security policy of any of the candidate namespaces, rejecting access to the data item; and

- upon successful demonstration by the reader to the mobile device of satisfaction of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1 is a schematic illustrating an exemplary use case scenario.

[0014] FIG. 2 is an external representation of a mobile device.

[0015] FIG. 3 is a block diagram illustrating major components of a hardware and software architecture for a mobile device.

[0016] FIG. 4 is a block diagram illustrating one embodiment organization for a reader.

[0017] FIG. 5 is a block diagram illustrating one embodiment organization for a verifier that contains a reader of FIG. 4.

[0018] FIG. 6 (which is partitioned onto FIGs. 6a and 6b) is a timing sequence diagram illustrating a process for communicating namespaces available on a mobile device to a reader.

[0019] FIG. 7 is a table illustrating an example protocol for namespace-security-policy messages.

[0020] FIG. 8 is a block diagram of a namespace security representation containing a template and additional information byte sequences.

[0021] FIG. 9 is a diagram showing a dialog box displayed on a mobile device to obtain user acquiescence for use of a namespace.

DETAILED DESCRIPTION OF THE INVENTION

[0022] In the following detailed description, reference is made to the accompanying drawings that show, by way of illustration, specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. It is to be understood that the various embodiments of the invention, although different, are not necessarily mutually exclusive. For example, a particular feature, structure, or characteristic described herein in connection with one embodiment may be implemented within other embodiments without departing from the spirit and scope of the invention. In addition, it is to be understood that the location or arrangement of individual elements within each disclosed embodiment may be modified without departing from the spirit and scope of the invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims, appropriately interpreted, along with the full range of equivalents to which the claims are entitled. In the drawings, like numerals refer to the same or similar functionality throughout the several views.

[0023] The following description includes references to various methods executed by a processor of mobile device or a terminal, known herein as the reader or the verifier. As is common in the field, there may be phrases herein that indicate these methods or method steps are performed by software instructions or software modules. As a person skilled in the art knows, such

descriptions should be taken to mean that a processor, in fact, executes the methods, software instructions, and software modules.

[0024] The herein described technology provides mechanisms to provide discoverability of security policies for electronic identification data organized in namespaces on mobile devices with total abstraction of the data structures used on the mobile devices. As such the technology provides an improvement to mobile devices used for electronic identification purposes and the overall system of electronic identification by providing technology by which security access rules may be assigned to namespaces that are used to address electronic identification data stored on mobile devices when mobile devices are used to make identity-based identification or attribute assertions whereby electronic identification readers and verifiers may select appropriate namespaces hosted by electronic devices for verifying electronic identification-based attribute assertions. The technology improves a mobile device by providing such devices the ability to offer more flexibility in assignment of security policies and communication of such security policies to readers and verifiers of electronic identification data.

[0025] First a use case. There are many instances in which an individual seeks to establish an attribute that will allow that individual a certain privilege. That may be an access to a restricted physical space, the right to participate in a program, access to a private or age-restricted material, or access to an attribute-restricted benefit. A reduced fare only available to students and senior citizens is an example of an attribute-restricted benefit.

[0026] Suppose, a person wishing to travel on a metro system is entitled to a 50% discount if the person is either a student or a senior citizen. A person may have on her mobile device several eID applications that may be useful to demonstrate satisfaction of one or both of the requirements for reduced fare, e.g.,

- a government issued identity card, for example, from AGENCE NATIONALE DES TITRES SÉCURISÉS (ants.gouv.fr; French National Agency for Secure Documents) or TEXAS DEPARTMENT OF PUBLIC SAFETY (dps.texas.gov)
- a university departmental ID, for example, University of Pau (univ-pau.fr) or University of Texas (utexas.edu)
- a club for a leisure activity, for example, a stamp collection club (pau-philatelie.asso.org) or a garden club (merryweeders.org)

[0027] Each of the eID applications may store information that can be used to prove that a person is a student or of a certain age; e.g., the government ID typically store birthdates and may have a professional status (e.g., retired or student), the university ID would certainly indicate if a person is a student, faculty or alumnus, and even the stamp club may charge a different membership fee for students and therefore have a flag set for a member being a student, and the garden club may store birthdates so that they can celebrate members on their respective birthdays.

[0028] When the prospective passenger wishes to purchase a monthly pass for the metro, they presents their mobile device to a ticket vendor, which may either be an automatic ticket self-use vending terminal or an individual employee of the metro authority, who would operate a verification terminal. If the passenger is a student or senior, the passenger offers his or her eID wallet to prove that fact. The passenger or the metro official places the mobile device on a terminal.

[0029] The eID wallet communicates the desired attribute to the terminal and the terminal decides whether to grant the discount or not.

[0030] FIG. 1 is a schematic illustrating the above-described use-case example scenario and alternatives. A user 101 operates a mobile device 103, e.g., a mobile telephone. The mobile device 103 contains an eID wallet with one or more eID applications (see FIG. 2). The eID functionality of the mobile device 103 may be used by the user 101 to prove identity or an identity-related attribute to a verifier. The verifier may be a human verifier 115 interacting with reader 109 and a verifier computer 105 via a user interface 117 connected to a reader 109. For example, if the user 101 seeks to obtain access to a facility based on a membership status, the user 101 may present the mobile device 103 to a security guard (human verifier) 115. A verifier module 111", executable by the reader 109 or the verifier 105, provides the dialog user interface 117 to the human verifier 115 to verify proffered identification from the user 101.

[0031] Alternatively, the verifier may be performed automatically when the user 101 places the mobile device 103 on the reader 109, for example, if the reader 109 is connected to an automated verifier 105', executing a software verifier module 111', in communication with a reader 109'. While depicted here as separate units, the reader 109' and the verifier 105' may be one machine. An example may be a ticket vending machine in which a traveler has to demonstrate being a member of a particular age group.

[0032] In an alternative use case, the mobile device 103 is used to provide identity functionality over the internet 113 to a remote server 115 on which a verifier module 111 is executing.

[0033] FIG. 2 is an external representation of a mobile device 103 and FIG. 3 is a block diagram illustrating major components of a hardware and software architecture for a mobile device 103. The mobile device 103 contains a touch screen user interface 201 for receiving input from the user 101 and for providing output to the user 101 as well as a camera 203 by which the mobile device may receive input from a reader 109, e.g., by scanning QR codes or bar codes displayed on the reader 109.

[0034] As illustrated in FIG. 3, the mobile device 103 contains a processor 301, a communications interface 303, and a non-volatile memory (NVM) 305. The NVM 305 contains programs including an operating system 307 and application programs, referred to as “apps”, which includes an eIDWallet app 309.

[0035] The communications interface 303, which may be used for mobile telephony, NFC, Bluetooth, WiFi, etc., allows the mobile device 103 to communicate with the reader 109 or the remote server 115. Alternatively, the mobile device 103 may communicate to the reader 109 via the screen 201 and camera 203 the reader 109 maybe an optical device that reads information transmitted via the screen 201 of the mobile device 103 and outputs information that the mobile device 103 may input via the camera 203.

[0036] The eIDWallet app 309 manages eIDWallet information, e.g., in an eIDWalletDB 311 organized around a number of namespaces 313a-n.

[0037] The architecture of FIG. 3 is merely one example. For example, in an alternative embodiment, there may be multiple eIDWallet apps each with its own namespace.

[0038] Each namespace provides access to a number of data elements and defines its own names for those data elements. An example namespace may be found in

ISO/IEC CD2 18013-5:2019, *Personal Identification — ISO-Compliant Driving Licence — Part 5: Mobile Driving Licence (mDL) application*, section 7 “Data Model”, incorporated herein by reference.

[0039] However, while two namespaces may contain the same data elements, these data elements may not have the same name in the two namespaces. For example, *Date of birth* (from the sample namespace in Appendix I) may be named *BirthDate* in another namespace. Similarly, two different data

elements may provide an equivalent piece of information, e.g., *Date of birth* may be used to derive *age*.

[0040] Namespaces may be addressed in different ways, for example, URI, URL, URN, OID, UUID, or reverse domain namespace representation. In reverse domain representation, the namespace may be defined as *reverseDomain.domainSpecificExtension*. For example, for the French National Agency for Secure Documents, the reverse domain namespace identifier may be *fr.gouv.ants.id*, and for a stamp club, *org.asso.philatelie.role*.

[0041] FIG. 4 is a block diagram illustrating one embodiment organization for a reader 109. The reader 109 includes a processor 401, a storage unit 403, an interface unit 405, for example, for interfacing with the processor of the verifier 105, and a communications module 407, for example, for NFC, WiFi, Bluetooth communication with the mobile device 103.

[0042] The storage unit 403 contains software modules including an operating system (OS) 409 and a reader module 411, which contains instructions to the processor 401 to carry out reader-side namespace selection as illustrated and described hereinbelow.

[0043] FIG. 5 is a block diagram illustrating one embodiment organization for a verifier 105. The verifier includes a processor 451, a storage unit 453, an input/output interface unit 405, for example, for interfacing with a user interface device for communicating with a human operator 115 or the user 101, and a communications module 457, for example, for NFC, WiFi, or Bluetooth communication with the mobile device 103. The storage unit 403 contains software modules including an operating system (OS) 459 and a verifier module 111 for carrying out tasks related to verifying an eID attribute assertion, for example, one related to verifying eligibility based on an attribute or identity.

[0044] Note, there are tasks of the reader module 411 as well as the verifier module 111 that may be carried out by a human operator. For example, as discussed in conjunction with the timing sequence diagram of FIG. 6 that follows hereinbelow, selection of a namespace based on level of security may be performed using a dialog with a human identity-based-assertion verifier (see, FIG. 1, 115). Accordingly, the verifier 105 may include an I/O interface 455 for connecting to user interface devices, such as a terminal for displaying graphic user interface elements 117.

[0045] FIG. 6 (which is partitioned onto FIGs. 6a and 6b) is a timing sequence diagram illustrating a process for communicating namespaces available

on a mobile device 103 to a verifier 105 including a reader 109. The process executed by the reader 109 may be under control of a software module referred to herein as the reader module 411. It should be noted that there is no strict demarcation between the reader 109 and verifier 105. Tasks described herein as performed by one may be performed by the other. Furthermore, the reader 109 and verifier 105 may be either completely separated or merged into one unit or any arrangement between those two extremes.

[0046] As a preliminary step a user 101 operating the mobile device 103 seeks to make an identity-based assertion, step 501. The identity-based assertion may be a request to access a service based on a certified attestation of an identity attribute, e.g., age, or to demonstrate that the user 101 is a particular person. The user 101 presents the mobile device 103, which contains and executes an eIDWallet app 309, to the reader 109 and a communications session, e.g., NFC, Bluetooth, WiFi, or optical transmission, is established between the mobile device 103 and the reader 109.

[0047] In response to the establishment of an eID communications session, the reader 109 responds by requesting from the mobile device 103 a listing of eID namespaces supported by the mobile device 103, step 503.

[0048] The mobile device 103 responds with a list of supported eID namespaces, step 505. The list may be a concatenation or structured set of namespace identifiers, for example, in the form of URI, URL, URN, OID, UUID, or reverse domain name representation. In an embodiment, the mobile device 103 requests confirmation by the user 101 that the user acquiesces to releasing particular namespaces to the reader 109 and verifier 105. For example, if one namespace that contains a birthdate is associated with a political organization, the user may prefer to not reveal membership in that organization to the reader 109 and verifier 105.

[0049] Using, for example, reverse domain name representation, for a French-citizen student at the University of Pau, France, who is a stamp collector, the mobile device 103 may return:

National identification: *fr.gouv.ants.id* (the French National Agency for Secure Documents)

Student identification: *fr.edu.univ-pau.labo.profile* (University of Pau)

Membership card in stamp club: *org.asso.philatelie.role* (Stamp collectors club)

[0050] Depending on the request for which the identity assertion (step 501) is made, the verifier 105 determines the level of security (LOS) that should be associated with the request, step 507. For example, a bank cashing a check may require an identity assertion associated with a national ID whereas for proving entitlement to a student fare, a university ID may be sufficient.

[0051] Based on the required LOS, the verifier 105 selects one or more namespaces that satisfy the required LOS, step 509, and sends a request for access to these namespaces to the mobile device 103, step 511. The verifier 105 may have a whitelist of namespaces that may be used to satisfy LOS for an identity-based assertion. For example, a metropolitan transit authority may accept national IDs as well as student IDs from local universities. Conversely, the verifier 105 may have a blacklist of namespaces that are not allowed to be used for an identity-based assertion; i.e., that are deemed to not meet the LOS required.

[0052] The mobile device 103 responds with the security policy access rules associated with each of the requested namespaces, step 513.

[0053] In a preferred embodiment, the security policies of namespaces are communicated according to a standard protocol or an interoperability template. The namespace-security-policy protocol may consist of a sequence of bytes in which each bit signifies a particular security policy attribute.

[0054] FIG. 7 is a table illustrating an example 601 protocol for namespace-security-policy messages.

[0055] In the example 601, the first byte is used to communicate a version number of the template used for communicating namespace security policy.

[0056] The second byte of the example template 601 contains a value for denoting the required authentication protocol. The first bit (b1) indicates whether digital signature is required or not. The second bit (b2) indicates whether reader authentication is required. The third bit (b3) is used to indicate whether certificate verification is required. The fourth bit (b4) is used to indicate whether secure messaging is required. The fifth bit (b5) is used to indicate whether role authentication is required. The sixth bit (b6) indicates whether user consent is required.

[0057] The third byte indicates the HASH type to be used. For example, first through third bit indicate to use SHA-256, SHA-384, and SHA-512, respectively. Other bits could be used to indicate alternative hashing schemes. No bit set indicates that hashing is not to be used.

[0058] The fourth byte indicates the scheme for digital signatures to be used. For example, the first and second bits indicate RSA and ECDSA, respectively. Other bits may indicate to use other digital signature schemes. No bit set indicates that digital signature is not required.

[0059] The fifth byte denotes which secure messaging option to use. The first through third bit indicate AES 128 bit-CMAC, AES 128 bit-EMAC, and AES-GCM, respectively. Other bits may indicate to use other secure messaging options. No bit set indicates that secure messaging is not required.

[0060] It should be noted that the template illustrated in FIG. 7 and described above is merely an example. Other arrangements are possible. For example, several of the bytes that only use a few bits to convey information can be combined.

[0061] Returning to FIG. 6, having received the security policy access rules (step 513), the reader 109 determines if there is at least one namespace with acceptable access rules, step 515. For example, if the mobile device 103 demands verification of a digital signature to access a namespace for verification of age to access a website, that may be considered too onerous by the verifier 105. Furthermore, if the verifier 105 may not have the capability to satisfy a demanding access rule and therefore be forced into requesting access to a namespace with a less demanding access rule. Accordingly, the verifier 105 may have, for example, selection rules such as to not select namespaces that require certificate verification or more than 128-bit encryption.

[0062] If there is no namespace provided by the mobile device 103 with acceptable level of confidence and acceptable access rules, the reader 109 may decline access to the service or benefit requested by the mobile device 103, step 515, and a message declining access to the requested service is transmitted to the mobile device 103, step 515.

[0063] Otherwise, the reader 109 selects a namespace with an acceptable security policy, step 519.

[0064] With the selected namespace, the reader satisfies the access rules required by the mobile device and sends an access request message with the namespace identifier, data element name (used by the namespace to address the required data element), required information or format according to the access rule for the namespace, e.g., certificate, hashed message, step 521.

[0065] In an embodiment, the namespace security policy representation 601 further contains additional information, e.g., a certificate route

or digital information necessary to resolve certain cryptographic references. For example, the security policy access rules can be satisfied by the verifier 105 or reader 109 if the verifier/reader has references to, e.g., the cryptographic keys to use, a route to a Certificate Authority root public key (for certificate verification), or an object identifier (OID) denoting a crypto-suite to be performed by the verifier/reader. To provide this additional information, the namespace security policy template 601 transmitted in step 513 may be appended with a byte sequence providing the required data for the defined security mechanisms to allow access to eID data from the mobile device 103 corresponding to each of the bytes in the template.

[0066] FIG. 8 is a block diagram of namespace security representation 701 containing a template 601' and additional information byte sequences 705a-e.

[0067] The example namespace security representation 701 contains the five bytes 703a-e corresponding to the five-byte template 601'. Each of these has a corresponding additional-information byte sequence 705a-e. Each of these additional byte sequences 705a-e are in length-value format, i.e., the first field 707a-e indicating the number of bytes of the value field 709a-e; a 0 value in the length field 707a-e indicates that there is no additional information sequence corresponding to a particular byte in the template and thus, the value field 709a-e would be an empty sequence.

[0068] There are many different possible syntaxes for the length fields. In a simple case, the length field is simply a fixed number of bytes, e.g., one or two bytes.

[0069] Thus, the security policy access rule communication may be:
 1st byte||2nd byte||3rd byte||4th byte||5th byte||0x00||0x0C||<12 byte
 OID>>||0x00||0x08||<eight byte key>>||0x00

where

- the first five bytes correspond to the security policy access rules as described in conjunction with FIG. 7
- 0x00 indicates a zero-length value field, i.e., no value, corresponding to the first byte 703a
- 0x0C is the length field with the hexadecimal value indicating that 12 bytes is to follow for additional information corresponding to the second byte 703b; in the example, the following 12 bytes is a representation of the OID denoting the

crypto-suite applying the authentication protocol defined in the 2nd byte of the security policy access rules

- The second 0x00 indicates that there is no additional information corresponding to the third byte 703c
- 0x08 indicates that the following value field, corresponding to the fourth byte 703d, is eight bytes long and the following eight bytes, in this example, is an eight-byte cryptographic key
- the third 0x00 indicates that for the fifth byte 703e there is no additional information byte sequence

[0070] Other mechanisms for indicating the length of the additional value field include using an escape sequence, e.g., 0xFF, to indicate that the following byte contains the length of the length field. For example, 0xFF020216 would indicate that the length field (0x02) is two bytes long and those two bytes indicate that the following byte sequence is 0x0216 (534) bytes long. Yet another mechanism is to have the first byte of each additional information sequence 705 indicate the length of the length field.

[0071] As noted above, user consent may be one possible access rule. Thus, if user consent is required, the mobile device 103 may display on the user interface 201 a message to the user indicating the access request, for example, as indicated in FIG. 9, which is a diagram showing a dialog box displayed on a mobile device 103. If the user cancels, the access is denied. Conversely, the access to the requested service also not granted. However, in a follow-up dialog, the user 101 may be provided the opportunity to select another eID namespace for the identity-based assertion required by the reader 109.

[0072] Returning again to FIG. 6, if the reader 109 has satisfied the requirements of the access rules for the requested namespace, the eWallet app 309 of the mobile device 103 retrieves the required data using the namespace data element name provided, step 523, and provides identity-based assertion to the reader 109, step 525.

[0073] The reader 109 or verifier 105 then determines whether the identity-based assertion has been proved by the eID namespace, step 527. If the assertion has not been proved, access is denied, step 517. Otherwise, access to the requested service based on the identity-assertion made using the requested eID data element addressed using the selected namespace and data-element name (step 521), the access to the requested service or benefit is provided, step 529.

[0074] From the foregoing it will be apparent that an efficient and secure mechanism for associating security policy access rules with namespaces used in eID wallets is provided.

[0075] Although specific embodiments of the invention have been described and illustrated, the invention is not to be limited to the specific forms or arrangements of parts so described and illustrated. The invention is limited only by the claims.

[0076] We Claim:

CLAIMS

1. A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

associating security policies with each of a plurality of supported namespaces on a mobile device; and

operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.

2. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device of Claim 1, comprising:

transmitting a list of supported namespaces to the verifier module executing on the verifier; and

selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.

3. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims, comprising:

transmitting a list of supported namespaces to the verifier module; and

selecting, by the verifier module, at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

4. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims further comprising:

prior to transmitting a list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

5. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims, comprising:

transmitting the security policy of each of the plurality of supported namespaces from the mobile device to the reader.

6. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

7. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims wherein the required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

8. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims further comprises operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier associates with each namespace in the plurality of supported namespaces.

9. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims further comprises operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

10. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims wherein the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory, the method further comprising operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.

11. A mobile device comprising:
 a processor; and
 a memory for storing instructions executable by the processor and for storing electronic identity (eID) data, the memory including an eID wallet application having instructions to cause the processor to:
 receive a list of selected namespaces from a reader;
 in response to receiving the list of selected namespaces from the reader, transmitting security rules associated with each selected namespace according to a defined bytestring template.

12. The mobile device of claim 10, wherein the eID wallet application further comprises instruction to cause the processor to:
 receive a request for supported namespaces from a reader;
 transmit a list of supported name spaces to the reader.

13. The mobile device according to claims 11 to 12, wherein the eID wallet application further comprises instruction to cause the processor to:
 prior transmitting a list of supported namespaces to a reader, filter out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the reader.

14. The mobile device according to claims 11 to 13, wherein the eID wallet application further comprises instruction to cause the processor to:
 transmit the security policy of each of the plurality of supported namespaces to a reader connected to a verifier.

15. The mobile device according to claims 11 to 12, wherein the eID wallet application wherein the security policy is transmitted as a sequence of bytes

having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

16. A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

- associating a security policy with each of a plurality of supported namespaces on a mobile device;

- transmitting the security policy of each of the plurality of supported namespaces to a reader connected to a verifier;

- selecting, by the reader, at least one of the namespaces as candidate namespaces, and transmitting from the reader to the mobile device, a list containing the candidate namespaces;

- transmitting to the reader by the mobile device, the security policy associated with each of the selected candidate namespaces;

- operating the reader to:

- determine for which of the candidate namespaces the reader can satisfy the security policy of the namespace; and

- if the verifier can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the verifier terminal can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the mobile device;

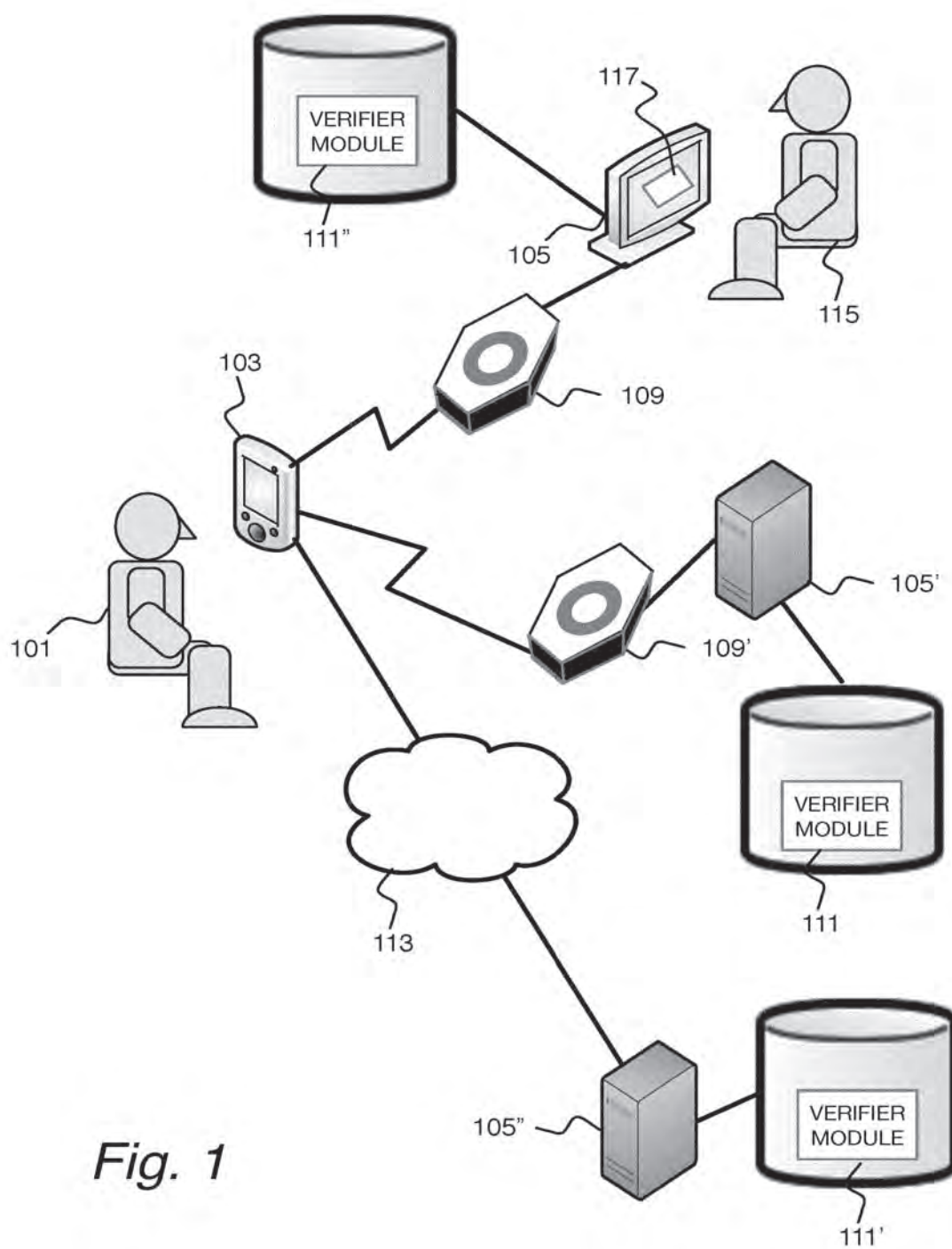
- if the verifier cannot satisfy the security policy of any of the candidate namespaces, rejecting access to the data item; and

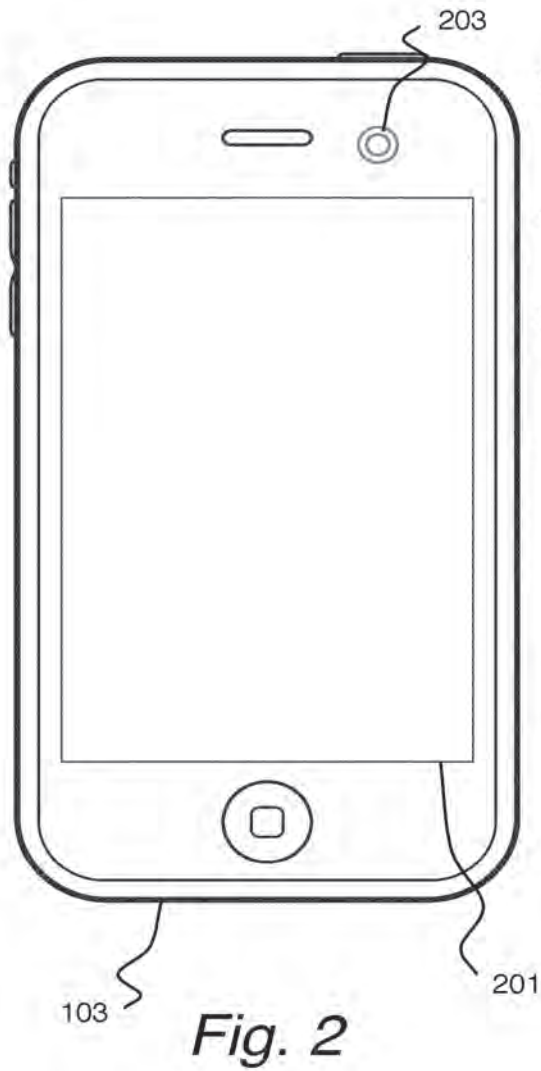
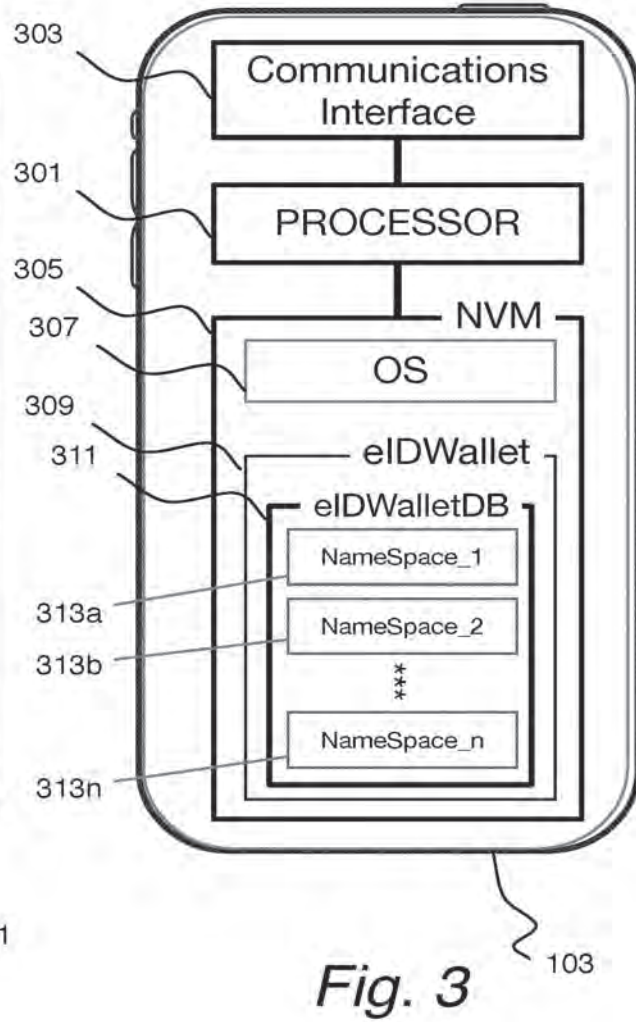
- upon successful demonstration by the reader to the mobile device of satisfaction of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

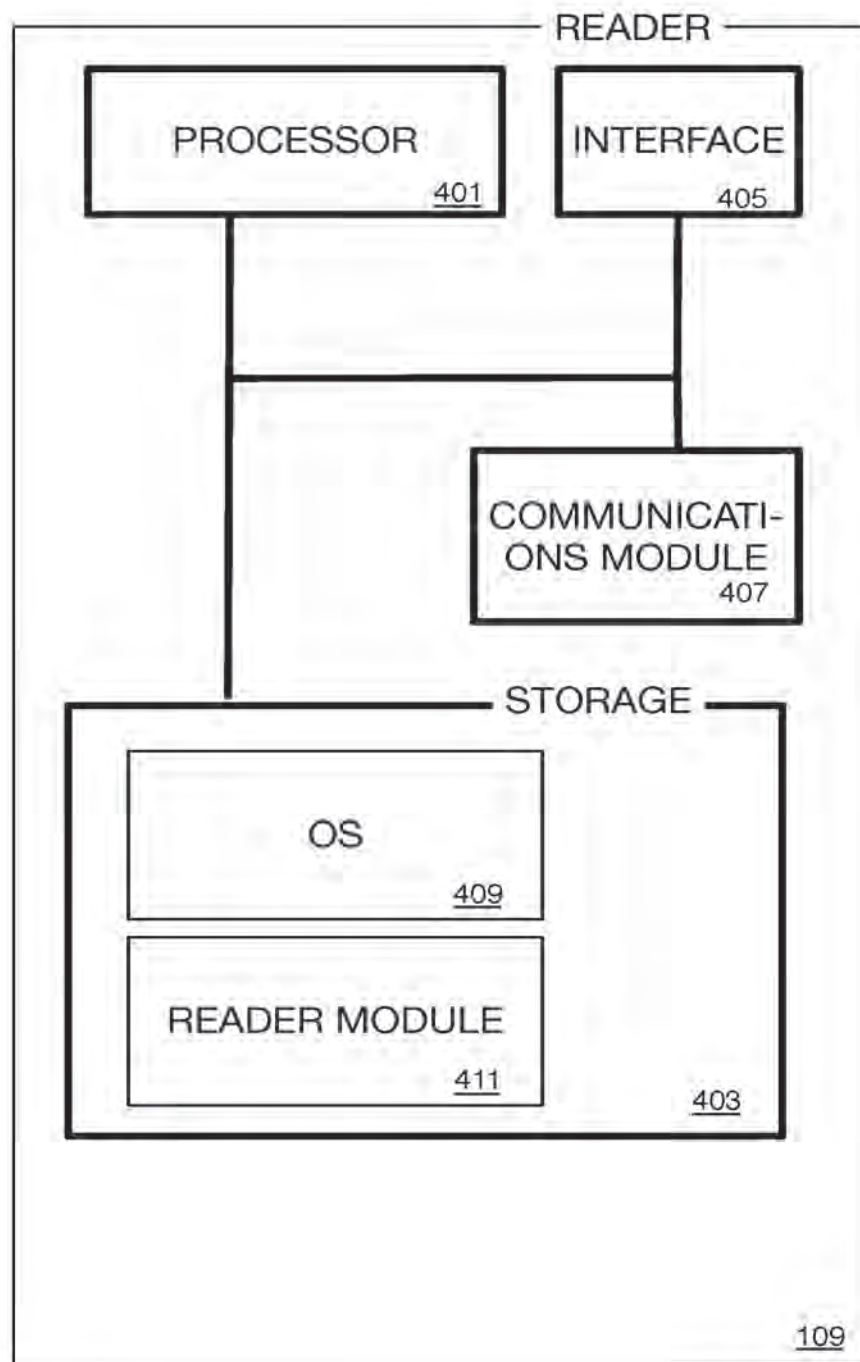
ABSTRACT**SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC
IDENTIFICATION ON MOBILE DEVICES**

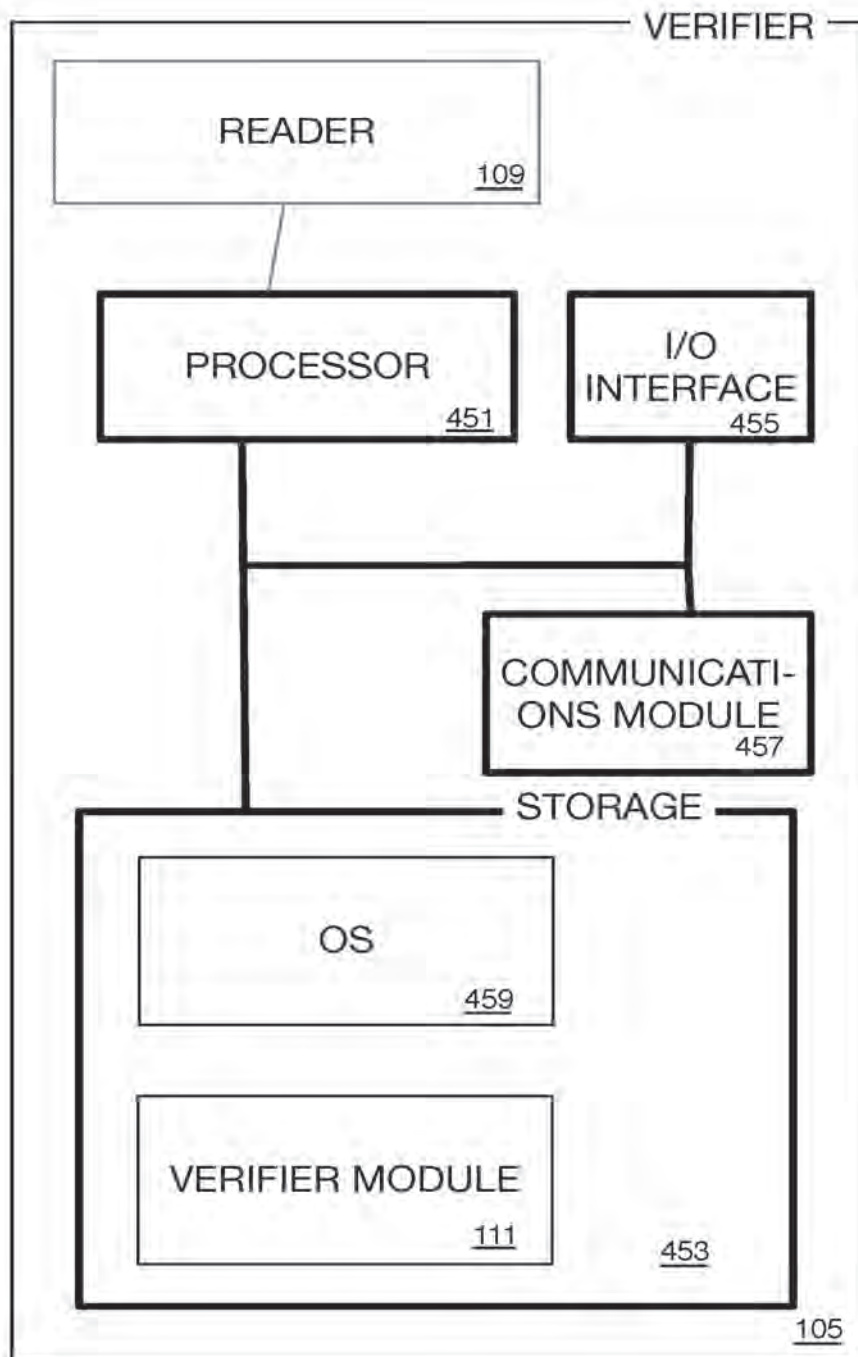
A system, mobile device, and method for managing security policies for data items stored in an electronic identification (eID) wallet on the mobile device. Security policies are associated with each of a plurality of supported namespaces on a mobile device and a verifier terminal operates to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.

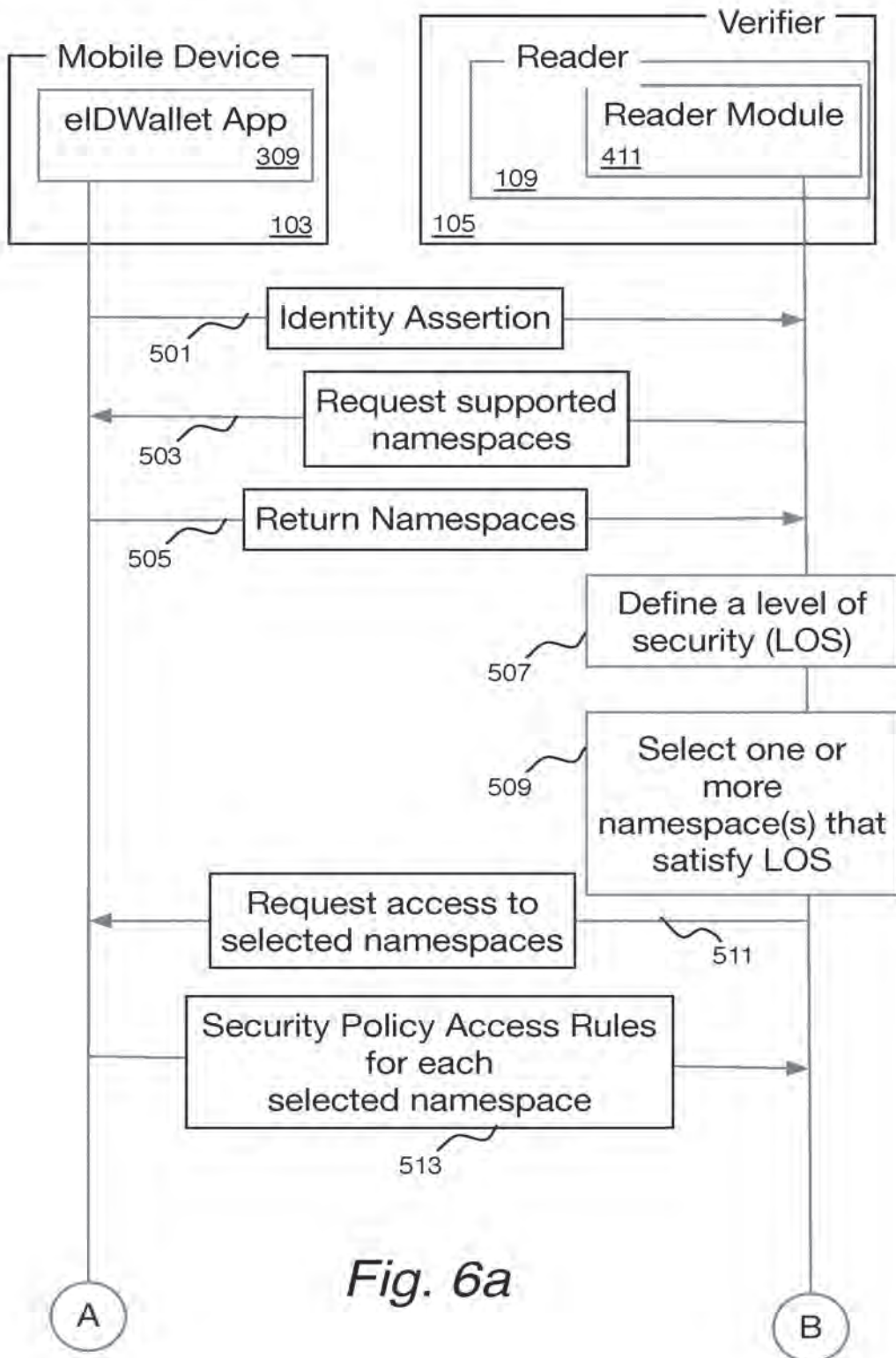
Figure 6a

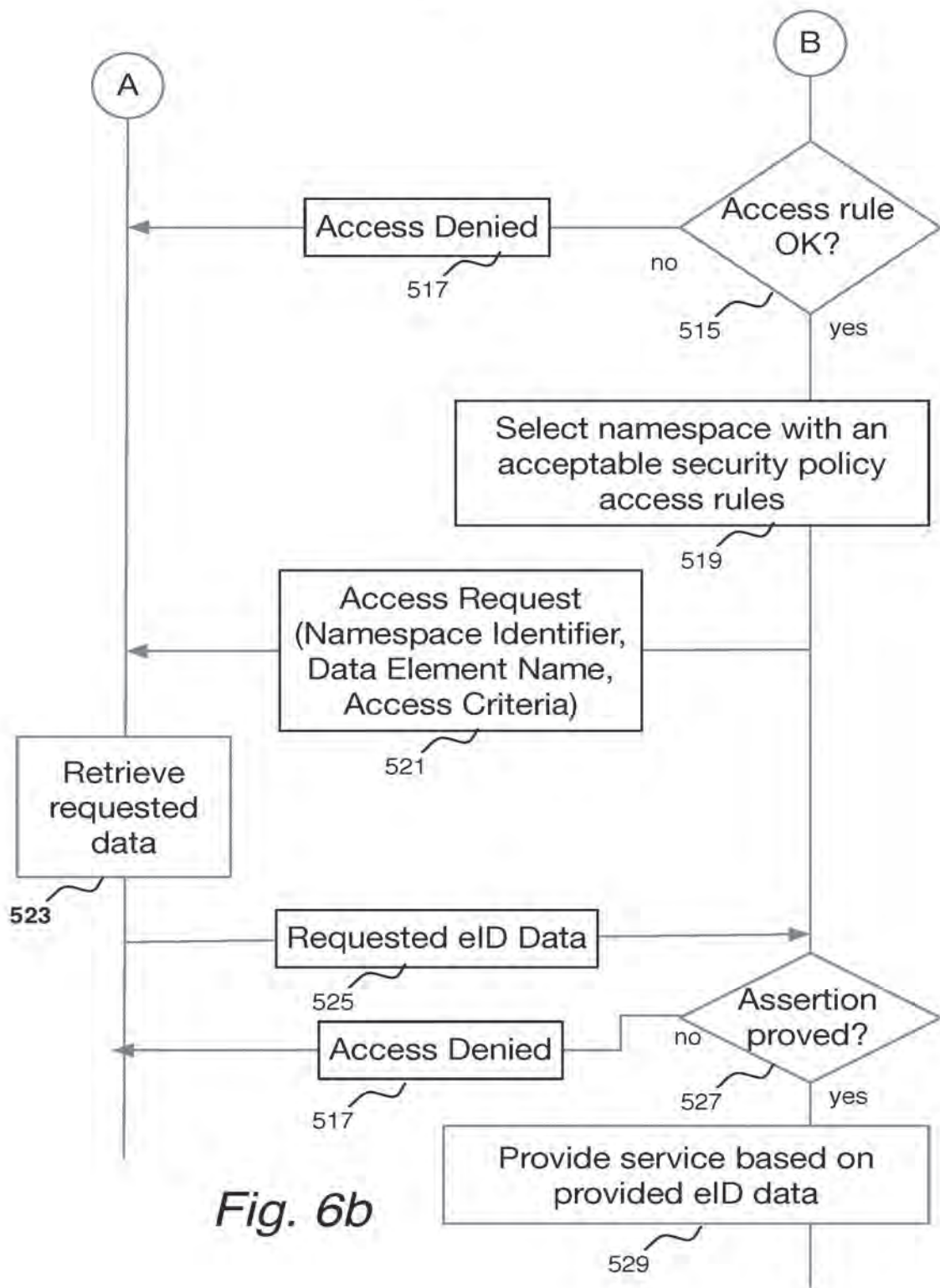
*Fig. 1*



*Fig. 4*

*Fig. 5*

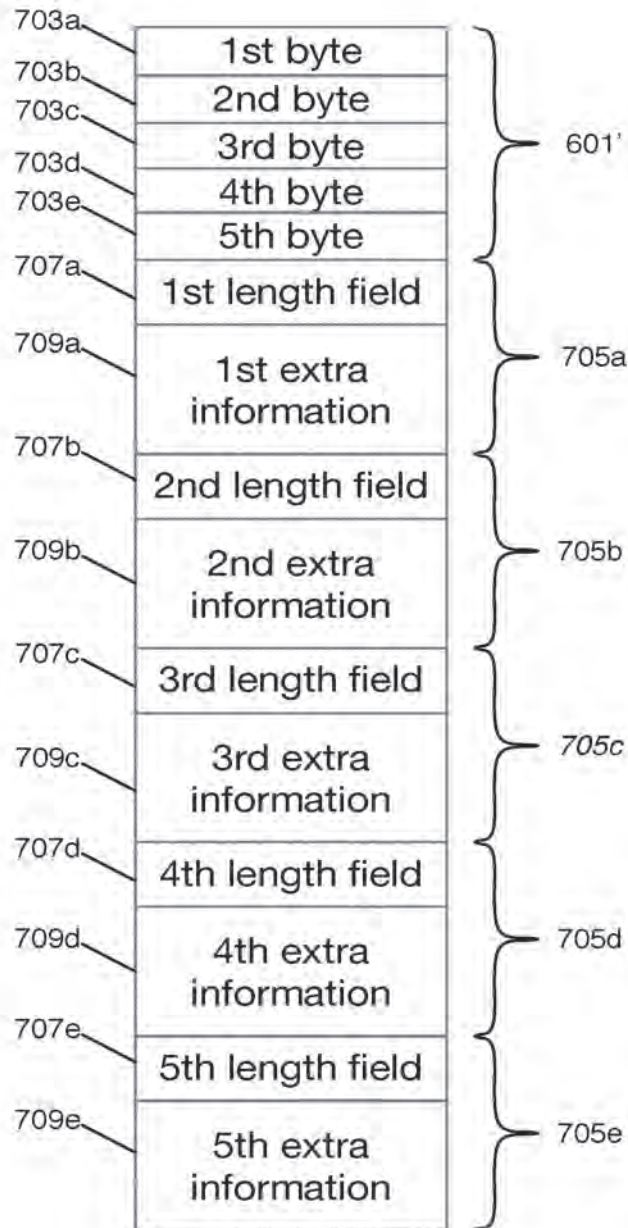


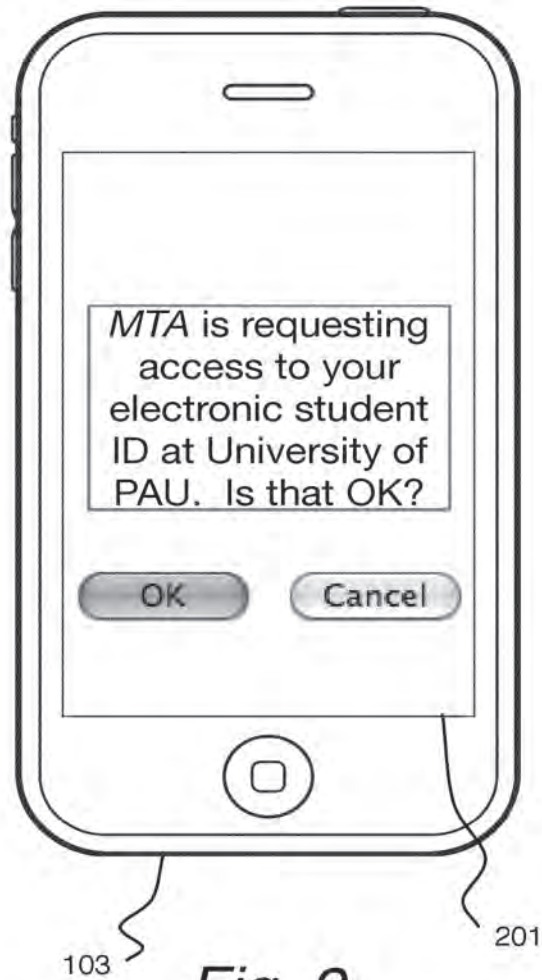
*Fig. 6b*

First byte								
b8	b7	b6	b5	b4	b3	b2	b1	
								Value determining the version of this template (for extensibility and interoperability)
Second byte								
b8	b7	b6	b5	b4	b3	b2	b1	value denoting the authentication protocol required
								e.g. digital signature
								e.g. reader authentication
								e.g. certificate verification
								e.g. secure messaging
								e.g. role authentication
								e.g. user consent ...
Third byte								NOTE: could be a coded over a nibble of the first byte if allowed
b8	b7	b6	b5	b4	b3	b2	b1	value denoting the HASH type
								e.g. SHA-256
								e.g. SHA-384
								e.g. SHA-512
								...
Fourth byte								
b8	b7	b6	b5	b4	b3	b2	b1	value denoting the signature scheme
								e.g. RSA
								e.g. ECDSA
								...
Fifth byte								
b8	b7	b6	b5	b4	b3	b2	b1	value denoting secure messaging options
								e.g. AES 128 bits - CMAC
								e.g. AES 128 bites - EMAC
								e.g. AES-GCM ...

601

Fig. 7

*Fig. 8*

*Fig. 9*

**DOCUMENT MADE AVAILABLE UNDER THE
PATENT COOPERATION TREATY (PCT)**

International application number:	PCT/EP2020/076906
International filing date:	25 September 2020 (25.09.2020)
Document type:	Certified copy of priority document
Document details:	Country/Office: EP
	Number: 19306357.5
	Filing date: 18 October 2019 (18.10.2019)
Date of receipt at the International Bureau:	30 September 2020 (30.09.2020)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-bis)

PCT

(PCT Rule 92*bis*.1 and
Administrative Instructions, Section 422)

LOTAUT, Yacine
THALES DIS FRANCE SAS
Intellectual Property Department
6 Rue de la Verrerie
92190 MEUDON
FRANCE

Date of mailing (<i>day/month/year</i>) 28 October 2021 (28.10.2021)	
Applicant's or agent's file reference GMT4110 WO/YL	IMPORTANT NOTIFICATION
International application No. PCT/EP2020/076906	International filing date (<i>day/month/year</i>) 25 September 2020 (25.09.2020)
1. The following indications appeared on record concerning: ☒ the applicant ☐ the inventor ☐ the agent ☐ the common representative	
Name and Address THALES DIS FRANCE SA 6, rue de la Verrerie 92190 MEUDON FRANCE	State of Nationality FR State of Residence FR Telephone No. Facsimile No. E-mail address:
2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning: ☒ the person ☐ the name ☐ the address ☐ the nationality ☐ the residence	
Name and Address THALES DIS FRANCE SAS 6, rue de la Verrerie 92190 MEUDON FRANCE	State of Nationality FR State of Residence FR Telephone No. Facsimile No. E-mail address: ☐ Notifications by e-mail authorized
3. Further observations, if necessary:	
4. A copy of this notification has been sent to: ☒ the receiving Office ☐ the International Preliminary Examining Authority ☐ the International Searching Authority ☒ the designated Offices concerned ☐ the Authority(ies) specified for supplementary search ☐ the elected Offices concerned ☐ other;	
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Blanc Veronique e-mail pct.team5@wipo.int Telephone No. +41 22 338 74 05

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

BACKGROUND OF THE INVENTION

[0001] The present invention relates, generally, mobile devices operating electronic identification (eID) wallet applications, and, more particularly, to security mechanisms for namespaces used to access data in eID wallet applications.

[0002] Mobile devices such as telephones and tablets provide users with many benefits that have allowed them to eliminate other devices and cards. For example, electronic wallets have allowed users to dispense with carrying many credit cards and enable users to load travel boarding passes and other tickets onto their mobile phones. Another emerging technology, known as electronic identification (eID), provides the ability to use mobile devices to store identification documents such as driver licenses, passports, national ID cards, university ID cards, and club membership cards.

[0003] At least one standard proposal for eID specifies the use of *namespaces* for accessing data stored in mobile Driving License application. ISO/IEC CD2 18013-5:2019, *Personal Identification — ISO-Compliant Driving Licence — Part 5: Mobile Driving Licence (mDL) application*. A namespace is a symbolic mechanism for organizing and identifying pieces of data. To access a piece of data a requestor specifies namespace identifier and a local name (unique within the namespace but not necessarily unique with respect to other namespaces).

[0004] Thus, using namespaces, within an eID wallet one or more eID applications may each have its own namespace that specifies the names of data managed by the eID application.

[0005] While multiple eID applications and associated namespaces managed by a mobile device can satisfy the same identification task, e.g., providing the age of a user, the level of confidence that a verifier associates with these multiple applications and namespaces may not be the same. For example, a government issued eID would typically provide a higher level of confidence than a club associated with a leisure activity.

[0006] Furthermore, eID applications may have security policy requirements before the eWallet allows access to the particular eID application and the information that it manages. Some such security policy requirements, e.g.,

cryptographic signatures of access requests, may be deemed overly cumbersome by certain attribute verifiers or a verifier may not be able to satisfy the requirements.

[0007] To allow a verifier to determine which namespace from which to request access, it is desirable to have a technology which allows uniform communication of namespaces available from a mobile device and namespace security policy access rules associated with such namespaces.

SUMMARY

[0008] A technology for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device provides for associating security policies with each of a plurality of supported namespaces on a mobile device and operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device. In an aspect, technology for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device includes transmitting a list of supported namespaces to the verifier module executing on the verifier and selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.

[0009] In a further aspect, a list of supported namespaces is transmitted to the verifier module and the verifier module selects at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace. In an aspect, prior to transmitting a list of supported namespaces to a verifier terminal via the reader, the mobile device filters out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

[0010] The security policy of each of the plurality of supported namespaces maybe transmitted from the mobile device to the reader, for examples, as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options. The required authentication may be selected from one or more of digital signature, reader

authentication, certificate verification, secure messaging, role authentication, and user consent.

[0011] In an aspect, the reader operates to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier associates with each namespace in the plurality of supported namespaces, for example, by selecting a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

[0012] In an aspect, the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory, the technology further including operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.

To achieve those and other advantages, and in accordance with the purpose of the invention as embodied and broadly described, the invention proposes a method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device, comprises the following steps:

- associating security policies with each of a plurality of supported namespaces on a mobile device; and

- operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device comprises the following steps:

- transmitting a list of supported namespaces to the verifier module executing on the verifier; and

- selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device, comprising the following steps:

transmitting a list of supported namespaces to the verifier module; and
selecting, by the verifier module, at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprising the following steps:

prior to transmitting a list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprising the following step of transmitting the security policy of each of the plurality of supported namespaces from the mobile device to the reader.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device wherein the required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprises operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier associates with each namespace in the plurality of supported namespaces.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprises

operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device wherein the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory, the method further comprising operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.

Another aspect of the invention is a mobile device comprising:

a processor; and

a memory for storing instructions executable by the processor and for storing electronic identity eID data, the memory including an eID wallet application having instructions to cause the processor to:

receive a list of selected namespaces from a reader;

in response to receiving the list of selected namespaces from the reader, transmitting security rules associated with each selected namespace according to a defined bytestring template.

In an aspect, the eID wallet application further comprises instruction to cause the processor to:

receive a request for supported namespaces from a reader;

transmit a list of supported name spaces to the reader.

In an aspect, the eID wallet application further comprises instruction to cause the processor to:

prior transmitting a list of supported namespaces to a reader, filter out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the reader.

In an aspect, the eID wallet application further comprises instruction to cause the processor to:

transmit the security policy of each of the plurality of supported namespaces to a reader connected to a verifier.

In an aspect, the eID wallet application wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

In an aspect, the present relates to a method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

- associating a security policy with each of a plurality of supported namespaces on a mobile device;

- transmitting the security policy of each of the plurality of supported namespaces to a reader connected to a verifier;

- selecting, by the reader, at least one of the namespaces as candidate namespaces, and transmitting from the reader to the mobile device, a list containing the candidate namespaces;

- transmitting to the reader by the mobile device, the security policy associated with each of the selected candidate namespaces;

- operating the reader to:

- determine for which of the candidate namespaces the reader can satisfy the security policy of the namespace; and

- if the verifier can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the verifier terminal can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the mobile device;

- if the verifier cannot satisfy the security policy of any of the candidate namespaces, rejecting access to the data item; and

- upon successful demonstration by the reader to the mobile device of satisfaction of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1 is a schematic illustrating an exemplary use case scenario.

[0014] FIG. 2 is an external representation of a mobile device.

[0015] FIG. 3 is a block diagram illustrating major components of a hardware and software architecture for a mobile device.

[0016] FIG. 4 is a block diagram illustrating one embodiment organization for a reader.

[0017] FIG. 5 is a block diagram illustrating one embodiment organization for a verifier that contains a reader of FIG. 4.

[0018] FIG. 6 (which is partitioned onto FIGs. 6a and 6b) is a timing sequence diagram illustrating a process for communicating namespaces available on a mobile device to a reader.

[0019] FIG. 7 is a table illustrating an example protocol for namespace-security-policy messages.

[0020] FIG. 8 is a block diagram of a namespace security representation containing a template and additional information byte sequences.

[0021] FIG. 9 is a diagram showing a dialog box displayed on a mobile device to obtain user acquiescence for use of a namespace.

DETAILED DESCRIPTION OF THE INVENTION

[0022] In the following detailed description, reference is made to the accompanying drawings that show, by way of illustration, specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. It is to be understood that the various embodiments of the invention, although different, are not necessarily mutually exclusive. For example, a particular feature, structure, or characteristic described herein in connection with one embodiment may be implemented within other embodiments without departing from the spirit and scope of the invention. In addition, it is to be understood that the location or arrangement of individual elements within each disclosed embodiment may be modified without departing from the spirit and scope of the invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims, appropriately interpreted, along with the full range of equivalents to which the claims are entitled. In the drawings, like numerals refer to the same or similar functionality throughout the several views.

[0023] The following description includes references to various methods executed by a processor of mobile device or a terminal, known herein as the reader or the verifier. As is common in the field, there may be phrases herein that indicate these methods or method steps are performed by software instructions or software modules. As a person skilled in the art knows, such

descriptions should be taken to mean that a processor, in fact, executes the methods, software instructions, and software modules.

[0024] The herein described technology provides mechanisms to provide discoverability of security policies for electronic identification data organized in namespaces on mobile devices with total abstraction of the data structures used on the mobile devices. As such the technology provides an improvement to mobile devices used for electronic identification purposes and the overall system of electronic identification by providing technology by which security access rules may be assigned to namespaces that are used to address electronic identification data stored on mobile devices when mobile devices are used to make identity-based identification or attribute assertions whereby electronic identification readers and verifiers may select appropriate namespaces hosted by electronic devices for verifying electronic identification-based attribute assertions. The technology improves a mobile device by providing such devices the ability to offer more flexibility in assignment of security policies and communication of such security policies to readers and verifiers of electronic identification data.

[0025] First a use case. There are many instances in which an individual seeks to establish an attribute that will allow that individual a certain privilege. That may be an access to a restricted physical space, the right to participate in a program, access to a private or age-restricted material, or access to an attribute-restricted benefit. A reduced fare only available to students and senior citizens is an example of an attribute-restricted benefit.

[0026] Suppose, a person wishing to travel on a metro system is entitled to a 50% discount if the person is either a student or a senior citizen. A person may have on her mobile device several eID applications that may be useful to demonstrate satisfaction of one or both of the requirements for reduced fare, e.g.,

- a government issued identity card, for example, from AGENCE NATIONALE DES TITRES SÉCURISÉS (ants.gouv.fr; French National Agency for Secure Documents) or TEXAS DEPARTMENT OF PUBLIC SAFETY (dps.texas.gov)
- a university departmental ID, for example, University of Pau (univ-pau.fr) or University of Texas (utexas.edu)
- a club for a leisure activity, for example, a stamp collection club (pau-philatelie.asso.org) or a garden club (merryweeders.org)

[0027] Each of the eID applications may store information that can be used to prove that a person is a student or of a certain age; e.g., the government ID typically store birthdates and may have a professional status (e.g., retired or student), the university ID would certainly indicate if a person is a student, faculty or alumnus, and even the stamp club may charge a different membership fee for students and therefore have a flag set for a member being a student, and the garden club may store birthdates so that they can celebrate members on their respective birthdays.

[0028] When the prospective passenger wishes to purchase a monthly pass for the metro, they presents their mobile device to a ticket vendor, which may either be an automatic ticket self-use vending terminal or an individual employee of the metro authority, who would operate a verification terminal. If the passenger is a student or senior, the passenger offers his or her eID wallet to prove that fact. The passenger or the metro official places the mobile device on a terminal.

[0029] The eID wallet communicates the desired attribute to the terminal and the terminal decides whether to grant the discount or not.

[0030] FIG. 1 is a schematic illustrating the above-described use-case example scenario and alternatives. A user 101 operates a mobile device 103, e.g., a mobile telephone. The mobile device 103 contains an eID wallet with one or more eID applications (see FIG. 2). The eID functionality of the mobile device 103 may be used by the user 101 to prove identity or an identity-related attribute to a verifier. The verifier may be a human verifier 115 interacting with reader 109 and a verifier computer 105 via a user interface 117 connected to a reader 109. For example, if the user 101 seeks to obtain access to a facility based on a membership status, the user 101 may present the mobile device 103 to a security guard (human verifier) 115. A verifier module 111", executable by the reader 109 or the verifier 105, provides the dialog user interface 117 to the human verifier 115 to verify proffered identification from the user 101.

[0031] Alternatively, the verifier may be performed automatically when the user 101 places the mobile device 103 on the reader 109, for example, if the reader 109 is connected to an automated verifier 105', executing a software verifier module 111', in communication with a reader 109'. While depicted here as separate units, the reader 109' and the verifier 105' may be one machine. An example may be a ticket vending machine in which a traveler has to demonstrate being a member of a particular age group.

[0032] In an alternative use case, the mobile device 103 is used to provide identity functionality over the internet 113 to a remote server 115 on which a verifier module 111 is executing.

[0033] FIG. 2 is an external representation of a mobile device 103 and FIG. 3 is a block diagram illustrating major components of a hardware and software architecture for a mobile device 103. The mobile device 103 contains a touch screen user interface 201 for receiving input from the user 101 and for providing output to the user 101 as well as a camera 203 by which the mobile device may receive input from a reader 109, e.g., by scanning QR codes or bar codes displayed on the reader 109.

[0034] As illustrated in FIG. 3, the mobile device 103 contains a processor 301, a communications interface 303, and a non-volatile memory (NVM) 305. The NVM 305 contains programs including an operating system 307 and application programs, referred to as “apps”, which includes an eIDWallet app 309.

[0035] The communications interface 303, which may be used for mobile telephony, NFC, Bluetooth, WiFi, etc., allows the mobile device 103 to communicate with the reader 109 or the remote server 115. Alternatively, the mobile device 103 may communicate to the reader 109 via the screen 201 and camera 203 the reader 109 maybe an optical device that reads information transmitted via the screen 201 of the mobile device 103 and outputs information that the mobile device 103 may input via the camera 203.

[0036] The eIDWallet app 309 manages eIDWallet information, e.g., in an eIDWalletDB 311 organized around a number of namespaces 313a-n.

[0037] The architecture of FIG. 3 is merely one example. For example, in an alternative embodiment, there may be multiple eIDWallet apps each with its own namespace.

[0038] Each namespace provides access to a number of data elements and defines its own names for those data elements. An example namespace may be found in

ISO/IEC CD2 18013-5:2019, *Personal Identification — ISO-Compliant Driving Licence — Part 5: Mobile Driving Licence (mDL) application*, section 7 “Data Model”, incorporated herein by reference.

[0039] However, while two namespaces may contain the same data elements, these data elements may not have the same name in the two namespaces. For example, *Date of birth* (from the sample namespace in Appendix I) may be named *BirthDate* in another namespace. Similarly, two different data

elements may provide an equivalent piece of information, e.g., *Date of birth* may be used to derive *age*.

[0040] Namespaces may be addressed in different ways, for example, URI, URL, URN, OID, UUID, or reverse domain namespace representation. In reverse domain representation, the namespace may be defined as *reverseDomain.domainSpecificExtension*. For example, for the French National Agency for Secure Documents, the reverse domain namespace identifier may be *fr.gouv.ants.id*, and for a stamp club, *org.asso.philatelie.role*.

[0041] FIG. 4 is a block diagram illustrating one embodiment organization for a reader 109. The reader 109 includes a processor 401, a storage unit 403, an interface unit 405, for example, for interfacing with the processor of the verifier 105, and a communications module 407, for example, for NFC, WiFi, Bluetooth communication with the mobile device 103.

[0042] The storage unit 403 contains software modules including an operating system (OS) 409 and a reader module 411, which contains instructions to the processor 401 to carry out reader-side namespace selection as illustrated and described hereinbelow.

[0043] FIG. 5 is a block diagram illustrating one embodiment organization for a verifier 105. The verifier includes a processor 451, a storage unit 453, an input/output interface unit 405, for example, for interfacing with a user interface device for communicating with a human operator 115 or the user 101, and a communications module 457, for example, for NFC, WiFi, or Bluetooth communication with the mobile device 103. The storage unit 403 contains software modules including an operating system (OS) 459 and a verifier module 111 for carrying out tasks related to verifying an eID attribute assertion, for example, one related to verifying eligibility based on an attribute or identity.

[0044] Note, there are tasks of the reader module 411 as well as the verifier module 111 that may be carried out by a human operator. For example, as discussed in conjunction with the timing sequence diagram of FIG. 6 that follows hereinbelow, selection of a namespace based on level of security may be performed using a dialog with a human identity-based-assertion verifier (see, FIG. 1, 115). Accordingly, the verifier 105 may include an I/O interface 455 for connecting to user interface devices, such as a terminal for displaying graphic user interface elements 117.

[0045] FIG. 6 (which is partitioned onto FIGs. 6a and 6b) is a timing sequence diagram illustrating a process for communicating namespaces available

on a mobile device 103 to a verifier 105 including a reader 109. The process executed by the reader 109 may be under control of a software module referred to herein as the reader module 411. It should be noted that there is no strict demarcation between the reader 109 and verifier 105. Tasks described herein as performed by one may be performed by the other. Furthermore, the reader 109 and verifier 105 may be either completely separated or merged into one unit or any arrangement between those two extremes.

[0046] As a preliminary step a user 101 operating the mobile device 103 seeks to make an identity-based assertion, step 501. The identity-based assertion may be a request to access a service based on a certified attestation of an identity attribute, e.g., age, or to demonstrate that the user 101 is a particular person. The user 101 presents the mobile device 103, which contains and executes an eIDWallet app 309, to the reader 109 and a communications session, e.g., NFC, Bluetooth, WiFi, or optical transmission, is established between the mobile device 103 and the reader 109.

[0047] In response to the establishment of an eID communications session, the reader 109 responds by requesting from the mobile device 103 a listing of eID namespaces supported by the mobile device 103, step 503.

[0048] The mobile device 103 responds with a list of supported eID namespaces, step 505. The list may be a concatenation or structured set of namespace identifiers, for example, in the form of URI, URL, URN, OID, UUID, or reverse domain name representation. In an embodiment, the mobile device 103 requests confirmation by the user 101 that the user acquiesces to releasing particular namespaces to the reader 109 and verifier 105. For example, if one namespace that contains a birthdate is associated with a political organization, the user may prefer to not reveal membership in that organization to the reader 109 and verifier 105.

[0049] Using, for example, reverse domain name representation, for a French-citizen student at the University of Pau, France, who is a stamp collector, the mobile device 103 may return:

National identification: *fr.gouv.ants.id* (the French National Agency for Secure Documents)

Student identification: *fr.edu.univ-pau.labo.profile* (University of Pau)

Membership card in stamp club: *org.asso.philatelie.role* (Stamp collectors club)

[0050] Depending on the request for which the identity assertion (step 501) is made, the verifier 105 determines the level of security (LOS) that should be associated with the request, step 507. For example, a bank cashing a check may require an identity assertion associated with a national ID whereas for proving entitlement to a student fare, a university ID may be sufficient.

[0051] Based on the required LOS, the verifier 105 selects one or more namespaces that satisfy the required LOS, step 509, and sends a request for access to these namespaces to the mobile device 103, step 511. The verifier 105 may have a whitelist of namespaces that may be used to satisfy LOS for an identity-based assertion. For example, a metropolitan transit authority may accept national IDs as well as student IDs from local universities. Conversely, the verifier 105 may have a blacklist of namespaces that are not allowed to be used for an identity-based assertion; i.e., that are deemed to not meet the LOS required.

[0052] The mobile device 103 responds with the security policy access rules associated with each of the requested namespaces, step 513.

[0053] In a preferred embodiment, the security policies of namespaces are communicated according to a standard protocol or an interoperability template. The namespace-security-policy protocol may consist of a sequence of bytes in which each bit signifies a particular security policy attribute.

[0054] FIG. 7 is a table illustrating an example 601 protocol for namespace-security-policy messages.

[0055] In the example 601, the first byte is used to communicate a version number of the template used for communicating namespace security policy.

[0056] The second byte of the example template 601 contains a value for denoting the required authentication protocol. The first bit (b1) indicates whether digital signature is required or not. The second bit (b2) indicates whether reader authentication is required. The third bit (b3) is used to indicate whether certificate verification is required. The fourth bit (b4) is used to indicate whether secure messaging is required. The fifth bit (b5) is used to indicate whether role authentication is required. The sixth bit (b6) indicates whether user consent is required.

[0057] The third byte indicates the HASH type to be used. For example, first through third bit indicate to use SHA-256, SHA-384, and SHA-512, respectively. Other bits could be used to indicate alternative hashing schemes. No bit set indicates that hashing is not to be used.

[0058] The fourth byte indicates the scheme for digital signatures to be used. For example, the first and second bits indicate RSA and ECDSA, respectively. Other bits may indicate to use other digital signature schemes. No bit set indicates that digital signature is not required.

[0059] The fifth byte denotes which secure messaging option to use. The first through third bit indicate AES 128 bit-CMAC, AES 128 bit-EMAC, and AES-GCM, respectively. Other bits may indicate to use other secure messaging options. No bit set indicates that secure messaging is not required.

[0060] It should be noted that the template illustrated in FIG. 7 and described above is merely an example. Other arrangements are possible. For example, several of the bytes that only use a few bits to convey information can be combined.

[0061] Returning to FIG. 6, having received the security policy access rules (step 513), the reader 109 determines if there is at least one namespace with acceptable access rules, step 515. For example, if the mobile device 103 demands verification of a digital signature to access a namespace for verification of age to access a website, that may be considered too onerous by the verifier 105. Furthermore, if the verifier 105 may not have the capability to satisfy a demanding access rule and therefore be forced into requesting access to a namespace with a less demanding access rule. Accordingly, the verifier 105 may have, for example, selection rules such as to not select namespaces that require certificate verification or more than 128-bit encryption.

[0062] If there is no namespace provided by the mobile device 103 with acceptable level of confidence and acceptable access rules, the reader 109 may decline access to the service or benefit requested by the mobile device 103, step 515, and a message declining access to the requested service is transmitted to the mobile device 103, step 515.

[0063] Otherwise, the reader 109 selects a namespace with an acceptable security policy, step 519.

[0064] With the selected namespace, the reader satisfies the access rules required by the mobile device and sends an access request message with the namespace identifier, data element name (used by the namespace to address the required data element), required information or format according to the access rule for the namespace, e.g., certificate, hashed message, step 521.

[0065] In an embodiment, the namespace security policy representation 601 further contains additional information, e.g., a certificate route

or digital information necessary to resolve certain cryptographic references. For example, the security policy access rules can be satisfied by the verifier 105 or reader 109 if the verifier/reader has references to, e.g., the cryptographic keys to use, a route to a Certificate Authority root public key (for certificate verification), or an object identifier (OID) denoting a crypto-suite to be performed by the verifier/reader. To provide this additional information, the namespace security policy template 601 transmitted in step 513 may be appended with a byte sequence providing the required data for the defined security mechanisms to allow access to eID data from the mobile device 103 corresponding to each of the bytes in the template.

[0066] FIG. 8 is a block diagram of namespace security representation 701 containing a template 601' and additional information byte sequences 705a-e.

[0067] The example namespace security representation 701 contains the five bytes 703a-e corresponding to the five-byte template 601'. Each of these has a corresponding additional-information byte sequence 705a-e. Each of these additional byte sequences 705a-e are in length-value format, i.e., the first field 707a-e indicating the number of bytes of the value field 709a-e; a 0 value in the length field 707a-e indicates that there is no additional information sequence corresponding to a particular byte in the template and thus, the value field 709a-e would be an empty sequence.

[0068] There are many different possible syntaxes for the length fields. In a simple case, the length field is simply a fixed number of bytes, e.g., one or two bytes.

[0069] Thus, the security policy access rule communication may be:
 1st byte||2nd byte||3rd byte||4th byte||5th byte||0x00||0x0C||<12 byte
 OID>>||0x00||0x08||<eight byte key>>||0x00

where

- the first five bytes correspond to the security policy access rules as described in conjunction with FIG. 7
- 0x00 indicates a zero-length value field, i.e., no value, corresponding to the first byte 703a
- 0x0C is the length field with the hexadecimal value indicating that 12 bytes is to follow for additional information corresponding to the second byte 703b; in the example, the following 12 bytes is a representation of the OID denoting the

crypto-suite applying the authentication protocol defined in the 2nd byte of the security policy access rules

- The second 0x00 indicates that there is no additional information corresponding to the third byte 703c
- 0x08 indicates that the following value field, corresponding to the fourth byte 703d, is eight bytes long and the following eight bytes, in this example, is an eight-byte cryptographic key
- the third 0x00 indicates that for the fifth byte 703e there is no additional information byte sequence

[0070] Other mechanisms for indicating the length of the additional value field include using an escape sequence, e.g., 0xFF, to indicate that the following byte contains the length of the length field. For example, 0xFF020216 would indicate that the length field (0x02) is two bytes long and those two bytes indicate that the following byte sequence is 0x0216 (534) bytes long. Yet another mechanism is to have the first byte of each additional information sequence 705 indicate the length of the length field.

[0071] As noted above, user consent may be one possible access rule. Thus, if user consent is required, the mobile device 103 may display on the user interface 201 a message to the user indicating the access request, for example, as indicated in FIG. 9, which is a diagram showing a dialog box displayed on a mobile device 103. If the user cancels, the access is denied. Conversely, the access to the requested service also not granted. However, in a follow-up dialog, the user 101 may be provided the opportunity to select another eID namespace for the identity-based assertion required by the reader 109.

[0072] Returning again to FIG. 6, if the reader 109 has satisfied the requirements of the access rules for the requested namespace, the eWallet app 309 of the mobile device 103 retrieves the required data using the namespace data element name provided, step 523, and provides identity-based assertion to the reader 109, step 525.

[0073] The reader 109 or verifier 105 then determines whether the identity-based assertion has been proved by the eID namespace, step 527. If the assertion has not been proved, access is denied, step 517. Otherwise, access to the requested service based on the identity-assertion made using the requested eID data element addressed using the selected namespace and data-element name (step 521), the access to the requested service or benefit is provided, step 529.

[0074] From the foregoing it will be apparent that an efficient and secure mechanism for associating security policy access rules with namespaces used in eID wallets is provided.

[0075] Although specific embodiments of the invention have been described and illustrated, the invention is not to be limited to the specific forms or arrangements of parts so described and illustrated. The invention is limited only by the claims.

[0076] We Claim:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appln. No.	: Unassigned	Confirmation No.	: Unassigned
Examiner	: Unassigned	TC/A.U.	: Unassigned
Applicant	: THALES DIS FRANCE SAS		
Inventors	: Mourad FAHER; et al.		
Filing Date	: Unassigned		
Title	:		

**SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC
IDENTIFICATION ON MOBILE DEVICES**

PRELIMINARY AMENDMENT

MAIL STOP AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

April 6, 2022

Commissioner for Patents:

Prior to examination of the above-captioned patent application, please kindly
amend the application as follows:

Amendments to the Claims begins on page **2** of this submission.

Amendments to the Abstract begin on page **7** of this submission

Applicant Remarks begin on page **10** of this submission.

The above preliminary amendments are timely filed in accordance with 37 CFR §
1.115, and in compliance with 37 CFR § 1.121. No new matter has been added.

This application is for entry to the U.S. national phase of a PCT application.

Please charge any deficiencies or credit any overpayment to Deposit Account
No. **60-4092**.

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the immediate application:

Listing of Claims:

1. ~~(Original)~~ A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:
 - associating security policies with each of a plurality of supported namespaces on a mobile device; and
 - operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.
2. ~~(Currently Amended)~~ The method of claim 1 for managing security policies for data items stored in ~~an the~~ electronic identification (eID) wallet on ~~a the~~ mobile device of ~~Claim 1~~, comprising:
 - transmitting a list of supported namespaces to the verifier module executing on the verifier; and
 - selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.
3. ~~(Currently Amended)~~ The method of claim 1 for managing security policies for data items stored in ~~an the~~ electronic identification (eID) wallet on ~~a the~~ mobile device ~~according to any previous claims~~, comprising:
 - transmitting a list of supported namespaces to the verifier module; and
 - selecting, by the verifier module, at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

4. ~~(Currently Amended)~~ The method ~~of claim 1~~ for managing security policies for data items stored in ~~an the~~ electronic identification (eID) wallet on ~~a the~~ mobile device ~~according to any previous claims~~ further comprising:

prior to transmitting a list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

5. ~~(Currently Amended)~~ The method ~~of claim 1~~ for managing security policies for data items stored in ~~an the~~ electronic identification (eID) wallet on ~~a the~~ mobile device ~~according to any previous claims~~, comprising:

transmitting the security policy of each of the plurality of supported namespaces from the mobile device to the reader.

6. ~~(Currently Amended)~~ The method ~~of claim 1~~ for managing security policies for data items stored in ~~an the~~ electronic identification (eID) wallet on ~~a the~~ mobile device, ~~according to any previous claims~~

wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

7. ~~(Currently Amended)~~ The method ~~of claim 1~~ for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device ~~according to any previous claims~~,

wherein the required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

8. ~~(Currently Amended)~~ The method ~~of claim 1~~ for managing security policies for data items stored in ~~an the~~ electronic identification (eID) wallet on ~~a the~~ mobile device ~~according to any previous claims~~ further comprises

operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier associates with each namespace in the plurality of supported namespaces.

9. ~~(Currently Amended)~~ The method ~~of claim 1~~ for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, ~~according to any previous claims~~ further comprises

operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

10. ~~(Currently Amended)~~ The method ~~of claim 1~~ for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, ~~according to any previous claims~~

wherein the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory, the method further comprising operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.

11. ~~(Original)~~ A mobile device comprising:

a processor; and

a memory for storing instructions executable by the processor and for storing electronic identity (eID) data, the memory including an eID wallet application having instructions to cause the processor to:

receive a list of selected namespaces from a reader;

in response to receiving the list of selected namespaces from the reader, transmitting security rules associated with each selected namespace according to a defined bytestring template.

12. ~~(Original)~~ The mobile device of claim 0, wherein the eID wallet application further comprises instruction to cause the processor to:

receive a request for supported namespaces from a reader;
transmit a list of supported name spaces to the reader.

13. (Currently Amended) The mobile device according to ~~claims 11 to 12~~ claim 12, wherein the eID wallet application further comprises instruction to cause the processor to:

prior transmitting a list of supported namespaces to a reader, filter out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the reader.

14. (Currently Amended) The mobile device according to ~~claims 11 to 13~~ claim 13, wherein the eID wallet application further comprises instruction to cause the processor to:

transmit the security policy of each of the plurality of supported namespaces to a reader connected to a verifier.

15. (Currently Amended) The mobile device according to ~~claims 11 to 12~~ claim 12, wherein the eID wallet application wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

16. (Original) A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

associating a security policy with each of a plurality of supported namespaces on a mobile device;

transmitting the security policy of each of the plurality of supported namespaces to a reader connected to a verifier;

selecting, by the reader, at least one of the namespaces as candidate namespaces, and transmitting from the reader to the mobile device, a list containing the candidate namespaces;

transmitting to the reader by the mobile device, the security policy associated with each of the selected candidate namespaces;

operating the reader to:

determine for which of the candidate namespaces the reader can satisfy the security policy of the namespace; and

if the verifier can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the verifier terminal can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the mobile device;

if the verifier cannot satisfy the security policy of any of the candidate namespaces, rejecting access to the data item; and

upon successful demonstration by the reader to the mobile device of satisfaction of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

ABSTRACT

A system, mobile device, and method for managing security policies for data items stored in an electronic identification (eID) wallet on the mobile device. Security policies are associated with each of a plurality of supported namespaces on a mobile device and a verifier terminal operates to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.

Application No. Unassigned
Amendment dated April 6, 2022
Attorney Docket No.: GMT4110US/WO

REMARKS

Favorable consideration of the application in view of the foregoing amendments is respectfully requested. Should any questions arise in connection with this application, it is respectfully requested that the undersigned be contacted at the number indicated below.

Respectfully submitted,

Date: April 6, 2022

/Marc Boillot/

Marc A. Boillot
USPTO Reg. No.: 56,164
Telephone: (954) 658-0418

Customer No.: 180929

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

BACKGROUND OF THE INVENTION

[0001] The present invention relates, generally, mobile devices operating electronic identification (eID) wallet applications, and, more particularly, to security mechanisms for namespaces used to access data in eID wallet applications.

[0002] Mobile devices such as telephones and tablets provide users with many benefits that have allowed them to eliminate other devices and cards. For example, electronic wallets have allowed users to dispense with carrying many credit cards and enable users to load travel boarding passes and other tickets onto their mobile phones. Another emerging technology, known as electronic identification (eID), provides the ability to use mobile devices to store identification documents such as driver licenses, passports, national ID cards, university ID cards, and club membership cards.

[0003] At least one standard proposal for eID specifies the use of *namespaces* for accessing data stored in mobile Driving License application. ISO/IEC CD2 18013-5:2019, *Personal Identification — ISO-Compliant Driving Licence — Part 5: Mobile Driving Licence (mDL) application*. A namespace is a symbolic mechanism for organizing and identifying pieces of data. To access a piece of data a requestor specifies namespace identifier and a local name (unique within the namespace but not necessarily unique with respect to other namespaces).

[0004] Thus, using namespaces, within an eID wallet one or more eID applications may each have its own namespace that specifies the names of data managed by the eID application.

[0005] While multiple eID applications and associated namespaces managed by a mobile device can satisfy the same identification task, e.g., providing the age of a user, the level of confidence that a verifier associates with these multiple applications and namespaces may not be the same. For example, a government issued eID would typically provide a higher level of confidence than a club associated with a leisure activity.

[0006] Furthermore, eID applications may have security policy requirements before the eWallet allows access to the particular eID application and the information that it manages. Some such security policy requirements, e.g.,

cryptographic signatures of access requests, may be deemed overly cumbersome by certain attribute verifiers or a verifier may not be able to satisfy the requirements.

[0007] To allow a verifier to determine which namespace from which to request access, it is desirable to have a technology which allows uniform communication of namespaces available from a mobile device and namespace security policy access rules associated with such namespaces.

SUMMARY

[0008] A technology for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device provides for associating security policies with each of a plurality of supported namespaces on a mobile device and operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device. In an aspect, technology for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device includes transmitting a list of supported namespaces to the verifier module executing on the verifier and selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.

[0009] In a further aspect, a list of supported namespaces is transmitted to the verifier module and the verifier module selects at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace. In an aspect, prior to transmitting a list of supported namespaces to a verifier terminal via the reader, the mobile device filters out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

[0010] The security policy of each of the plurality of supported namespaces maybe transmitted from the mobile device to the reader, for examples, as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options. The required authentication may be selected from one or more of digital signature, reader

authentication, certificate verification, secure messaging, role authentication, and user consent.

[0011] In an aspect, the reader operates to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier associates with each namespace in the plurality of supported namespaces, for example, by selecting a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

[0012] In an aspect, the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory, the technology further including operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.

To achieve those and other advantages, and in accordance with the purpose of the invention as embodied and broadly described, the invention proposes a method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device, comprises the following steps:

- associating security policies with each of a plurality of supported namespaces on a mobile device; and

- operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device comprises the following steps:

- transmitting a list of supported namespaces to the verifier module executing on the verifier; and

- selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device, comprising the following steps:

- transmitting a list of supported namespaces to the verifier module; and
- selecting, by the verifier module, at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprising the following steps:

- prior to transmitting a list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprising the following step of transmitting the security policy of each of the plurality of supported namespaces from the mobile device to the reader.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device wherein the required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprises operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier associates with each namespace in the plurality of supported namespaces.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprises

operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device wherein the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory, the method further comprising operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.

Another aspect of the invention is a mobile device comprising:

a processor; and

a memory for storing instructions executable by the processor and for storing electronic identity eID data, the memory including an eID wallet application having instructions to cause the processor to:

receive a list of selected namespaces from a reader;

in response to receiving the list of selected namespaces from the reader, transmitting security rules associated with each selected namespace according to a defined bytestring template.

In an aspect, the eID wallet application further comprises instruction to cause the processor to:

receive a request for supported namespaces from a reader;

transmit a list of supported name spaces to the reader.

In an aspect, the eID wallet application further comprises instruction to cause the processor to:

prior transmitting a list of supported namespaces to a reader, filter out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the reader.

In an aspect, the eID wallet application further comprises instruction to cause the processor to:

transmit the security policy of each of the plurality of supported namespaces to a reader connected to a verifier.

In an aspect, the eID wallet application wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

In an aspect, the present relates to a method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

- associating a security policy with each of a plurality of supported namespaces on a mobile device;

- transmitting the security policy of each of the plurality of supported namespaces to a reader connected to a verifier;

- selecting, by the reader, at least one of the namespaces as candidate namespaces, and transmitting from the reader to the mobile device, a list containing the candidate namespaces;

- transmitting to the reader by the mobile device, the security policy associated with each of the selected candidate namespaces;

- operating the reader to:

- determine for which of the candidate namespaces the reader can satisfy the security policy of the namespace; and

- if the verifier can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the verifier terminal can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the mobile device;

- if the verifier cannot satisfy the security policy of any of the candidate namespaces, rejecting access to the data item; and

- upon successful demonstration by the reader to the mobile device of satisfaction of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1 is a schematic illustrating an exemplary use case scenario.

[0014] FIG. 2 is an external representation of a mobile device.

[0015] FIG. 3 is a block diagram illustrating major components of a hardware and software architecture for a mobile device.

[0016] FIG. 4 is a block diagram illustrating one embodiment organization for a reader.

[0017] FIG. 5 is a block diagram illustrating one embodiment organization for a verifier that contains a reader of FIG. 4.

[0018] FIG. 6 (which is partitioned onto FIGs. 6a and 6b) is a timing sequence diagram illustrating a process for communicating namespaces available on a mobile device to a reader.

[0019] FIG. 7 is a table illustrating an example protocol for namespace-security-policy messages.

[0020] FIG. 8 is a block diagram of a namespace security representation containing a template and additional information byte sequences.

[0021] FIG. 9 is a diagram showing a dialog box displayed on a mobile device to obtain user acquiescence for use of a namespace.

DETAILED DESCRIPTION OF THE INVENTION

[0022] In the following detailed description, reference is made to the accompanying drawings that show, by way of illustration, specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. It is to be understood that the various embodiments of the invention, although different, are not necessarily mutually exclusive. For example, a particular feature, structure, or characteristic described herein in connection with one embodiment may be implemented within other embodiments without departing from the spirit and scope of the invention. In addition, it is to be understood that the location or arrangement of individual elements within each disclosed embodiment may be modified without departing from the spirit and scope of the invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims, appropriately interpreted, along with the full range of equivalents to which the claims are entitled. In the drawings, like numerals refer to the same or similar functionality throughout the several views.

[0023] The following description includes references to various methods executed by a processor of mobile device or a terminal, known herein as the reader or the verifier. As is common in the field, there may be phrases herein that indicate these methods or method steps are performed by software instructions or software modules. As a person skilled in the art knows, such

descriptions should be taken to mean that a processor, in fact, executes the methods, software instructions, and software modules.

[0024] The herein described technology provides mechanisms to provide discoverability of security policies for electronic identification data organized in namespaces on mobile devices with total abstraction of the data structures used on the mobile devices. As such the technology provides an improvement to mobile devices used for electronic identification purposes and the overall system of electronic identification by providing technology by which security access rules may be assigned to namespaces that are used to address electronic identification data stored on mobile devices when mobile devices are used to make identity-based identification or attribute assertions whereby electronic identification readers and verifiers may select appropriate namespaces hosted by electronic devices for verifying electronic identification-based attribute assertions. The technology improves a mobile device by providing such devices the ability to offer more flexibility in assignment of security policies and communication of such security policies to readers and verifiers of electronic identification data.

[0025] First a use case. There are many instances in which an individual seeks to establish an attribute that will allow that individual a certain privilege. That may be an access to a restricted physical space, the right to participate in a program, access to a private or age-restricted material, or access to an attribute-restricted benefit. A reduced fare only available to students and senior citizens is an example of an attribute-restricted benefit.

[0026] Suppose, a person wishing to travel on a metro system is entitled to a 50% discount if the person is either a student or a senior citizen. A person may have on her mobile device several eID applications that may be useful to demonstrate satisfaction of one or both of the requirements for reduced fare, e.g.:

- a government issued identity card, for example, from AGENCE NATIONALE DES TITRES SÉCURISÉS (ants.gouv.fr; French National Agency for Secure Documents) or TEXAS DEPARTMENT OF PUBLIC SAFETY (dps.texas.gov)
- a university departmental ID, for example, University of Pau (univ-pau.fr) or University of Texas (utexas.edu)
- a club for a leisure activity, for example, a stamp collection club (pau-philatelie.asso.org) or a garden club (merryweeders.org)

[0027] Each of the eID applications may store information that can be used to prove that a person is a student or of a certain age; e.g., the government ID typically store birthdates and may have a professional status (e.g., retired or student), the university ID would certainly indicate if a person is a student, faculty or alumnus, and even the stamp club may charge a different membership fee for students and therefore have a flag set for a member being a student, and the garden club may store birthdates so that they can celebrate members on their respective birthdays.

[0028] When the prospective passenger wishes to purchase a monthly pass for the metro, they presents their mobile device to a ticket vendor, which may either be an automatic ticket self-use vending terminal or an individual employee of the metro authority, who would operate a verification terminal. If the passenger is a student or senior, the passenger offers his or her eID wallet to prove that fact. The passenger or the metro official places the mobile device on a terminal.

[0029] The eID wallet communicates the desired attribute to the terminal and the terminal decides whether to grant the discount or not.

[0030] FIG. 1 is a schematic illustrating the above-described use-case example scenario and alternatives. A user 101 operates a mobile device 103, e.g., a mobile telephone. The mobile device 103 contains an eID wallet with one or more eID applications (see FIG. 2). The eID functionality of the mobile device 103 may be used by the user 101 to prove identity or an identity-related attribute to a verifier. The verifier may be a human verifier 115 interacting with reader 109 and a verifier computer 105 via a user interface 117 connected to a reader 109. For example, if the user 101 seeks to obtain access to a facility based on a membership status, the user 101 may present the mobile device 103 to a security guard (human verifier) 115. A verifier module 111", executable by the reader 109 or the verifier 105, provides the dialog user interface 117 to the human verifier 115 to verify proffered identification from the user 101.

[0031] Alternatively, the verifier may be performed automatically when the user 101 places the mobile device 103 on the reader 109, for example, if the reader 109 is connected to an automated verifier 105', executing a software verifier module 111', in communication with a reader 109'. While depicted here as separate units, the reader 109' and the verifier 105' may be one machine. An example may be a ticket vending machine in which a traveler has to demonstrate being a member of a particular age group.

[0032] In an alternative use case, the mobile device 103 is used to provide identity functionality over the internet 113 to a remote server 115 on which a verifier module 111 is executing.

[0033] FIG. 2 is an external representation of a mobile device 103 and FIG. 3 is a block diagram illustrating major components of a hardware and software architecture for a mobile device 103. The mobile device 103 contains a touch screen user interface 201 for receiving input from the user 101 and for providing output to the user 101 as well as a camera 203 by which the mobile device may receive input from a reader 109, e.g., by scanning QR codes or bar codes displayed on the reader 109.

[0034] As illustrated in FIG. 3, the mobile device 103 contains a processor 301, a communications interface 303, and a non-volatile memory (NVM) 305. The NVM 305 contains programs including an operating system 307 and application programs, referred to as "apps", which includes an eIDWallet app 309.

[0035] The communications interface 303, which may be used for mobile telephony, NFC, Bluetooth, WiFi, etc., allows the mobile device 103 to communicate with the reader 109 or the remote server 115. Alternatively, the mobile device 103 may communicate to the reader 109 via the screen 201 and camera 203 the reader 109 maybe an optical device that reads information transmitted via the screen 201 of the mobile device 103 and outputs information that the mobile device 103 may input via the camera 203.

[0036] The eIDWallet app 309 manages eIDWallet information, e.g., in an eIDWalletDB 311 organized around a number of namespaces 313a-n.

[0037] The architecture of FIG. 3 is merely one example. For example, in an alternative embodiment, there may be multiple eIDWallet apps each with its own namespace.

[0038] Each namespace provides access to a number of data elements and defines its own names for those data elements. An example namespace may be found in

ISO/IEC CD2 18013-5:2019, *Personal Identification — ISO-Compliant Driving Licence — Part 5: Mobile Driving Licence (mDL) application*, section 7 "Data Model", incorporated herein by reference.

[0039] However, while two namespaces may contain the same data elements, these data elements may not have the same name in the two namespaces. For example, *Date of birth* (from the sample namespace in Appendix I) may be named *BirthDate* in another namespace. Similarly, two different data

elements may provide an equivalent piece of information, e.g., *Date of birth* may be used to derive *age*.

[0040] Namespaces may be addressed in different ways, for example, URI, URL, URN, OID, UUID, or reverse domain namespace representation. In reverse domain representation, the namespace may be defined as *reverseDomain.domainSpecificExtension*. For example, for the French National Agency for Secure Documents, the reverse domain namespace identifier may be *fr.gouv.ants.id*, and for a stamp club, *org.asso.philatelie.role*.

[0041] FIG. 4 is a block diagram illustrating one embodiment organization for a reader 109. The reader 109 includes a processor 401, a storage unit 403, an interface unit 405, for example, for interfacing with the processor of the verifier 105, and a communications module 407, for example, for NFC, WiFi, Bluetooth communication with the mobile device 103.

[0042] The storage unit 403 contains software modules including an operating system (OS) 409 and a reader module 411, which contains instructions to the processor 401 to carry out reader-side namespace selection as illustrated and described hereinbelow.

[0043] FIG. 5 is a block diagram illustrating one embodiment organization for a verifier 105. The verifier includes a processor 451, a storage unit 453, an input/output interface unit 405, for example, for interfacing with a user interface device for communicating with a human operator 115 or the user 101, and a communications module 457, for example, for NFC, WiFi, or Bluetooth communication with the mobile device 103. The storage unit 403 contains software modules including an operating system (OS) 459 and a verifier module 111 for carrying out tasks related to verifying an eID attribute assertion, for example, one related to verifying eligibility based on an attribute or identity.

[0044] Note, there are tasks of the reader module 411 as well as the verifier module 111 that may be carried out by a human operator. For example, as discussed in conjunction with the timing sequence diagram of FIG. 6 that follows hereinbelow, selection of a namespace based on level of security may be performed using a dialog with a human identity-based-assertion verifier (see, FIG. 1, 115). Accordingly, the verifier 105 may include an I/O interface 455 for connecting to user interface devices, such as a terminal for displaying graphic user interface elements 117.

[0045] FIG. 6 (which is partitioned onto FIGs. 6a and 6b) is a timing sequence diagram illustrating a process for communicating namespaces available

on a mobile device 103 to a verifier 105 including a reader 109. The process executed by the reader 109 may be under control of a software module referred to herein as the reader module 411. It should be noted that there is no strict demarcation between the reader 109 and verifier 105. Tasks described herein as performed by one may be performed by the other. Furthermore, the reader 109 and verifier 105 may be either completely separated or merged into one unit or any arrangement between those two extremes.

[0046] As a preliminary step a user 101 operating the mobile device 103 seeks to make an identity-based assertion, step 501. The identity-based assertion may be a request to access a service based on a certified attestation of an identity attribute, e.g., age, or to demonstrate that the user 101 is a particular person. The user 101 presents the mobile device 103, which contains and executes an eIDWallet app 309, to the reader 109 and a communications session, e.g., NFC, Bluetooth, WiFi, or optical transmission, is established between the mobile device 103 and the reader 109.

[0047] In response to the establishment of an eID communications session, the reader 109 responds by requesting from the mobile device 103 a listing of eID namespaces supported by the mobile device 103, step 503.

[0048] The mobile device 103 responds with a list of supported eID namespaces, step 505. The list may be a concatenation or structured set of namespace identifiers, for example, in the form of URI, URL, URN, OID, UUID, or reverse domain name representation. In an embodiment, the mobile device 103 requests confirmation by the user 101 that the user acquiesces to releasing particular namespaces to the reader 109 and verifier 105. For example, if one namespace that contains a birthdate is associated with a political organization, the user may prefer to not reveal membership in that organization to the reader 109 and verifier 105.

[0049] Using, for example, reverse domain name representation, for a French-citizen student at the University of Pau, France, who is a stamp collector, the mobile device 103 may return:

National identification: *fr.gouv.ants.id* (the French National Agency for Secure Documents)

Student identification: *fr.edu.univ-pau.labo.profile* (University of Pau)

Membership card in stamp club: *org.asso.philatelie.role* (Stamp collectors club)

[0050] Depending on the request for which the identity assertion (step 501) is made, the verifier 105 determines the level of security (LOS) that should be associated with the request, step 507. For example, a bank cashing a check may require an identity assertion associated with a national ID whereas for proving entitlement to a student fare, a university ID may be sufficient.

[0051] Based on the required LOS, the verifier 105 selects one or more namespaces that satisfy the required LOS, step 509, and sends a request for access to these namespaces to the mobile device 103, step 511. The verifier 105 may have a whitelist of namespaces that may be used to satisfy LOS for an identity-based assertion. For example, a metropolitan transit authority may accept national IDs as well as student IDs from local universities. Conversely, the verifier 105 may have a blacklist of namespaces that are not allowed to be used for an identity-based assertion; i.e., that are deemed to not meet the LOS required.

[0052] The mobile device 103 responds with the security policy access rules associated with each of the requested namespaces, step 513.

[0053] In a preferred embodiment, the security policies of namespaces are communicated according to a standard protocol or an interoperability template. The namespace-security-policy protocol may consist of a sequence of bytes in which each bit signifies a particular security policy attribute.

[0054] FIG. 7 is a table illustrating an example 601 protocol for namespace-security-policy messages.

[0055] In the example 601, the first byte is used to communicate a version number of the template used for communicating namespace security policy.

[0056] The second byte of the example template 601 contains a value for denoting the required authentication protocol. The first bit (b1) indicates whether digital signature is required or not. The second bit (b2) indicates whether reader authentication is required. The third bit (b3) is used to indicate whether certificate verification is required. The fourth bit (b4) is used to indicate whether secure messaging is required. The fifth bit (b5) is used to indicate whether role authentication is required. The sixth bit (b6) indicates whether user consent is required.

[0057] The third byte indicates the HASH type to be used. For example, first through third bit indicate to use SHA-256, SHA-384, and SHA-512, respectively. Other bits could be used to indicate alternative hashing schemes. No bit set indicates that hashing is not to be used.

[0058] The fourth byte indicates the scheme for digital signatures to be used. For example, the first and second bits indicate RSA and ECDSA, respectively. Other bits may indicate to use other digital signature schemes. No bit set indicates that digital signature is not required.

[0059] The fifth byte denotes which secure messaging option to use. The first through third bit indicate AES 128 bit-CMAC, AES 128 bit-EMAC, and AES-GCM, respectively. Other bits may indicate to use other secure messaging options. No bit set indicates that secure messaging is not required.

[0060] It should be noted that the template illustrated in FIG. 7 and described above is merely an example. Other arrangements are possible. For example, several of the bytes that only use a few bits to convey information can be combined.

[0061] Returning to FIG. 6, having received the security policy access rules (step 513), the reader 109 determines if there is at least one namespace with acceptable access rules, step 515. For example, if the mobile device 103 demands verification of a digital signature to access a namespace for verification of age to access a website, that may be considered too onerous by the verifier 105. Furthermore, if the verifier 105 may not have the capability to satisfy a demanding access rule and therefore be forced into requesting access to a namespace with a less demanding access rule. Accordingly, the verifier 105 may have, for example, selection rules such as to not select namespaces that require certificate verification or more than 128-bit encryption.

[0062] If there is no namespace provided by the mobile device 103 with acceptable level of confidence and acceptable access rules, the reader 109 may decline access to the service or benefit requested by the mobile device 103, step 515, and a message declining access to the requested service is transmitted to the mobile device 103, step 515.

[0063] Otherwise, the reader 109 selects a namespace with an acceptable security policy, step 519.

[0064] With the selected namespace, the reader satisfies the access rules required by the mobile device and sends an access request message with the namespace identifier, data element name (used by the namespace to address the required data element), required information or format according to the access rule for the namespace, e.g., certificate, hashed message, step 521.

[0065] In an embodiment, the namespace security policy representation 601 further contains additional information, e.g., a certificate route

or digital information necessary to resolve certain cryptographic references. For example, the security policy access rules can be satisfied by the verifier 105 or reader 109 if the verifier/reader has references to, e.g., the cryptographic keys to use, a route to a Certificate Authority root public key (for certificate verification), or an object identifier (OID) denoting a crypto-suite to be performed by the verifier/reader. To provide this additional information, the namespace security policy template 601 transmitted in step 513 may be appended with a byte sequence providing the required data for the defined security mechanisms to allow access to eID data from the mobile device 103 corresponding to each of the bytes in the template.

[0066] FIG. 8 is a block diagram of namespace security representation 701 containing a template 601' and additional information byte sequences 705a-e.

[0067] The example namespace security representation 701 contains the five bytes 703a-e corresponding to the five-byte template 601'. Each of these has a corresponding additional-information byte sequence 705a-e. Each of these additional byte sequences 705a-e are in length-value format, i.e., the first field 707a-e indicating the number of bytes of the value field 709a-e; a 0 value in the length field 707a-e indicates that there is no additional information sequence corresponding to a particular byte in the template and thus, the value field 709a-e would be an empty sequence.

[0068] There are many different possible syntaxes for the length fields. In a simple case, the length field is simply a fixed number of bytes, e.g., one or two bytes.

[0069] Thus, the security policy access rule communication may be:
 1st byte||2nd byte||3rd byte||4th byte||5th byte||0x00||0x0C||<12 byte
 OID>>||0x00||0x08||<eight byte key>>||0x00

where

- the first five bytes correspond to the security policy access rules as described in conjunction with FIG. 7
- 0x00 indicates a zero-length value field, i.e., no value, corresponding to the first byte 703a
- 0x0C is the length field with the hexadecimal value indicating that 12 bytes is to follow for additional information corresponding to the second byte 703b; in the example, the following 12 bytes is a representation of the OID denoting the

crypto-suite applying the authentication protocol defined in the 2nd byte of the security policy access rules

- The second 0x00 indicates that there is no additional information corresponding to the third byte 703c
- 0x08 indicates that the following value field, corresponding to the fourth byte 703d, is eight bytes long and the following eight bytes, in this example, is an eight-byte cryptographic key
- the third 0x00 indicates that for the fifth byte 703e there is no additional information byte sequence

[0070] Other mechanisms for indicating the length of the additional value field include using an escape sequence, e.g., 0xFF, to indicate that the following byte contains the length of the length field. For example, 0xFF020216 would indicate that the length field (0x02) is two bytes long and those two bytes indicate that the following byte sequence is 0x0216 (534) bytes long. Yet another mechanism is to have the first byte of each additional information sequence 705 indicate the length of the length field.

[0071] As noted above, user consent may be one possible access rule. Thus, if user consent is required, the mobile device 103 may display on the user interface 201 a message to the user indicating the access request, for example, as indicated in FIG. 9, which is a diagram showing a dialog box displayed on a mobile device 103. If the user cancels, the access is denied. Conversely, the access to the requested service also not granted. However, in a follow-up dialog, the user 101 may be provided the opportunity to select another eID namespace for the identity-based assertion required by the reader 109.

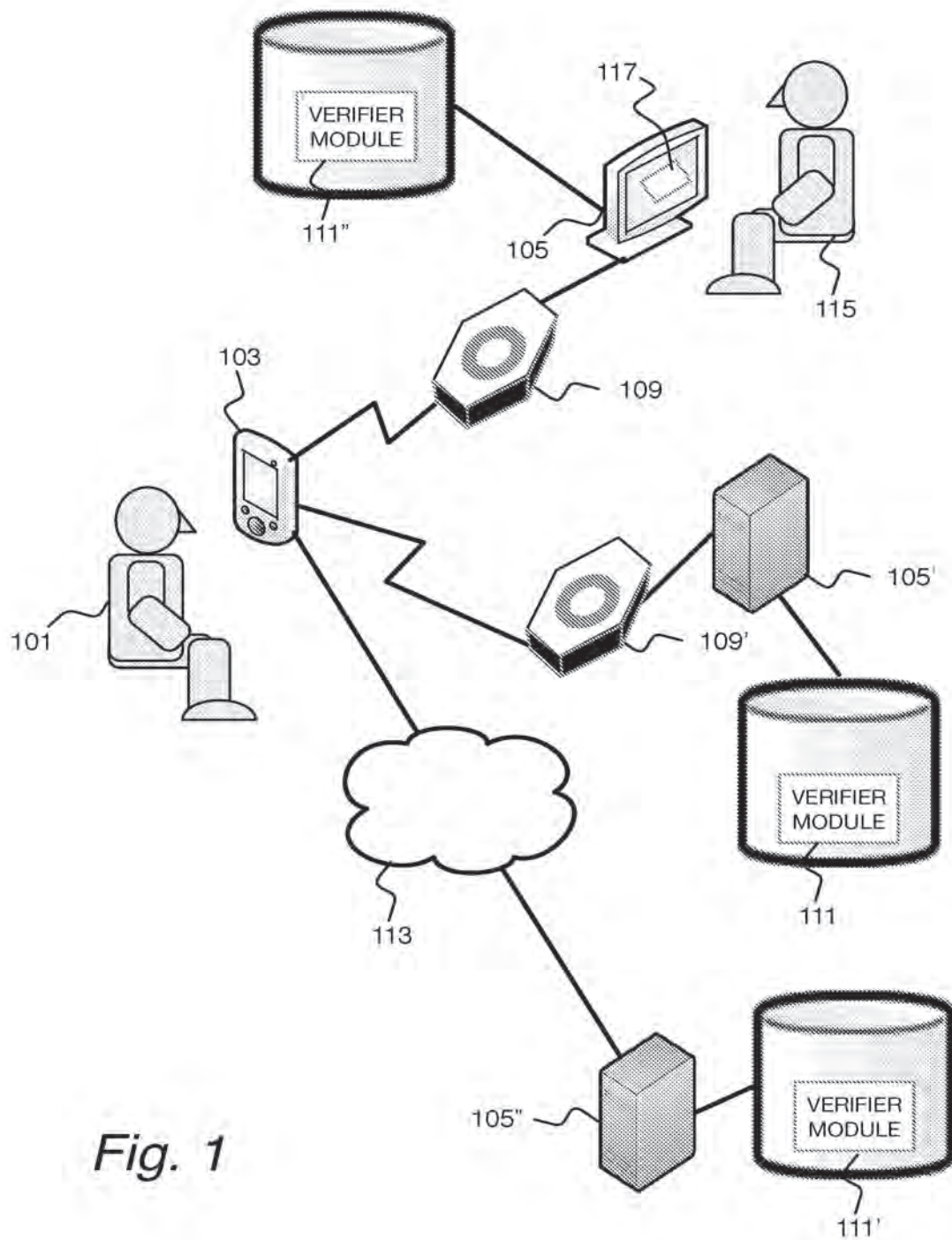
[0072] Returning again to FIG. 6, if the reader 109 has satisfied the requirements of the access rules for the requested namespace, the eWallet app 309 of the mobile device 103 retrieves the required data using the namespace data element name provided, step 523, and provides identity-based assertion to the reader 109, step 525.

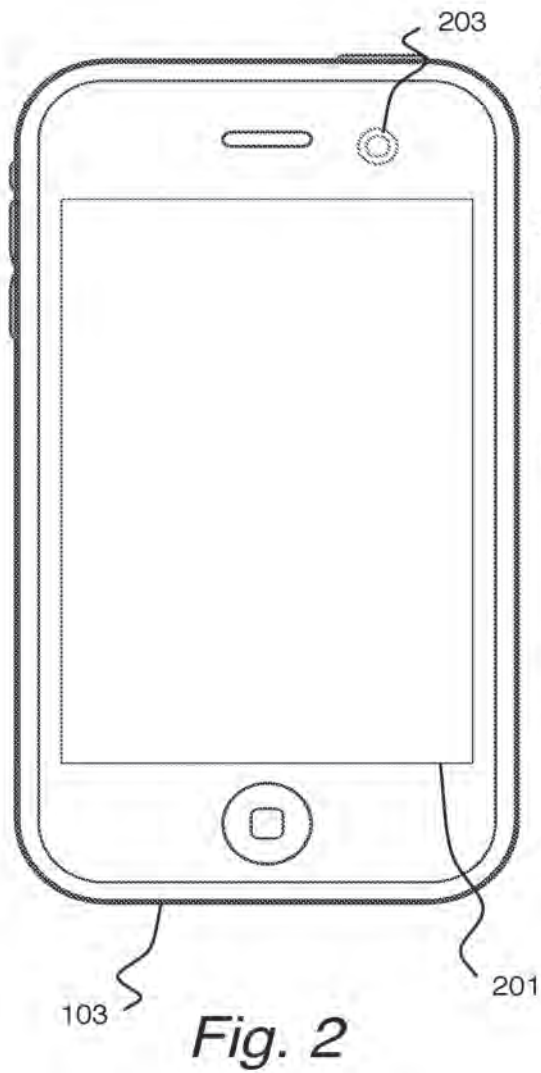
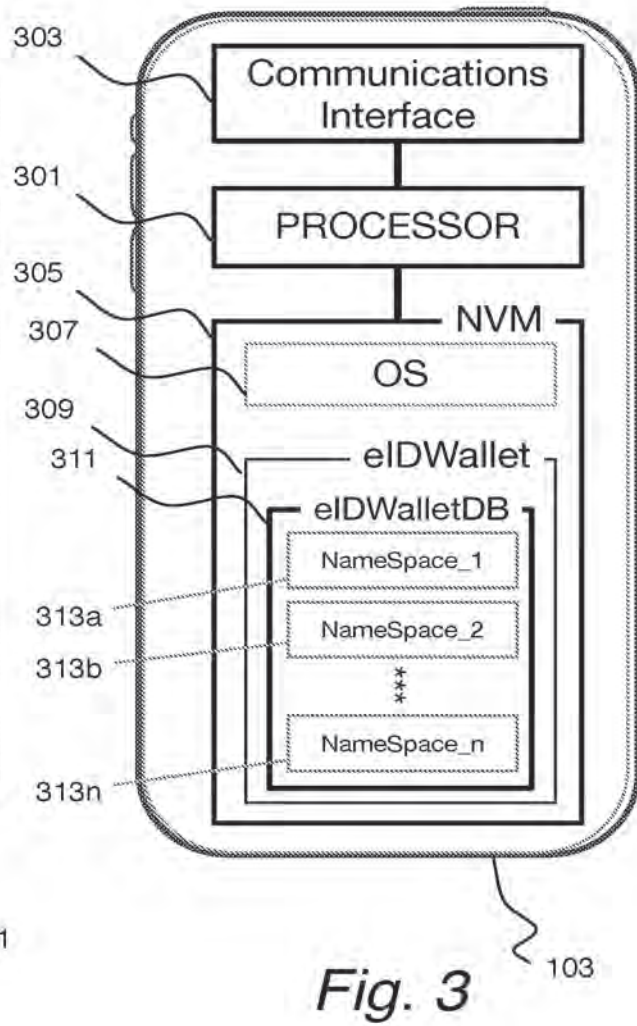
[0073] The reader 109 or verifier 105 then determines whether the identity-based assertion has been proved by the eID namespace, step 527. If the assertion has not been proved, access is denied, step 517. Otherwise, access to the requested service based on the identity-assertion made using the requested eID data element addressed using the selected namespace and data-element name (step 521), the access to the requested service or benefit is provided, step 529.

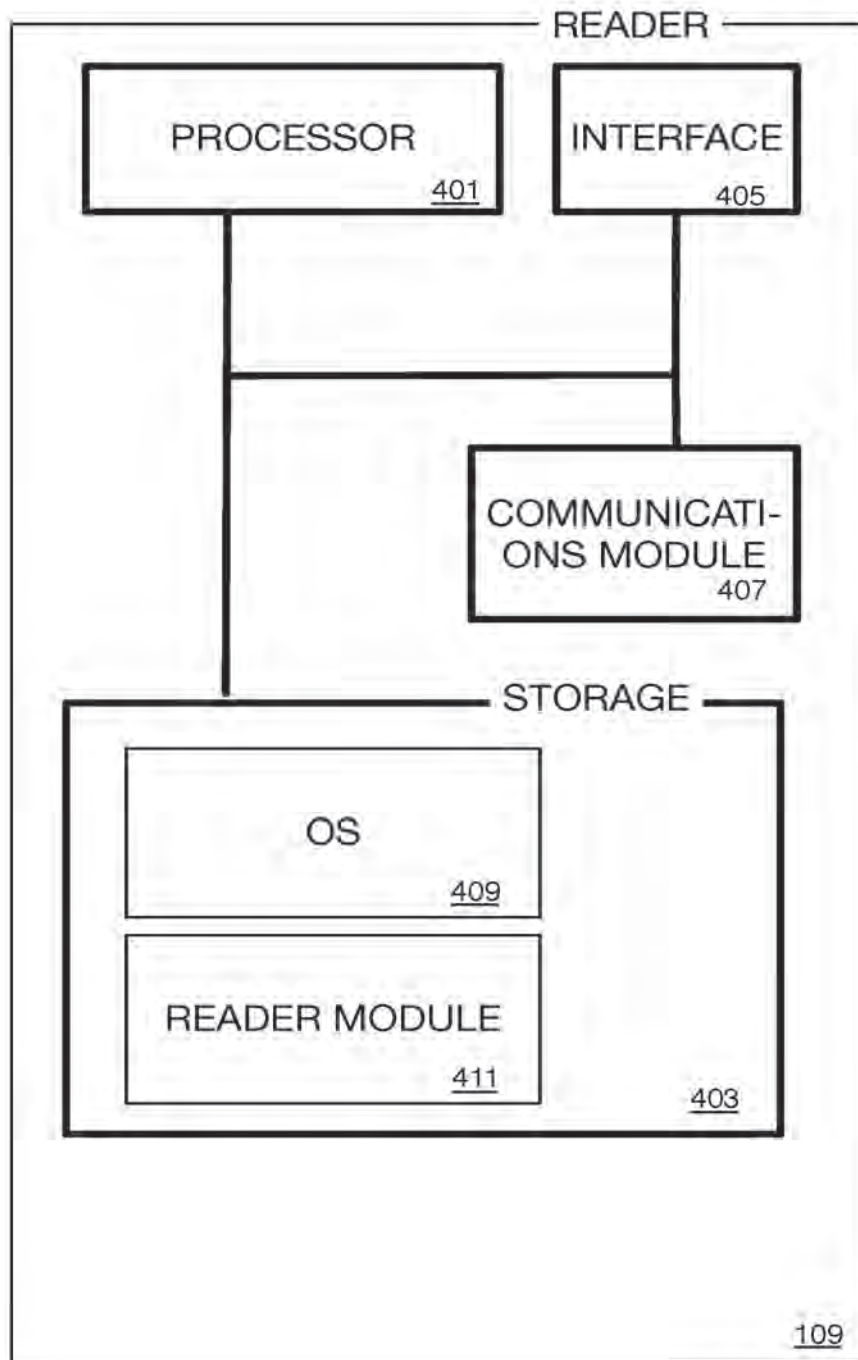
[0074] From the foregoing it will be apparent that an efficient and secure mechanism for associating security policy access rules with namespaces used in eID wallets is provided.

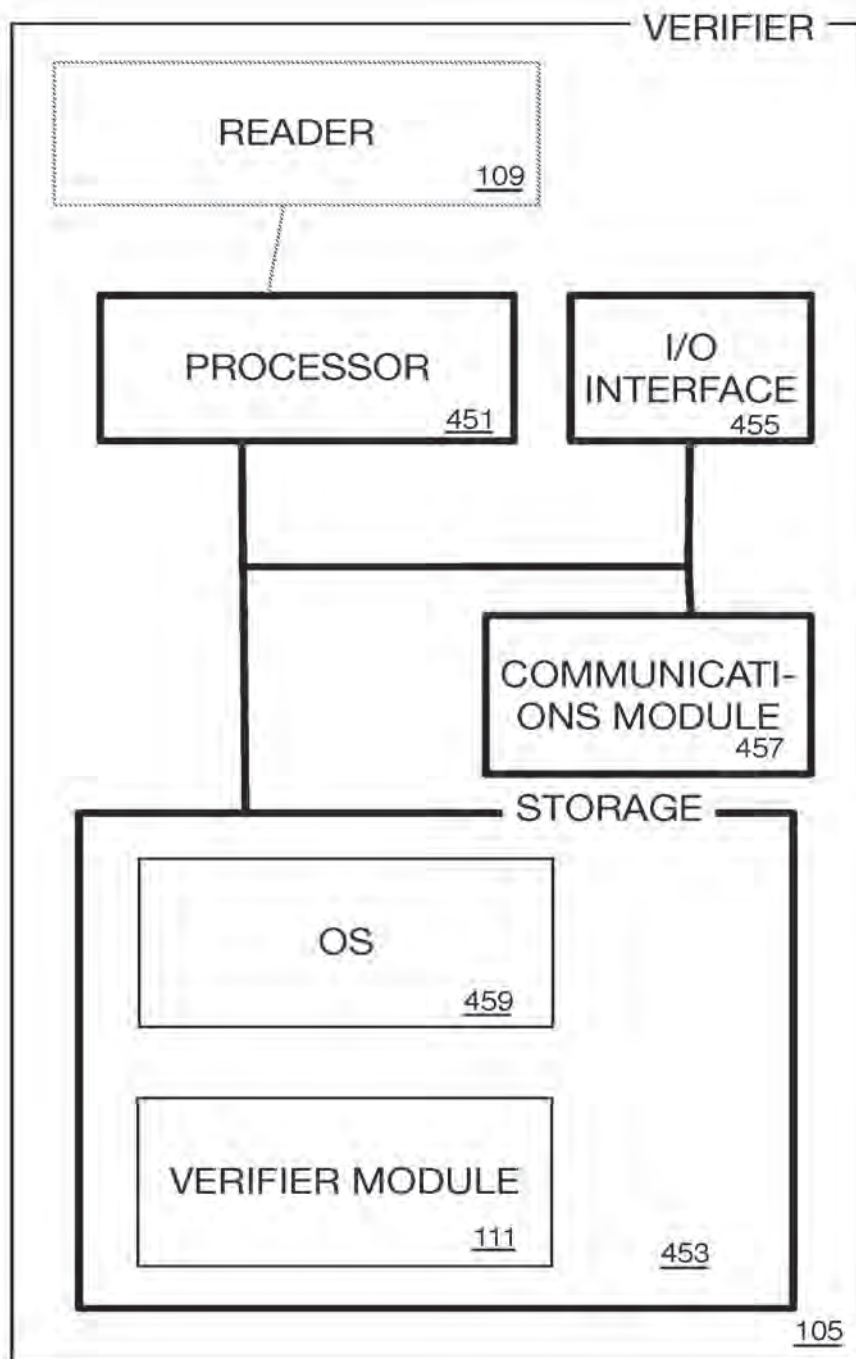
[0075] Although specific embodiments of the invention have been described and illustrated, the invention is not to be limited to the specific forms or arrangements of parts so described and illustrated. The invention is limited only by the claims.

[0076] We Claim:

*Fig. 1*



*Fig. 4*

*Fig. 5*

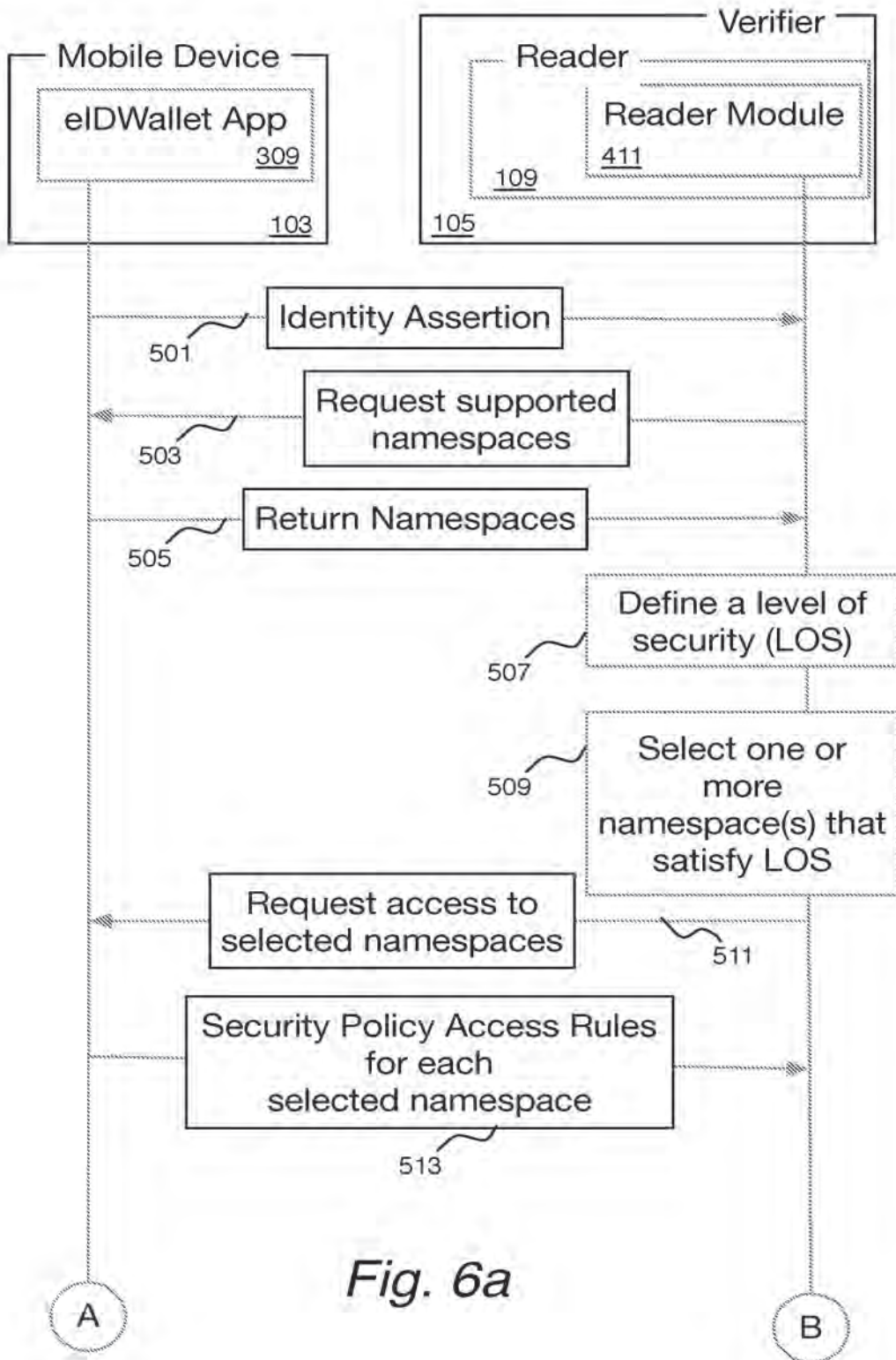
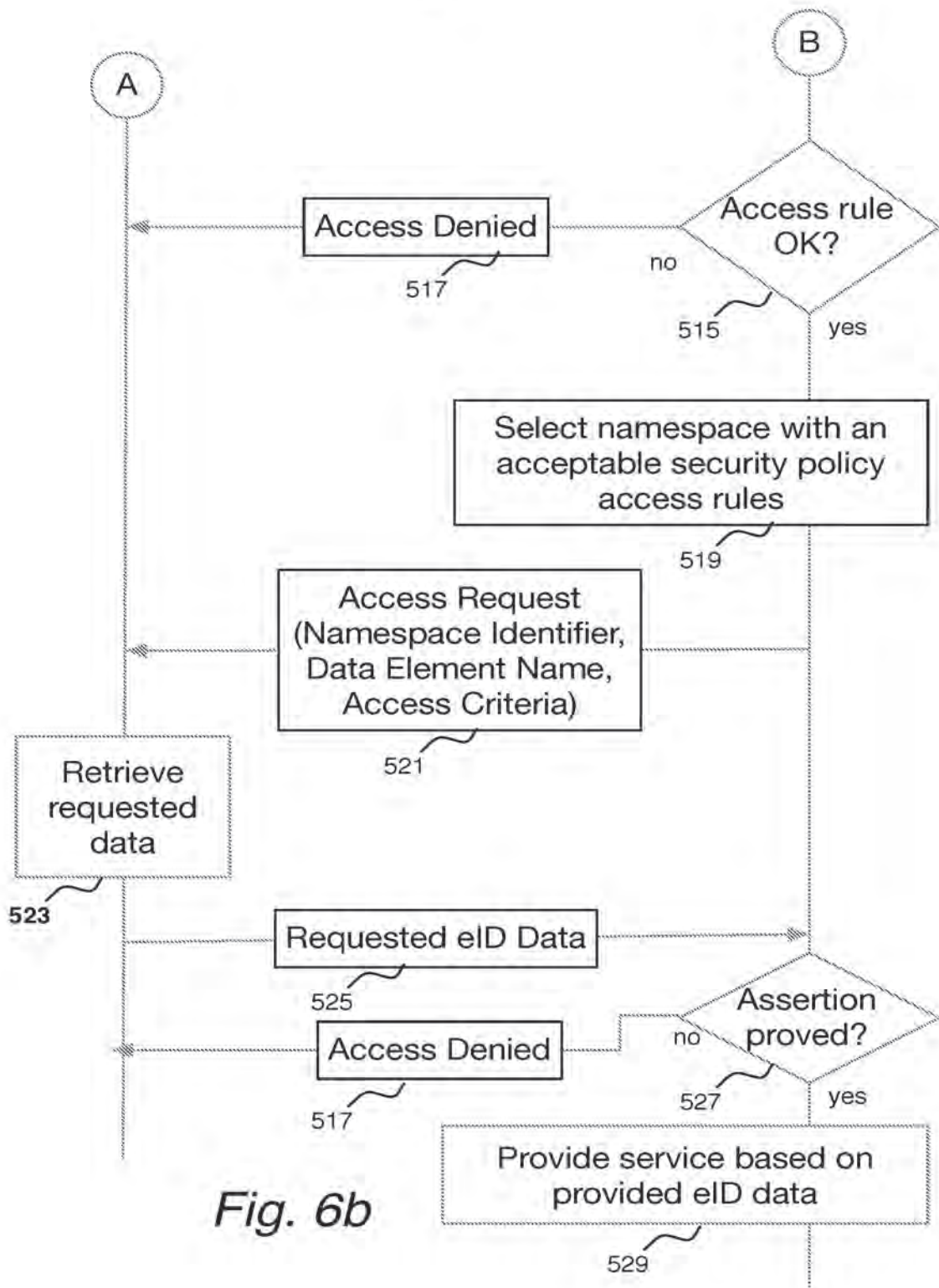


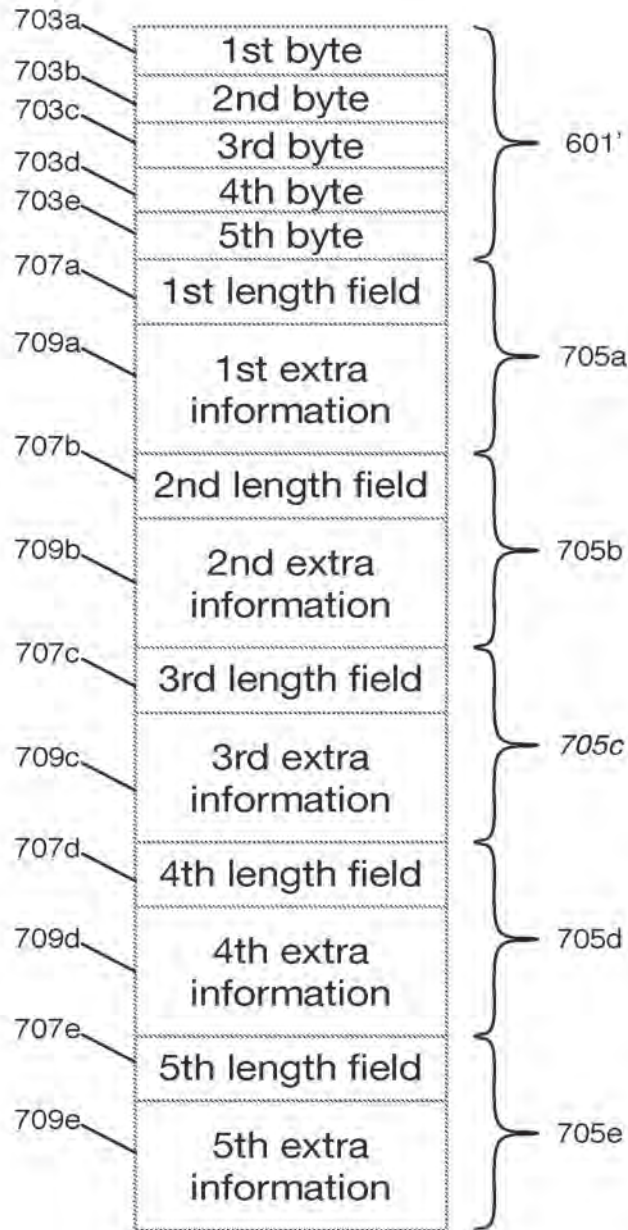
Fig. 6a

*Fig. 6b*

First byte								
b8	b7	b6	b5	b4	b3	b2	b1	
								Value determining the version of this template (for extensibility and interoperability)
Second byte								
b8	b7	b6	b5	b4	b3	b2	b1	value denoting the authentication protocol required
								e.g. digital signature
								e.g. reader authentication
								e.g. certificate verification
								e.g. secure messaging
								e.g. role authentication
								e.g. user consent ...
Third byte								NOTE: could be a coded over a nibble of the first byte if allowed
b8	b7	b6	b5	b4	b3	b2	b1	value denoting the HASH type
								e.g. SHA-256
								e.g. SHA-384
								e.g. SHA-512
								...
Fourth byte								
b8	b7	b6	b5	b4	b3	b2	b1	value denoting the signature scheme
								e.g. RSA
								e.g. ECDSA
								...
Fifth byte								
b8	b7	b6	b5	b4	b3	b2	b1	value denoting secure messaging options
								e.g. AES 128 bits – CMAC
								e.g. AES 128 bites – EMAC
								e.g. AES-GCM ...

601

Fig. 7

*Fig. 8*

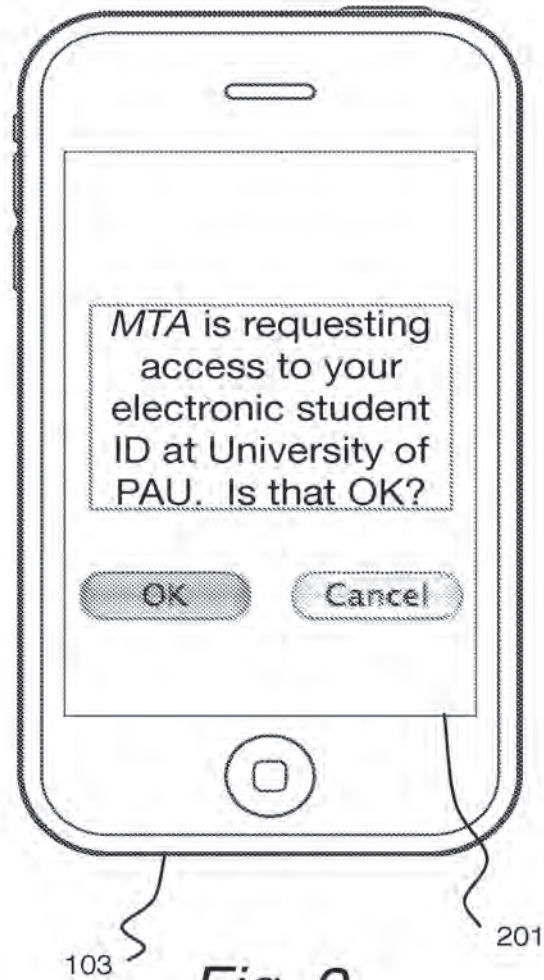


Fig. 9



(51) International Patent Classification:

G06Q 50/26 (2012.01) G06Q 20/36 (2012.01)
G06Q 20/32 (2012.01)

(21) International Application Number:

PCT/EP2020/076906

(22) International Filing Date:

25 September 2020 (25.09.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

19306357.5 18 October 2019 (18.10.2019) EP

(71) Applicant: **THALES DIS FRANCE SA** [FR/FR]; 6, rue de la Verrerie, 92190 MEUDON (FR).

(72) Inventors: **FAHER, Mourad**; THALES DIS FRANCE SA, Intellectual Property Department, 6 Rue de la Verrerie, 92190 MEUDON (FR). **BAYLE, Carole**; THALES DIS FRANCE SA, Intellectual Property Department, 6 Rue de la Verrerie, 92190 MEUDON (FR).

(74) Agent: **LOTAUT, Yacine**; THALES DIS FRANCE SA, Intellectual Property Department, 6 Rue de la Verrerie, 92190 MEUDON (FR).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

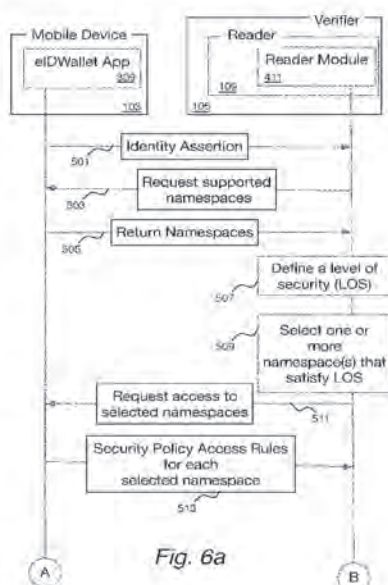


Fig. 6a

(57) Abstract: A system, mobile device, and method for managing security policies for data items stored in an electronic identification (eID) wallet on the mobile device. Security policies are associated with each of a plurality of supported namespaces on a mobile device and a verifier terminal operates to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

BACKGROUND OF THE INVENTION

[0001] The present invention relates, generally, mobile devices operating electronic identification (eID) wallet applications, and, more particularly, to security mechanisms for namespaces used to access data in eID wallet applications.

[0002] Mobile devices such as telephones and tablets provide users with many benefits that have allowed them to eliminate other devices and cards. For example, electronic wallets have allowed users to dispense with carrying many credit cards and enable users to load travel boarding passes and other tickets onto their mobile phones. Another emerging technology, known as electronic identification (eID), provides the ability to use mobile devices to store identification documents such as driver licenses, passports, national ID cards, university ID cards, and club membership cards.

[0003] At least one standard proposal for eID specifies the use of *namespaces* for accessing data stored in mobile Driving License application. ISO/IEC CD2 18013-5:2019, *Personal Identification — ISO-Compliant Driving Licence — Part 5: Mobile Driving Licence (mDL) application*. A namespace is a symbolic mechanism for organizing and identifying pieces of data. To access a piece of data a requestor specifies namespace identifier and a local name (unique within the namespace but not necessarily unique with respect to other namespaces).

[0004] Thus, using namespaces, within an eID wallet one or more eID applications may each have its own namespace that specifies the names of data managed by the eID application.

[0005] While multiple eID applications and associated namespaces managed by a mobile device can satisfy the same identification task, e.g., providing the age of a user, the level of confidence that a verifier associates with these multiple applications and namespaces may not be the same. For example, a government issued eID would typically provide a higher level of confidence than a club associated with a leisure activity.

[0006] Furthermore, eID applications may have security policy requirements before the eWallet allows access to the particular eID application and the information that it manages. Some such security policy requirements, e.g.,

cryptographic signatures of access requests, may be deemed overly cumbersome by certain attribute verifiers or a verifier may not be able to satisfy the requirements.

[0007] To allow a verifier to determine which namespace from which to request access, it is desirable to have a technology which allows uniform communication of namespaces available from a mobile device and namespace security policy access rules associated with such namespaces.

SUMMARY

[0008] A technology for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device provides for associating security policies with each of a plurality of supported namespaces on a mobile device and operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device. In an aspect, technology for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device includes transmitting a list of supported namespaces to the verifier module executing on the verifier and selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.

[0009] In a further aspect, a list of supported namespaces is transmitted to the verifier module and the verifier module selects at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace. In an aspect, prior to transmitting a list of supported namespaces to a verifier terminal via the reader, the mobile device filters out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

[0010] The security policy of each of the plurality of supported namespaces maybe transmitted from the mobile device to the reader, for examples, as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options. The required authentication may be selected from one or more of digital signature, reader

authentication, certificate verification, secure messaging, role authentication, and user consent.

[0011] In an aspect, the reader operates to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier associates with each namespace in the plurality of supported namespaces, for example, by selecting a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

[0012] In an aspect, the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory, the technology further including operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.

To achieve those and other advantages, and in accordance with the purpose of the invention as embodied and broadly described, the invention proposes a method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device, comprises the following steps:

- associating security policies with each of a plurality of supported namespaces on a mobile device; and

- operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device comprises the following steps:

- transmitting a list of supported namespaces to the verifier module executing on the verifier; and

- selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device, comprising the following steps:

- transmitting a list of supported namespaces to the verifier module; and
- selecting, by the verifier module, at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprising the following steps:

- prior to transmitting a list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprising the following step of transmitting the security policy of each of the plurality of supported namespaces from the mobile device to the reader.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device wherein the required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprises operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier associates with each namespace in the plurality of supported namespaces.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device further comprises

operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

In an aspect, the method for managing security policies for data items stored in an electronic identification eID wallet on a mobile device wherein the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory, the method further comprising operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.

Another aspect of the invention is a mobile device comprising:

a processor; and

a memory for storing instructions executable by the processor and for storing electronic identity eID data, the memory including an eID wallet application having instructions to cause the processor to:

receive a list of selected namespaces from a reader;

in response to receiving the list of selected namespaces from the reader, transmitting security rules associated with each selected namespace according to a defined bytestring template.

In an aspect, the eID wallet application further comprises instruction to cause the processor to:

receive a request for supported namespaces from a reader;

transmit a list of supported name spaces to the reader.

In an aspect, the eID wallet application further comprises instruction to cause the processor to:

prior transmitting a list of supported namespaces to a reader, filter out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the reader.

In an aspect, the eID wallet application further comprises instruction to cause the processor to:

transmit the security policy of each of the plurality of supported namespaces to a reader connected to a verifier.

In an aspect, the eID wallet application wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

In an aspect, the present relates to a method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

- associating a security policy with each of a plurality of supported namespaces on a mobile device;

- transmitting the security policy of each of the plurality of supported namespaces to a reader connected to a verifier;

- selecting, by the reader, at least one of the namespaces as candidate namespaces, and transmitting from the reader to the mobile device, a list containing the candidate namespaces;

- transmitting to the reader by the mobile device, the security policy associated with each of the selected candidate namespaces;

- operating the reader to:

- determine for which of the candidate namespaces the reader can satisfy the security policy of the namespace; and

- if the verifier can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the verifier terminal can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the mobile device;

- if the verifier cannot satisfy the security policy of any of the candidate namespaces, rejecting access to the data item; and

- upon successful demonstration by the reader to the mobile device of satisfaction of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1 is a schematic illustrating an exemplary use case scenario.

[0014] FIG. 2 is an external representation of a mobile device.

[0015] FIG. 3 is a block diagram illustrating major components of a hardware and software architecture for a mobile device.

[0016] FIG. 4 is a block diagram illustrating one embodiment organization for a reader.

[0017] FIG. 5 is a block diagram illustrating one embodiment organization for a verifier that contains a reader of FIG. 4.

[0018] FIG. 6 (which is partitioned onto FIGs. 6a and 6b) is a timing sequence diagram illustrating a process for communicating namespaces available on a mobile device to a reader.

[0019] FIG. 7 is a table illustrating an example protocol for namespace-security-policy messages.

[0020] FIG. 8 is a block diagram of a namespace security representation containing a template and additional information byte sequences.

[0021] FIG. 9 is a diagram showing a dialog box displayed on a mobile device to obtain user acquiescence for use of a namespace.

DETAILED DESCRIPTION OF THE INVENTION

[0022] In the following detailed description, reference is made to the accompanying drawings that show, by way of illustration, specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. It is to be understood that the various embodiments of the invention, although different, are not necessarily mutually exclusive. For example, a particular feature, structure, or characteristic described herein in connection with one embodiment may be implemented within other embodiments without departing from the spirit and scope of the invention. In addition, it is to be understood that the location or arrangement of individual elements within each disclosed embodiment may be modified without departing from the spirit and scope of the invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims, appropriately interpreted, along with the full range of equivalents to which the claims are entitled. In the drawings, like numerals refer to the same or similar functionality throughout the several views.

[0023] The following description includes references to various methods executed by a processor of mobile device or a terminal, known herein as the reader or the verifier. As is common in the field, there may be phrases herein that indicate these methods or method steps are performed by software instructions or software modules. As a person skilled in the art knows, such

descriptions should be taken to mean that a processor, in fact, executes the methods, software instructions, and software modules.

[0024] The herein described technology provides mechanisms to provide discoverability of security policies for electronic identification data organized in namespaces on mobile devices with total abstraction of the data structures used on the mobile devices. As such the technology provides an improvement to mobile devices used for electronic identification purposes and the overall system of electronic identification by providing technology by which security access rules may be assigned to namespaces that are used to address electronic identification data stored on mobile devices when mobile devices are used to make identity-based identification or attribute assertions whereby electronic identification readers and verifiers may select appropriate namespaces hosted by electronic devices for verifying electronic identification-based attribute assertions. The technology improves a mobile device by providing such devices the ability to offer more flexibility in assignment of security policies and communication of such security policies to readers and verifiers of electronic identification data.

[0025] First a use case. There are many instances in which an individual seeks to establish an attribute that will allow that individual a certain privilege. That may be an access to a restricted physical space, the right to participate in a program, access to a private or age-restricted material, or access to an attribute-restricted benefit. A reduced fare only available to students and senior citizens is an example of an attribute-restricted benefit.

[0026] Suppose, a person wishing to travel on a metro system is entitled to a 50% discount if the person is either a student or a senior citizen. A person may have on her mobile device several eID applications that may be useful to demonstrate satisfaction of one or both of the requirements for reduced fare, e.g.:

- a government issued identity card, for example, from AGENCE NATIONALE DES TITRES SÉCURISÉS (ants.gouv.fr; French National Agency for Secure Documents) or TEXAS DEPARTMENT OF PUBLIC SAFETY (dps.texas.gov)
- a university departmental ID, for example, University of Pau (univ-pau.fr) or University of Texas (utexas.edu)
- a club for a leisure activity, for example, a stamp collection club (pau-philatelie.asso.org) or a garden club (merryweeders.org)

[0027] Each of the eID applications may store information that can be used to prove that a person is a student or of a certain age; e.g., the government ID typically store birthdates and may have a professional status (e.g., retired or student), the university ID would certainly indicate if a person is a student, faculty or alumnus, and even the stamp club may charge a different membership fee for students and therefore have a flag set for a member being a student, and the garden club may store birthdates so that they can celebrate members on their respective birthdays.

[0028] When the prospective passenger wishes to purchase a monthly pass for the metro, they presents their mobile device to a ticket vendor, which may either be an automatic ticket self-use vending terminal or an individual employee of the metro authority, who would operate a verification terminal. If the passenger is a student or senior, the passenger offers his or her eID wallet to prove that fact. The passenger or the metro official places the mobile device on a terminal.

[0029] The eID wallet communicates the desired attribute to the terminal and the terminal decides whether to grant the discount or not.

[0030] FIG. 1 is a schematic illustrating the above-described use-case example scenario and alternatives. A user 101 operates a mobile device 103, e.g., a mobile telephone. The mobile device 103 contains an eID wallet with one or more eID applications (see FIG. 2). The eID functionality of the mobile device 103 may be used by the user 101 to prove identity or an identity-related attribute to a verifier. The verifier may be a human verifier 115 interacting with reader 109 and a verifier computer 105 via a user interface 117 connected to a reader 109. For example, if the user 101 seeks to obtain access to a facility based on a membership status, the user 101 may present the mobile device 103 to a security guard (human verifier) 115. A verifier module 111^{''}, executable by the reader 109 or the verifier 105, provides the dialog user interface 117 to the human verifier 115 to verify proffered identification from the user 101.

[0031] Alternatively, the verifier may be performed automatically when the user 101 places the mobile device 103 on the reader 109, for example, if the reader 109 is connected to an automated verifier 105', executing a software verifier module 111', in communication with a reader 109'. While depicted here as separate units, the reader 109' and the verifier 105' may be one machine. An example may be a ticket vending machine in which a traveler has to demonstrate being a member of a particular age group.

[0032] In an alternative use case, the mobile device 103 is used to provide identity functionality over the internet 113 to a remote server 115 on which a verifier module 111 is executing.

[0033] FIG. 2 is an external representation of a mobile device 103 and FIG. 3 is a block diagram illustrating major components of a hardware and software architecture for a mobile device 103. The mobile device 103 contains a touch screen user interface 201 for receiving input from the user 101 and for providing output to the user 101 as well as a camera 203 by which the mobile device may receive input from a reader 109, e.g., by scanning QR codes or bar codes displayed on the reader 109.

[0034] As illustrated in FIG. 3, the mobile device 103 contains a processor 301, a communications interface 303, and a non-volatile memory (NVM) 305. The NVM 305 contains programs including an operating system 307 and application programs, referred to as "apps", which includes an eIDWallet app 309.

[0035] The communications interface 303, which may be used for mobile telephony, NFC, Bluetooth, WiFi, etc., allows the mobile device 103 to communicate with the reader 109 or the remote server 115. Alternatively, the mobile device 103 may communicate to the reader 109 via the screen 201 and camera 203 the reader 109 maybe an optical device that reads information transmitted via the screen 201 of the mobile device 103 and outputs information that the mobile device 103 may input via the camera 203.

[0036] The eIDWallet app 309 manages eIDWallet information, e.g., in an eIDWalletDB 311 organized around a number of namespaces 313a-n.

[0037] The architecture of FIG. 3 is merely one example. For example, in an alternative embodiment, there may be multiple eIDWallet apps each with its own namespace.

[0038] Each namespace provides access to a number of data elements and defines its own names for those data elements. An example namespace may be found in

ISO/IEC CD2 18013-5:2019, *Personal Identification — ISO-Compliant Driving Licence — Part 5: Mobile Driving Licence (mDL) application*, section 7 "Data Model", incorporated herein by reference.

[0039] However, while two namespaces may contain the same data elements, these data elements may not have the same name in the two namespaces. For example, *Date of birth* (from the sample namespace in Appendix I) may be named *BirthDate* in another namespace. Similarly, two different data

elements may provide an equivalent piece of information, e.g., *Date of birth* may be used to derive *age*.

[0040] Namespaces may be addressed in different ways, for example, URI, URL, URN, OID, UUID, or reverse domain namespace representation. In reverse domain representation, the namespace may be defined as *reverseDomain.domainSpecificExtension*. For example, for the French National Agency for Secure Documents, the reverse domain namespace identifier may be *fr.gouv.ants.id*, and for a stamp club, *org.asso.philatelie.role*.

[0041] FIG. 4 is a block diagram illustrating one embodiment organization for a reader 109. The reader 109 includes a processor 401, a storage unit 403, an interface unit 405, for example, for interfacing with the processor of the verifier 105, and a communications module 407, for example, for NFC, WiFi, Bluetooth communication with the mobile device 103.

[0042] The storage unit 403 contains software modules including an operating system (OS) 409 and a reader module 411, which contains instructions to the processor 401 to carry out reader-side namespace selection as illustrated and described hereinbelow.

[0043] FIG. 5 is a block diagram illustrating one embodiment organization for a verifier 105. The verifier includes a processor 451, a storage unit 453, an input/output interface unit 405, for example, for interfacing with a user interface device for communicating with a human operator 115 or the user 101, and a communications module 457, for example, for NFC, WiFi, or Bluetooth communication with the mobile device 103. The storage unit 403 contains software modules including an operating system (OS) 459 and a verifier module 111 for carrying out tasks related to verifying an eID attribute assertion, for example, one related to verifying eligibility based on an attribute or identity.

[0044] Note, there are tasks of the reader module 411 as well as the verifier module 111 that may be carried out by a human operator. For example, as discussed in conjunction with the timing sequence diagram of FIG. 6 that follows hereinbelow, selection of a namespace based on level of security may be performed using a dialog with a human identity-based-assertion verifier (see, FIG. 1, 115). Accordingly, the verifier 105 may include an I/O interface 455 for connecting to user interface devices, such as a terminal for displaying graphic user interface elements 117.

[0045] FIG. 6 (which is partitioned onto FIGs. 6a and 6b) is a timing sequence diagram illustrating a process for communicating namespaces available

on a mobile device 103 to a verifier 105 including a reader 109. The process executed by the reader 109 may be under control of a software module referred to herein as the reader module 411. It should be noted that there is no strict demarcation between the reader 109 and verifier 105. Tasks described herein as performed by one may be performed by the other. Furthermore, the reader 109 and verifier 105 may be either completely separated or merged into one unit or any arrangement between those two extremes.

[0046] As a preliminary step a user 101 operating the mobile device 103 seeks to make an identity-based assertion, step 501. The identity-based assertion may be a request to access a service based on a certified attestation of an identity attribute, e.g., age, or to demonstrate that the user 101 is a particular person. The user 101 presents the mobile device 103, which contains and executes an eIDWallet app 309, to the reader 109 and a communications session, e.g., NFC, Bluetooth, WiFi, or optical transmission, is established between the mobile device 103 and the reader 109.

[0047] In response to the establishment of an eID communications session, the reader 109 responds by requesting from the mobile device 103 a listing of eID namespaces supported by the mobile device 103, step 503.

[0048] The mobile device 103 responds with a list of supported eID namespaces, step 505. The list may be a concatenation or structured set of namespace identifiers, for example, in the form of URI, URL, URN, OID, UUID, or reverse domain name representation. In an embodiment, the mobile device 103 requests confirmation by the user 101 that the user acquiesces to releasing particular namespaces to the reader 109 and verifier 105. For example, if one namespace that contains a birthdate is associated with a political organization, the user may prefer to not reveal membership in that organization to the reader 109 and verifier 105.

[0049] Using, for example, reverse domain name representation, for a French-citizen student at the University of Pau, France, who is a stamp collector, the mobile device 103 may return:

National identification: *fr.gouv.ants.id* (the French National Agency for Secure Documents)

Student identification: *fr.edu.univ-pau.labo.profile* (University of Pau)

Membership card in stamp club: *org.asso.philatelie.role* (Stamp collectors club)

[0050] Depending on the request for which the identity assertion (step 501) is made, the verifier 105 determines the level of security (LOS) that should be associated with the request, step 507. For example, a bank cashing a check may require an identity assertion associated with a national ID whereas for proving entitlement to a student fare, a university ID may be sufficient.

[0051] Based on the required LOS, the verifier 105 selects one or more namespaces that satisfy the required LOS, step 509, and sends a request for access to these namespaces to the mobile device 103, step 511. The verifier 105 may have a whitelist of namespaces that may be used to satisfy LOS for an identity-based assertion. For example, a metropolitan transit authority may accept national IDs as well as student IDs from local universities. Conversely, the verifier 105 may have a blacklist of namespaces that are not allowed to be used for an identity-based assertion; i.e., that are deemed to not meet the LOS required.

[0052] The mobile device 103 responds with the security policy access rules associated with each of the requested namespaces, step 513.

[0053] In a preferred embodiment, the security policies of namespaces are communicated according to a standard protocol or an interoperability template. The namespace-security-policy protocol may consist of a sequence of bytes in which each bit signifies a particular security policy attribute.

[0054] FIG. 7 is a table illustrating an example 601 protocol for namespace-security-policy messages.

[0055] In the example 601, the first byte is used to communicate a version number of the template used for communicating namespace security policy.

[0056] The second byte of the example template 601 contains a value for denoting the required authentication protocol. The first bit (b1) indicates whether digital signature is required or not. The second bit (b2) indicates whether reader authentication is required. The third bit (b3) is used to indicate whether certificate verification is required. The fourth bit (b4) is used to indicate whether secure messaging is required. The fifth bit (b5) is used to indicate whether role authentication is required. The sixth bit (b6) indicates whether user consent is required.

[0057] The third byte indicates the HASH type to be used. For example, first through third bit indicate to use SHA-256, SHA-384, and SHA-512, respectively. Other bits could be used to indicate alternative hashing schemes. No bit set indicates that hashing is not to be used.

[0058] The fourth byte indicates the scheme for digital signatures to be used. For example, the first and second bits indicate RSA and ECDSA, respectively. Other bits may indicate to use other digital signature schemes. No bit set indicates that digital signature is not required.

[0059] The fifth byte denotes which secure messaging option to use. The first through third bit indicate AES 128 bit-CMAC, AES 128 bit-EMAC, and AES-GCM, respectively. Other bits may indicate to use other secure messaging options. No bit set indicates that secure messaging is not required.

[0060] It should be noted that the template illustrated in FIG. 7 and described above is merely an example. Other arrangements are possible. For example, several of the bytes that only use a few bits to convey information can be combined.

[0061] Returning to FIG. 6, having received the security policy access rules (step 513), the reader 109 determines if there is at least one namespace with acceptable access rules, step 515. For example, if the mobile device 103 demands verification of a digital signature to access a namespace for verification of age to access a website, that may be considered too onerous by the verifier 105. Furthermore, if the verifier 105 may not have the capability to satisfy a demanding access rule and therefore be forced into requesting access to a namespace with a less demanding access rule. Accordingly, the verifier 105 may have, for example, selection rules such as to not select namespaces that require certificate verification or more than 128-bit encryption.

[0062] If there is no namespace provided by the mobile device 103 with acceptable level of confidence and acceptable access rules, the reader 109 may decline access to the service or benefit requested by the mobile device 103, step 515, and a message declining access to the requested service is transmitted to the mobile device 103, step 515.

[0063] Otherwise, the reader 109 selects a namespace with an acceptable security policy, step 519.

[0064] With the selected namespace, the reader satisfies the access rules required by the mobile device and sends an access request message with the namespace identifier, data element name (used by the namespace to address the required data element), required information or format according to the access rule for the namespace, e.g., certificate, hashed message, step 521.

[0065] In an embodiment, the namespace security policy representation 601 further contains additional information, e.g., a certificate route

or digital information necessary to resolve certain cryptographic references. For example, the security policy access rules can be satisfied by the verifier 105 or reader 109 if the verifier/reader has references to, e.g., the cryptographic keys to use, a route to a Certificate Authority root public key (for certificate verification), or an object identifier (OID) denoting a crypto-suite to be performed by the verifier/reader. To provide this additional information, the namespace security policy template 601 transmitted in step 513 may be appended with a byte sequence providing the required data for the defined security mechanisms to allow access to eID data from the mobile device 103 corresponding to each of the bytes in the template.

[0066] FIG. 8 is a block diagram of namespace security representation 701 containing a template 601' and additional information byte sequences 705a-e.

[0067] The example namespace security representation 701 contains the five bytes 703a-e corresponding to the five-byte template 601'. Each of these has a corresponding additional-information byte sequence 705a-e. Each of these additional byte sequences 705a-e are in length-value format, i.e., the first field 707a-e indicating the number of bytes of the value field 709a-e; a 0 value in the length field 707a-e indicates that there is no additional information sequence corresponding to a particular byte in the template and thus, the value field 709a-e would be an empty sequence.

[0068] There are many different possible syntaxes for the length fields. In a simple case, the length field is simply a fixed number of bytes, e.g., one or two bytes.

[0069] Thus, the security policy access rule communication may be:
 1st byte||2nd byte||3rd byte||4th byte||5th byte||0x00||0x0C||<12 byte
 OID>>||0x00||0x08||<eight byte key>>||0x00

where

- the first five bytes correspond to the security policy access rules as described in conjunction with FIG. 7
- 0x00 indicates a zero-length value field, i.e., no value, corresponding to the first byte 703a
- 0x0C is the length field with the hexadecimal value indicating that 12 bytes is to follow for additional information corresponding to the second byte 703b; in the example, the following 12 bytes is a representation of the OID denoting the

crypto-suite applying the authentication protocol defined in the 2nd byte of the security policy access rules

- The second 0x00 indicates that there is no additional information corresponding to the third byte 703c
- 0x08 indicates that the following value field, corresponding to the fourth byte 703d, is eight bytes long and the following eight bytes, in this example, is an eight-byte cryptographic key
- the third 0x00 indicates that for the fifth byte 703e there is no additional information byte sequence

[0070] Other mechanisms for indicating the length of the additional value field include using an escape sequence, e.g., 0xFF, to indicate that the following byte contains the length of the length field. For example, 0xFF020216 would indicate that the length field (0x02) is two bytes long and those two bytes indicate that the following byte sequence is 0x0216 (534) bytes long. Yet another mechanism is to have the first byte of each additional information sequence 705 indicate the length of the length field.

[0071] As noted above, user consent may be one possible access rule. Thus, if user consent is required, the mobile device 103 may display on the user interface 201 a message to the user indicating the access request, for example, as indicated in FIG. 9, which is a diagram showing a dialog box displayed on a mobile device 103. If the user cancels, the access is denied. Conversely, the access to the requested service also not granted. However, in a follow-up dialog, the user 101 may be provided the opportunity to select another eID namespace for the identity-based assertion required by the reader 109.

[0072] Returning again to FIG. 6, if the reader 109 has satisfied the requirements of the access rules for the requested namespace, the eWallet app 309 of the mobile device 103 retrieves the required data using the namespace data element name provided, step 523, and provides identity-based assertion to the reader 109, step 525.

[0073] The reader 109 or verifier 105 then determines whether the identity-based assertion has been proved by the eID namespace, step 527. If the assertion has not been proved, access is denied, step 517. Otherwise, access to the requested service based on the identity-assertion made using the requested eID data element addressed using the selected namespace and data-element name (step 521), the access to the requested service or benefit is provided, step 529.

[0074] From the foregoing it will be apparent that an efficient and secure mechanism for associating security policy access rules with namespaces used in eID wallets is provided.

[0075] Although specific embodiments of the invention have been described and illustrated, the invention is not to be limited to the specific forms or arrangements of parts so described and illustrated. The invention is limited only by the claims.

[0076] We Claim:

CLAIMS

1. A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

associating security policies with each of a plurality of supported namespaces on a mobile device; and

operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.

2. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device of Claim 1, comprising:

transmitting a list of supported namespaces to the verifier module executing on the verifier; and

selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.

3. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims, comprising:

transmitting a list of supported namespaces to the verifier module; and

selecting, by the verifier module, at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

4. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims further comprising:

prior to transmitting a list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

5. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims, comprising:

transmitting the security policy of each of the plurality of supported namespaces from the mobile device to the reader.

6. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

7. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims wherein the required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

8. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims further comprises operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier associates with each namespace in the plurality of supported namespaces.

9. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims further comprises operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

10. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims wherein the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory, the method further comprising operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.

11. A mobile device comprising:
a processor; and
a memory for storing instructions executable by the processor and for storing electronic identity (eID) data, the memory including an eID wallet application having instructions to cause the processor to:
receive a list of selected namespaces from a reader;
in response to receiving the list of selected namespaces from the reader, transmitting security rules associated with each selected namespace according to a defined bytestring template.

12. The mobile device of claim 10, wherein the eID wallet application further comprises instruction to cause the processor to:
receive a request for supported namespaces from a reader;
transmit a list of supported name spaces to the reader.

13. The mobile device according to claims 11 to 12, wherein the eID wallet application further comprises instruction to cause the processor to:
prior transmitting a list of supported namespaces to a reader, filter out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the reader.

14. The mobile device according to claims 11 to 13, wherein the eID wallet application further comprises instruction to cause the processor to:
transmit the security policy of each of the plurality of supported namespaces to a reader connected to a verifier.

15. The mobile device according to claims 11 to 12, wherein the eID wallet application wherein the security policy is transmitted as a sequence of bytes

having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

16. A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

- associating a security policy with each of a plurality of supported namespaces on a mobile device;

- transmitting the security policy of each of the plurality of supported namespaces to a reader connected to a verifier;

- selecting, by the reader, at least one of the namespaces as candidate namespaces, and transmitting from the reader to the mobile device, a list containing the candidate namespaces;

- transmitting to the reader by the mobile device, the security policy associated with each of the selected candidate namespaces;

- operating the reader to:

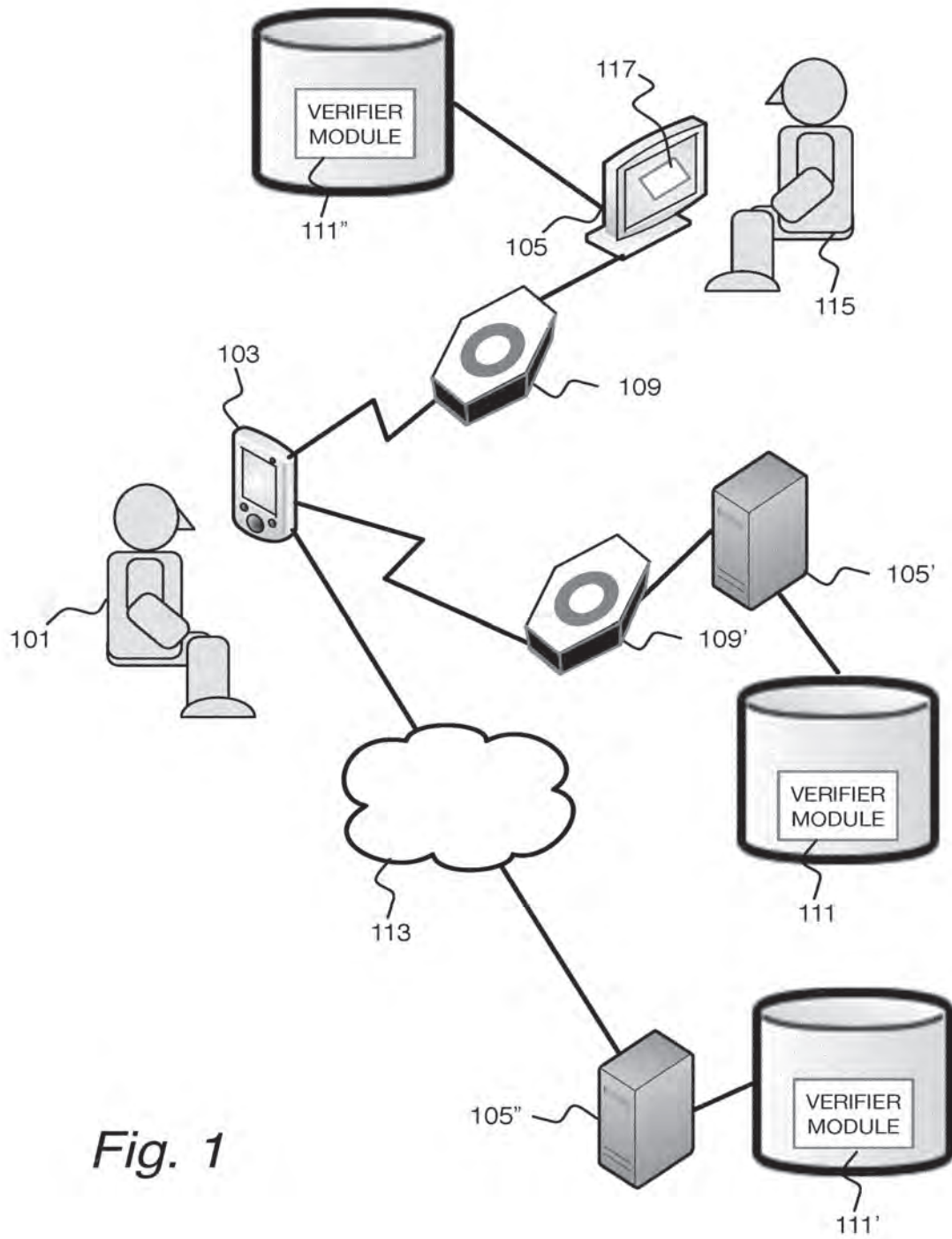
- determine for which of the candidate namespaces the reader can satisfy the security policy of the namespace; and

- if the verifier can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the verifier terminal can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the mobile device;

- if the verifier cannot satisfy the security policy of any of the candidate namespaces, rejecting access to the data item; and

- upon successful demonstration by the reader to the mobile device of satisfaction of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

1/9



2/9

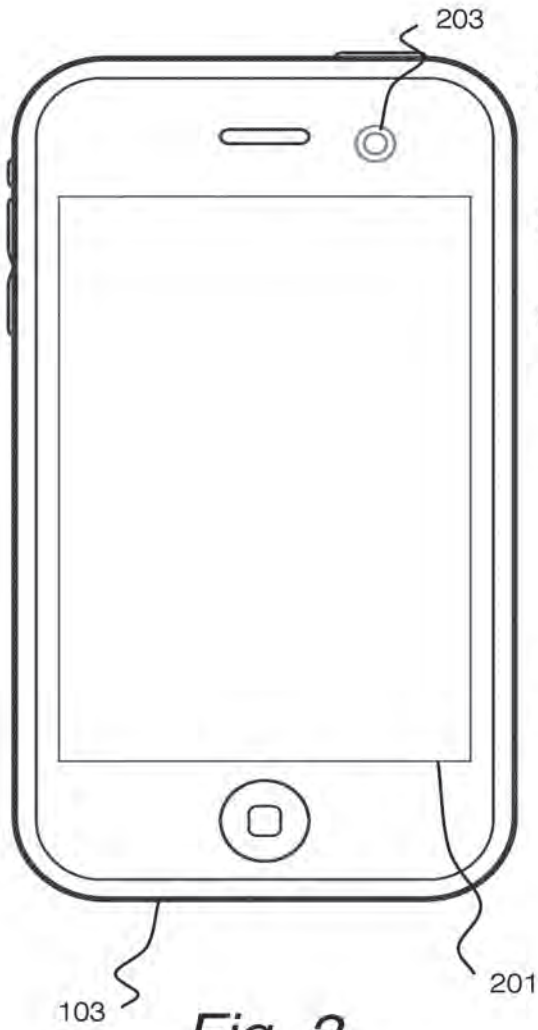


Fig. 2

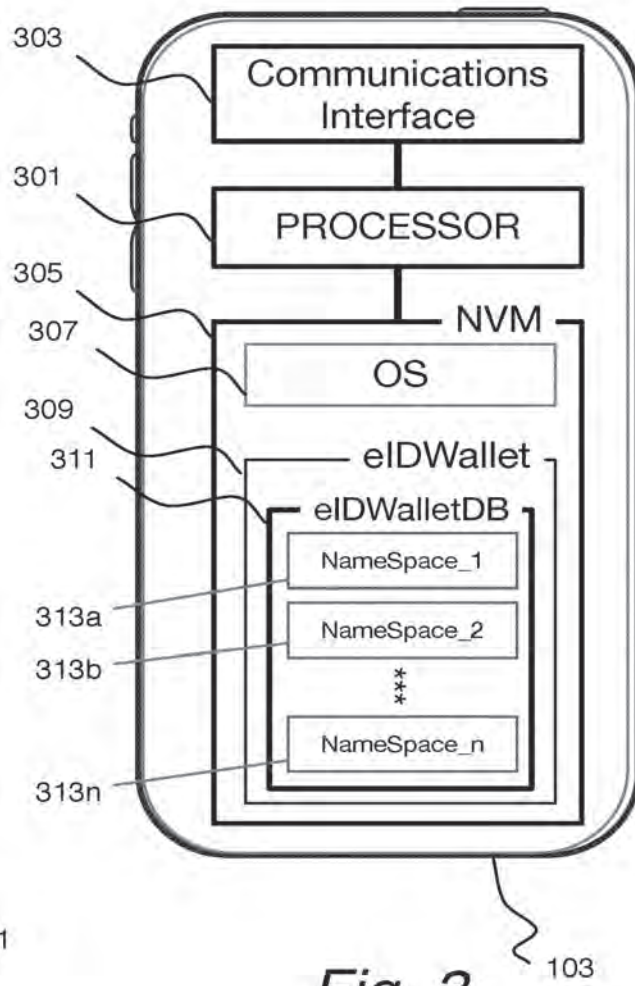
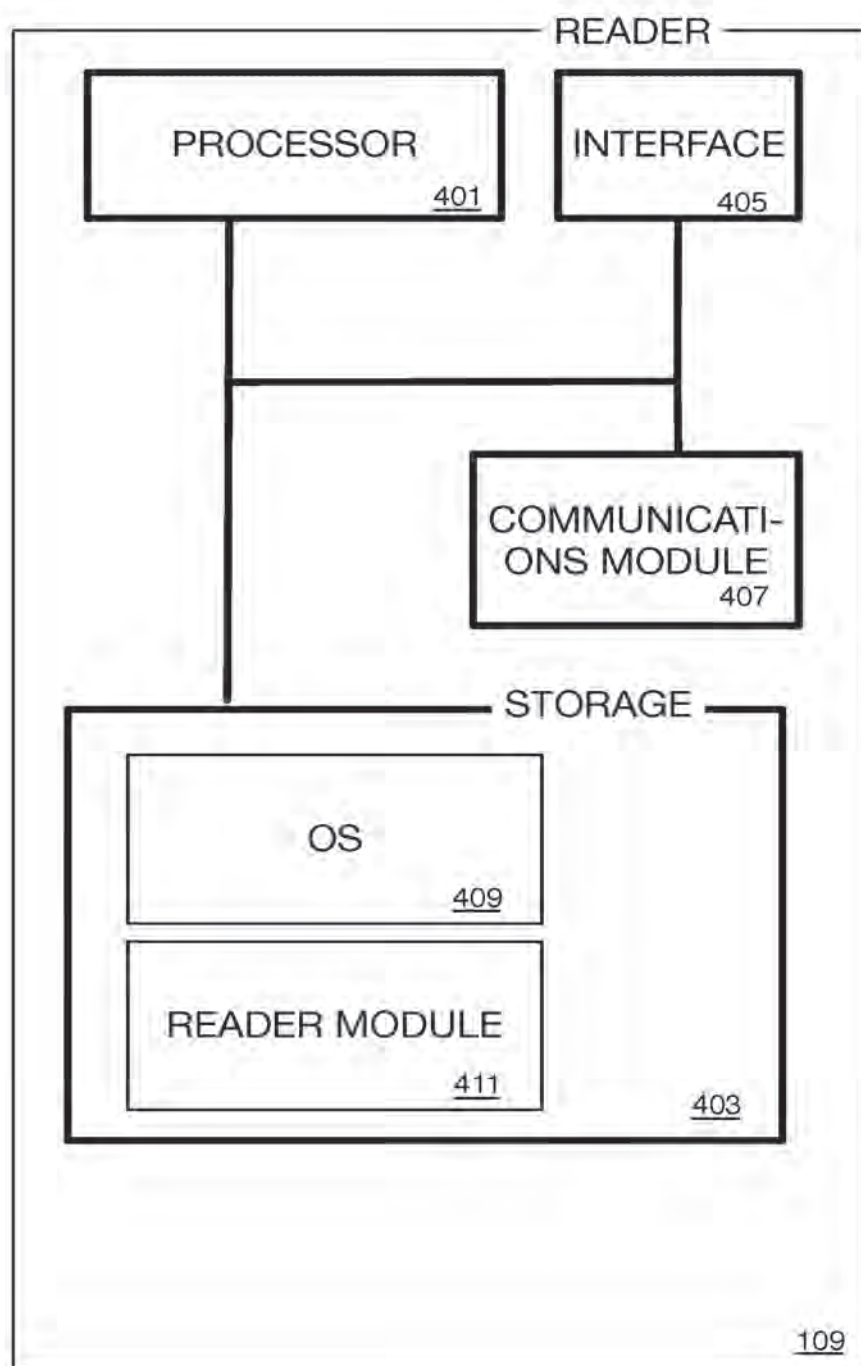
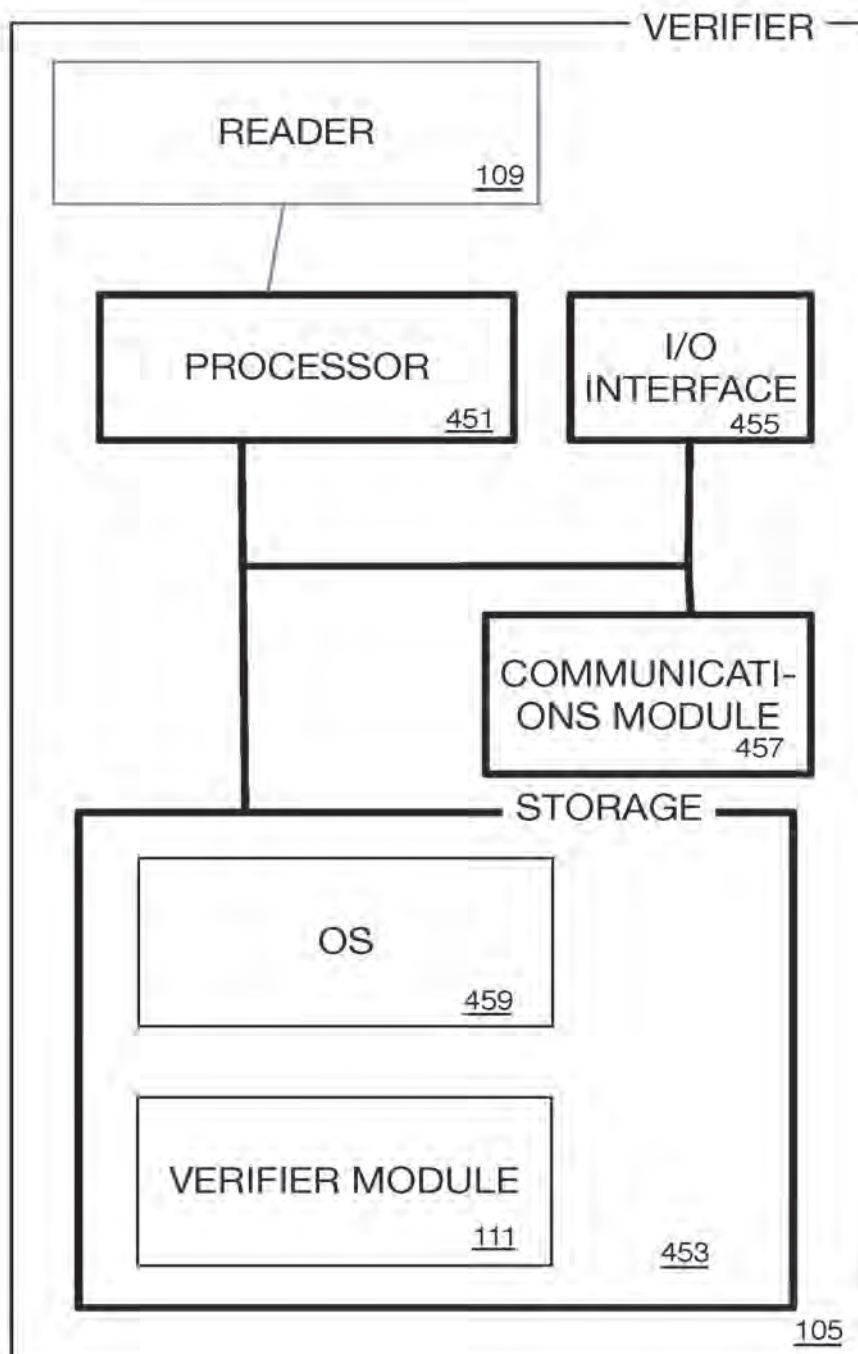


Fig. 3

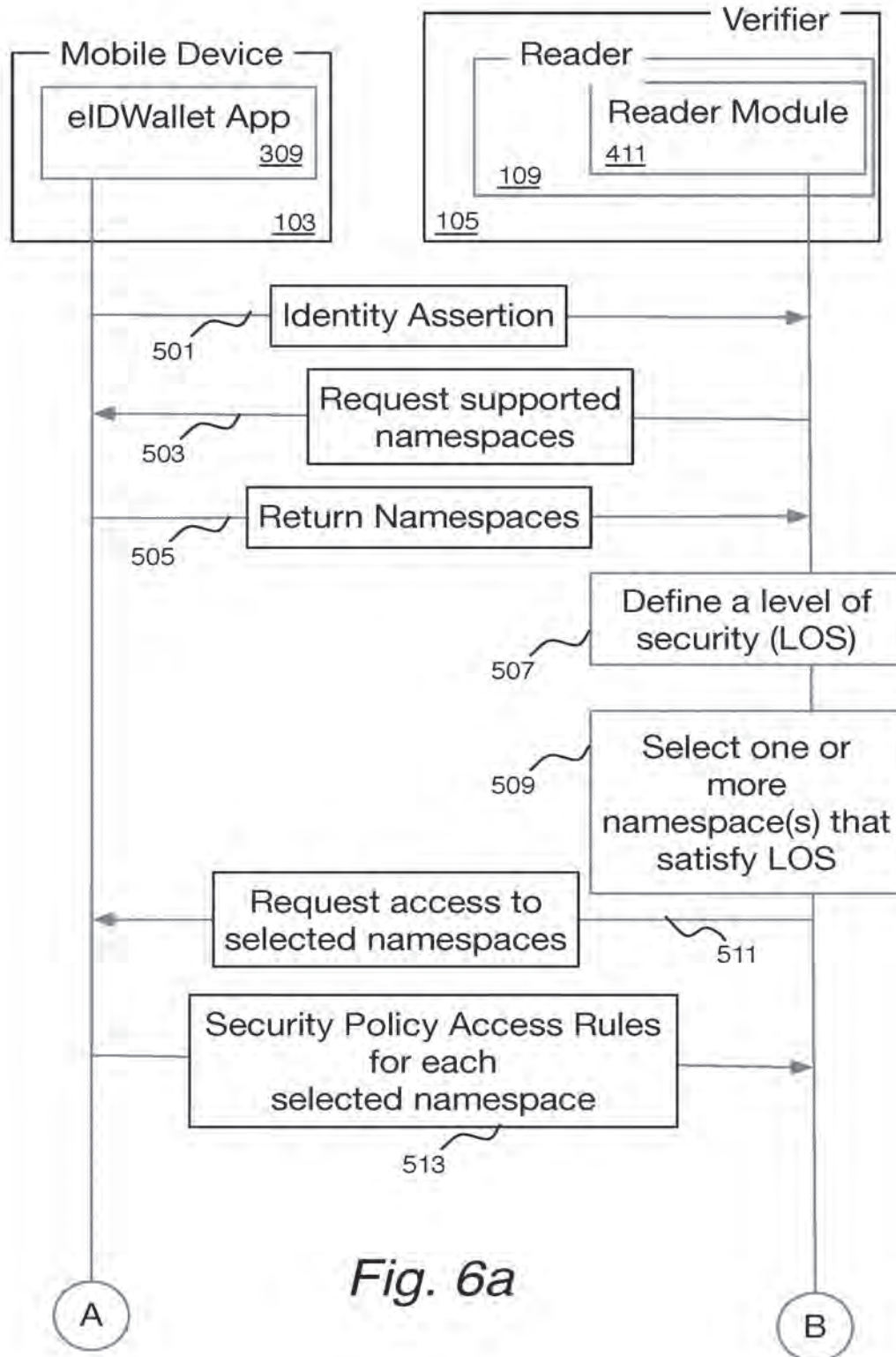
3/9

*Fig. 4*

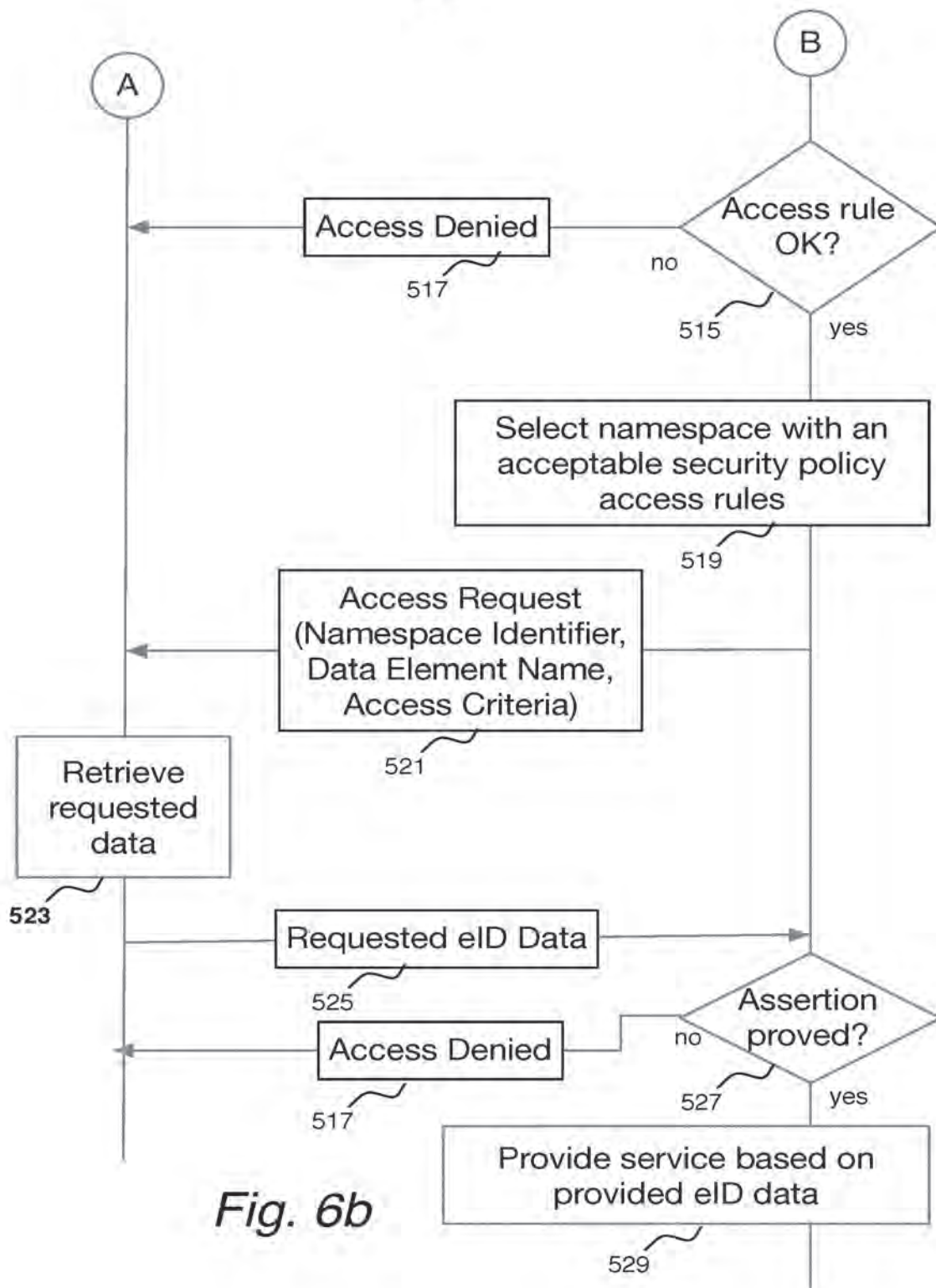
4/9

*Fig. 5*

5/9



6/9



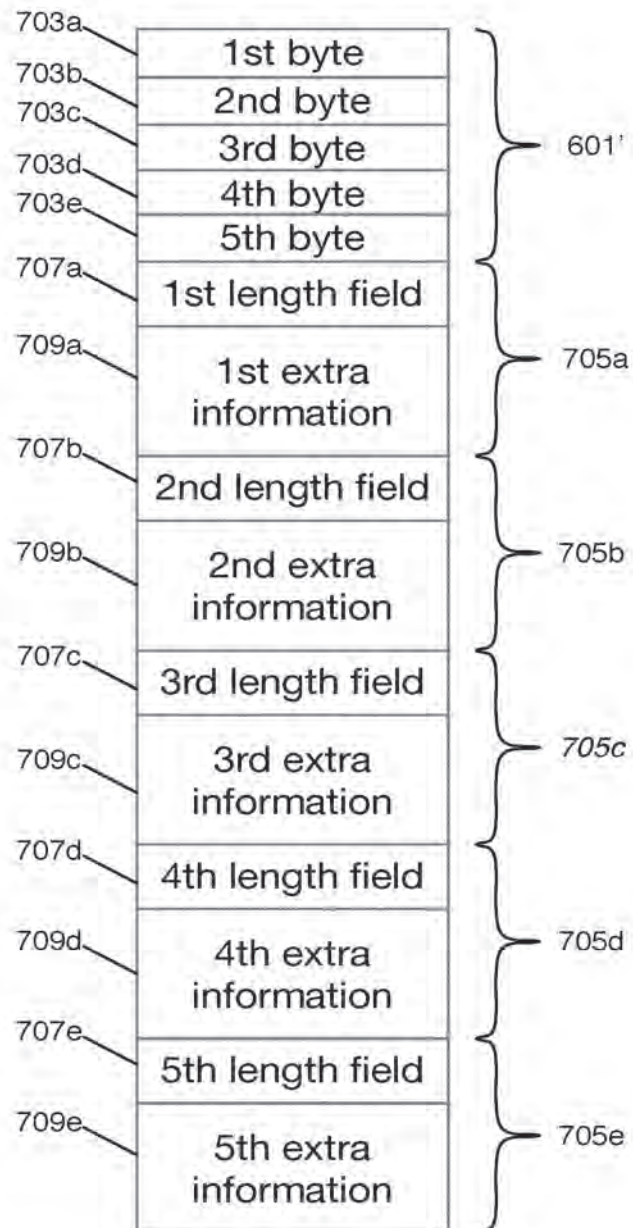
7/9

First byte							
b8	b7	b6	b5	b4	b3	b2	b1
Value determining the version of this template (for extensibility and interoperability)							
Second byte							
b8	b7	b6	b5	b4	b3	b2	b1
value denoting the authentication protocol required							
e.g. digital signature							
e.g. reader authentication							
e.g. certificate verification							
e.g. secure messaging							
e.g. role authentication							
e.g. user consent ...							
Third byte							
NOTE: could be coded over a nibble of the first byte if allowed							
b8	b7	b6	b5	b4	b3	b2	b1
value denoting the HASH type							
e.g. SHA-256							
e.g. SHA-384							
e.g. SHA-512							
...							
Fourth byte							
b8	b7	b6	b5	b4	b3	b2	b1
value denoting the signature scheme							
e.g. RSA							
e.g. ECDSA							
...							
Fifth byte							
b8	b7	b6	b5	b4	b3	b2	b1
value denoting secure messaging options							
e.g. AES 128 bits - CMAC							
e.g. AES 128 bits - EMAC							
e.g. AES-GCM ...							

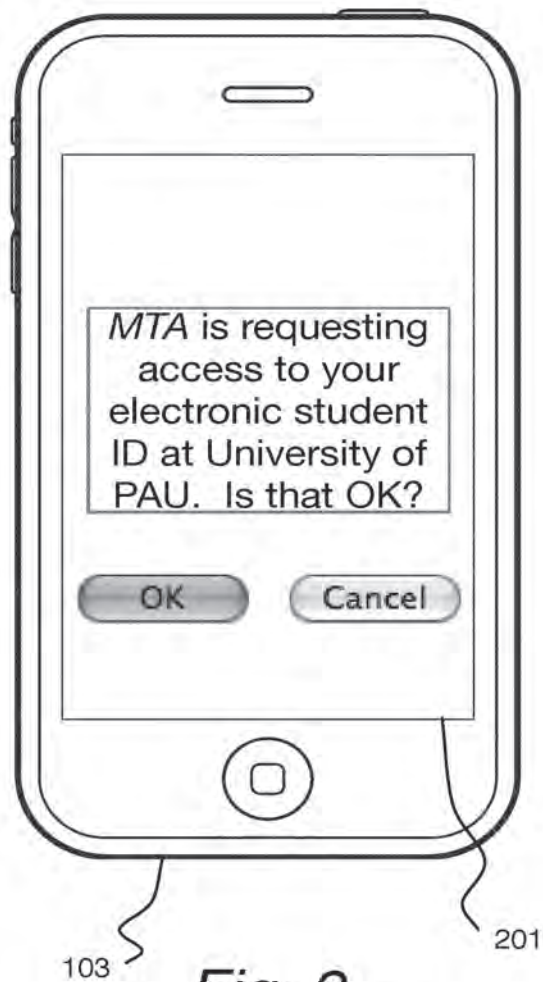
601

Fig. 7

8/9

*Fig. 8*

9/9

*Fig. 9*

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/076906

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06Q50/26 G06Q20/32 G06Q20/36
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q G07G

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EP0-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2016/294831 A1 (BORUNDA ADRIAN [US] ET AL) 6 October 2016 (2016-10-06) paragraph [0005] - paragraph [0008] paragraph [0021] - paragraph [0034] figures 1-2	1-16
X	WO 2015/036957 A1 (TORO DEV LTD [CN]) 19 March 2015 (2015-03-19) abstract page 1, line 25 - page 3, line 18 page 6, line 28 - page 13, line 32 figures 1, 2, 3A, 3B ----- -/--	1-16

☒ Further documents are listed in the continuation of Box C

☒ See patent family annex.

Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

12 November 2020

Date of mailing of the international search report

20/11/2020

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Nicoli, Félix

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/076906

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016/156386 A1 (VAN NIEUWENHUYZE OLIVIER [BE] ET AL) 2 June 2016 (2016-06-02) paragraph [0005] - paragraph [0007] paragraph [0050] - paragraph [0065]; figure 4	1-16
A	EMVCO: "EMV '96 Integrated Circuit Card Application Specification for Payment Systems", EMV, EMVCO * vol. 3.1.1 ; Contact 1 July 2006 (2006-07-01), pages 1-62, XP061034511, Retrieved from the Internet: URL:https://www.emvco.com/wp-content/uploads/documents/Emvapp_20090126073328.pdf [retrieved on 2020-01-06] page 15 - page 16	1-16
A	Anonymous: "Thales lance son nouveau portefeuille d'identité numérique - vos documents d'identité accessibles où que vous soyez Thales Group", * 29 July 2019 (2019-07-29), pages 1-7, XP055689283, Retrieved from the Internet: URL:https://www.thalesgroup.com/fr/group/journaliste/press_release/thales-lance-son-nouveau-portefeuille-didentite-numerique-vos [retrieved on 2020-04-24] the whole document	1-16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2020/076906

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016294831 A1	06-10-2016	AU 2016242966 A1 CA 2981659 A1 EP 3278248 A1 US 2016294831 A1 WO 2016161272 A1	26-10-2017 06-10-2016 07-02-2018 06-10-2016 06-10-2016
WO 2015036957 A1	19-03-2015	EP 3044902 A1 US 2015081538 A1 WO 2015036957 A1	20-07-2016 19-03-2015 19-03-2015
US 2016156386 A1	02-06-2016	CN 105657637 A CN 205029877 U FR 3029324 A1 US 2016156386 A1	08-06-2016 10-02-2016 03-06-2016 02-06-2016

Amendments to the Abstract:

Per CFR 1.121(b)(2)(ii), Applicant hereby amends the abstract by using strike-through and underlining as the methods to show all changes relative to the immediate prior version—the amendments are minor in nature.

The marked-up version of the Abstract is set forth on the following page.

The clean version of the Abstract is set forth on a page after the one above.

ABSTRACT

~~SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES~~

A system, mobile device, and method for managing security policies for data items stored in an electronic identification (eID) wallet on the mobile device. Security policies are associated with each of a plurality of supported namespaces on a mobile device and a verifier terminal operates to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.

~~Figure 6a~~

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	
	First Named Inventor	Mourad FAHER
	Art Unit	
	Examiner Name	
	Attorney Docket Number	GMT4110US/WO MQ/MB

U.S. PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S. PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1	20160294831	A1	2016-10-06	BORUNDA ADRIAN [US] ET AL	paragraph [0005] - paragraph [0008] paragraph [0021] - paragraph [0034] figures 1-2		
	2	20160156386	A1	2016-06-02	VAN NIEUWENHUYZE OLIVIER [BE] ET AL	paragraph [0005] - paragraph [0007] paragraph [0050] - paragraph [0065]; figure 4		
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ^{2j}	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	WO2015/036957	WO	A1	2015-03-19	TORO DEV LTD [CN]	abstract page 1, line 25-page 3, line 18 page 6, line 28-page 13, line 32	
If you wish to add additional Foreign Patent Document citation information please click the Add button.							Add	
NON-PATENT LITERATURE DOCUMENTS							Remove	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	Mourad FAHER
Art Unit	
Examiner Name	
Attorney Docket Number	GMT4110US/WO MQ/MB

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	International Search Report (PCT/ISA/210) and Written Opinion (PCT/ISA/237) mailed on November 20 2020, by the European Patent Office as the International Searching Authority for current International Application No. PCT/EP2020/076906 - [16 pages]	
	2	EMVCO: "EMV '96 Integrated Circuit Card Application Specification for Payment Systems", EMV, EMVCO vol. 3.1.1 ; Contact, 1 July 2006 (2006-07-01), pages 1-62, XP061034511, Retrieved from the Internet: URL:https://www.emvco.com/wp-content/uploads/documents/Emvapp_20090126073328.pdf [retrieved on 2020-01-06] - page 15 - page 16	
	3	Anonymous: "Thales lance son nouveau portefeuille d'identité numérique - vos documents d'identité accessibles où que vous soyez "Thales Group", 29 July 2019 (2019-07-29), pages 1-7, XP055689283, Retrieved from the Internet: URL:https://www.thalesgroup.com/fr/group/journaliste/press_release/thales-lance-son-nouveau-portefeuille-didentite-numerique-vos [retrieved on 2020-04-24] the whole document	
	4		
	5		

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	Mourad FAHER
Art Unit	
Examiner Name	
Attorney Docket Number	GMT4110US/WO MQ/MB

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).



See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Marc BOILLOT/	Date (YYYY-MM-DD)	2022-04-07
Name/Print	Marc BOILLOT	Registration Number	56164

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(51) International Patent Classification:
H04L 9/32 (2006.01)(21) International Application Number:
PCT/IB2014/064439(22) International Filing Date:
11 September 2014 (11.09.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/026,330 13 September 2013 (13.09.2013) US(71) Applicant: **TORO DEVELOPMENT LIMITED**
[CN/CN]; 5F-1, No. 51 Dongxing Road, Xinyi District,
Taipei City, 110 (TW).(72) Inventors: **RENARD, Laurent**; 5F-1, No. 51 Dongxing
Road, Xinyi District, Taipei City, 110 (TW). **PUEN-
TE-CASTAN, Gregory**; 5F-1, No. 51 Dongxing Road,
Xinyi District, Taipei City, 110 (TW).(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG,
MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM,
PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ,
TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,
TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,
DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,
LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, KM, ML, MR, NE, SN, TD, TG).**Published:**

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments (Rule 48.2(h))

(54) Title: SYSTEMS AND METHODS FOR PROVIDING SECURE DIGITAL IDENTIFICATION

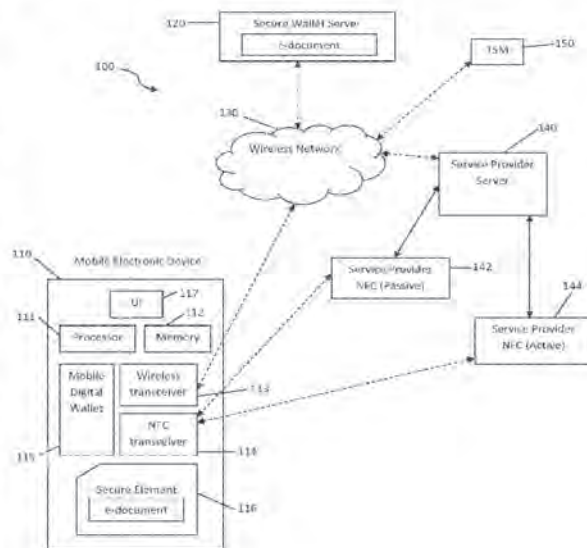


Fig. 1

(57) **Abstract:** Systems and methods for providing secure digital identification are described. The system comprises a mobile digital wallet installed on a NFC-enabled mobile electronic device. The mobile digital wallet is configured to receive a service provider request for personal ID information to enable the service provider to provide a service. The personal ID information is stored both in a secure element and at a secure wallet server. The system can determine a minimum-required-subset of the personal ID information necessary to satisfy the requested personal ID information and analyze whether to provide the minimum-required-subset from the secure element via the NFC transceiver or from the secure wallet server via the wireless network. 10 The system can then cause the minimum-required-subset of the set of personal ID information to be provided to the service provider in response to the analyzing step. A method of implementing the system is also described.

SYSTEMS AND METHODS FOR PROVIDING SECURE DIGITAL IDENTIFICATION

FIELD OF THE INVENTION

The present invention relates to a secure digital identification system and
5 method, and more particularly, to a mobile digital wallet identification system and
method for Near-Field Communication (NFC) services and a mobile electronic device
thereof.

BACKGROUND OF THE INVENTION

10 With the proliferation of technology and the rapid integration of nearly every
commercial industry, financial institution, educational organization, and government
agency with the World Wide Web, it has become increasingly difficult for individuals
to protect their identities. Identity theft is rampant, and yet individuals are asked to
provide personal identification information to service providers or to security personnel
15 to gain access to particular locations, without any guarantee of the security of their
information. In fact, individuals are often requested to provide more personal
information than is actually required to verify who they are, both over the internet and
in everyday transactions. Conversely, service providers, vendors, security personnel,
etc., would like as much assurance as possible that individuals are who they claim to be.

20 Presently there are no suitable options for harnessing technology to provide
“bulletproof” identification, while protecting the identity and privacy of those
providing their personal information.

SUMMARY OF THE INVENTION

25 Technologies are presented here in support of systems and methods of
providing secure digital identification.

According to a broad aspect of the invention, NFC-enabled systems and
methods receive a request at user's mobile device for the user to provide personal
identification (ID) information to a service provider. A subset of the user's personal

ID information sufficient to satisfy the request is determined and provided to the service provider, either via a NFC connection or via a secure server over a network.

According to a more particular aspect of the invention, a method for providing a mobile digital wallet identification system for use with a mobile electronic device having a processor, memory, code in the memory for implementing in the processor a mobile digital wallet, and an NFC transceiver is provided. In accordance with the method, the mobile electronic device is operatively coupled to a secure element and is in wireless communication with a secure wallet server over at least one wireless network.

The mobile digital wallet receives a service provider request which requests access to a subset of a set of personal ID information to enable the service provider to provide a service, the set of personal ID information being stored both in the secure element and at the secure wallet server. The mobile digital wallet then determines, using code executing in the processor, a minimum-required-subset of the set of personal ID information necessary to satisfy the access request to the requested subset of the set of personal ID information. The mobile digital wallet then analyzes, using code executing in the processor, whether to provide the minimum-required-subset of the personal ID information from the secure element via the NFC transceiver or from the secure wallet server via the wireless network. The method concludes with causing the minimum-required-subset of the set of personal ID information to be provided to the service provider in response to the analyzing step having concluded to provide the minimum-required-subset of the set of personal ID information.

Methods in accordance with more particular aspects of the invention can include further steps. For instance, the method can further include initializing a wireless download of at least one of a widget and a secure application over the wireless network from a server of the service provider subsequent to the service provider receiving the minimum-required-subset of the set of personal ID information as a result of the causing step.

In further embodiments, the method can further include, prior to the causing step, acquiring by the mobile digital wallet an account identifier and an access identifier from the user, the account identifier being associated with an account comprising the set of personal ID information and the access identifier indicating a right of the user to access the account. In some embodiments, the access identifier is a numeric code, an alphabetical code, an alphanumeric code, and/or a gesture, and the access identifier is

acquired via a User Interface (UI) of the mobile electronic device and detected by the mobile digital wallet. In some embodiments, the service provider request is an initiator request generated by a service provider-NFC transceiver, and the mobile electronic device is a target of the initiator request. In alternative embodiments, the service provider request is a response generated by a target service provider-NFC transceiver in response to an initiator request sent from the NFC transceiver of the mobile electronic device. The method can further include activating the NFC transceiver for radio frequency (RF) communication prior to the receiving step, enabling the receiving of the service provider request.

In yet further detailed embodiments of the invention, the receiving step can further comprise receiving at the mobile digital wallet an electronic notification comprising the service provider request, which can be one of a text message, multimedia message, instant message, and e-mail, notifying the user of a desire of the service provider to access the subset of the set of personal ID information. In accordance with aspects of the invention, the set of personal ID information includes at least one of the user's government-issued ID information, identifying image, biometric data, secure login credentials, membership information, address, and contact information.

According to yet another broad aspect of the invention, a system includes a mobile electronic device having a processor, memory, code in the memory which, when executed in the processor, implements a mobile digital wallet, and an NFC transceiver. The system further includes a secure element, the mobile electronic device being operatively coupled to the secure element; and a secure wallet server, the mobile electronic device being in wireless communication with the secure wallet server over at least one wireless network.

In a more particular aspect, the system executes the code in the processor for implementing the mobile digital wallet on the mobile electronic device which, when executed, configures the processor to: receive at the mobile digital wallet a service provider request which requests access to a subset of a set of personal ID information to enable the service provider to provide a service, the set of personal ID information being stored both in the secure element and at the secure wallet server; determine by the mobile digital wallet, using code executing in the processor, a minimum-required-subset of the set of personal ID information necessary to satisfy the access request to the requested subset of the set of personal ID information; analyze, by

the mobile digital wallet, using code executing in the processor, whether to provide the minimum-required-subset of the personal ID information from the secure element via the NFC transceiver or from the secure wallet server via the wireless network; and cause the minimum-required-subset of the set of personal ID information to be provided to the service provider in response to the analyzing step having concluded to provide the minimum-required-subset of the set of personal ID information.

These and other aspects, features and advantages of systems and method will be understood with reference to the following description of certain embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a high-level diagram illustrating an exemplary configuration of a system for providing secure digital identification according to embodiments of the invention;

Fig. 2 is a high-level flow diagram illustrating elements of a method for providing secure digital identification according to embodiments of the invention;

Fig. 3A and Fig. 3B are flow diagrams illustrating detailed elements of the method of Fig. 2 according to embodiments of the invention;

Fig. 4 is a high-level diagram illustrating a further exemplary configuration of a system for providing secure digital identification according to embodiments of the invention; and

Fig. 5 is a high-level flow diagram illustrating elements of a further method for providing secure digital identification according to embodiments of the invention.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

By way of overview and introduction, various systems and methods are described herein that facilitate providing secure digital identification by employing Near Field Communication (NFC) services to provide access to personal identification (ID) information stored in a secure element on a user's mobile electronic device ("MED" or "mobile device") and on a secure server accessible over a wireless network. An electronic document (e-document) is compiled containing a user's most private and sensitive personal ID data (e.g., social security number, passport number, ID photo,

biometric data, home address, drivers license, etc.), and the document is stored both in the secure element of the user's mobile device and on a secure server. An application installed on the user's mobile device manages access to the data. When a request for personal ID information is made, for example, by a service provider (SP), a secure NFC connection is created. The application then determines the minimum required set of data needed for the specific purpose of the request, and analyses whether to provide the data from the secure element over the NFC connection or from the secure server, depending on the nature of the request and the nature of the situation. The data can then be transmitted to the service provider via the selected path.

NFC is a short-range wireless connectivity technology that evolved from a combination of existing contactless identification and interconnection technologies. Products with built-in NFC simplify the way consumer devices interact with one another, helping people speed connections, receive and share information and make fast and secure payments.

Operating at a center frequency of 13.56 MHz and transferring data at up to 424 Kbits/second, NFC provides intuitive, simple, and safe communication between electronic devices. NFC is both a "read" and "write" technology. Communication between two NFC-compatible devices occurs when they are brought within four centimeters of one another: a simple wave or touch can establish an NFC connection, which is then compatible with other known wireless technologies such as Bluetooth or Wi-Fi for continuing the communication session initiated using NFC. The underlying layers of NFC technology follow universally implemented ISO, ECMA, and ETSI standards. Because the transmission range is so short, NFC-enabled transactions are inherently secure. Also, physical proximity of the device to the reader gives users the reassurance of being in control of the process.

NFC can be used with a variety of devices, from mobile phones that enable payment or transfer information, to digital cameras that send their photos to a TV set with just a touch.

An NFC connection always includes at least two devices, an initiator and a target. The initiator is the device that starts the NFC connection, by generating a radio frequency (RF) field that modulates toward a target device in the form of a request for connection. The target then responds to the initiator request and communication begins.

An NFC connection can be established in two modes, Active communication mode and Passive communication mode, depending on the target device. While the initiator is always a powered device capable of generating an RF field, the target may or may not be capable of generating its own RF field. In Active mode, both the initiator and target are powered and capable of generating their own RF field to communicate. The initiator starts the communication, and the target responds by modulating its own RF field toward the initiator. In Passive mode, the initiator starts the communication, and the target responds by modulating the initiator's RF field back to the initiator. By employing one of these modes of NFC, a secure connection between a user and a service provider can be established.

In accordance with embodiments of the invention, a service provider may be any individual, group, corporation, agency, etc. that provides a service or product to the user. For example, a service provider can be a retail or wholesale vendor, a professional services firm, a healthcare professional network, a financial institution, an educational organization, a transportation company, or a government agency. It should be noted that, while the systems and methods are described herein primarily as they relate to a transaction between a user and a service provider, transactions between a user and other entities can also be performed using the systems and methods. As such, a user may use the systems and methods described herein in order to securely provide a digital form of the user's identification in situations in which identification of the user is required, but in which a service or product is not necessarily being provided. For example, the systems and methods described herein can be used for security purposes to enable entry into otherwise restricted areas (e.g., at an airport, or to access a nightclub), or simply to identify one's self, such as when requested by a police officer. Therefore, the term 'service provider' as used herein should not be considered limiting except inasmuch as it refers to an individual or entity requesting identification from a user.

Fig. 1 shows a high-level diagram illustrating an exemplary configuration of a system for providing secure digital identification according to embodiments of the invention. System 100 includes MED 110, secure wallet server 120, wireless network 130, service provider server 140, and Trusted Service Manager (TSM) 150. MED 110 can be a smartphone, PDA, cell phone, multimedia player, tablet, laptop, or any other hand-held device capable of providing a NFC connection. MED 110 can include processor 111, memory 112, wireless transceiver 113, and user NFC transceiver 114.

Wireless transceiver 113 can use a wireless protocol such as 3G, LTE, GPRS, Bluetooth, IR, WiFi, or any other wireless communication protocol such that mobile electronic device 110 can communicate with wireless network 130.

5 In embodiments of the invention, code stored in memory 112 implements a mobile digital wallet 115 in processor 111. Mobile digital wallet 115 is an application which manages access to a user's personal information, as is explained in further detail below. MED 110 also includes secure element 116, which, in embodiments of the present invention, is implemented by a SIM card for a cell phone or a secure memory card, such as a micro-SD card, but which can comprise a variety of read/writeable storage devices. Secure element 116 can be hardware integrated into MED 110, and/or can be a memory card plugged into a memory card slot of MED 110. In some embodiments of the present invention, mobile electronic device 110 can comprise a plurality of secure elements 116. For example, both a SIM card and a memory card can be embedded into a NFC mobile device such as MED 116.

15 In some embodiments, secure element 116 can be operatively connected to the mobile electronic device 110 as described above. In some embodiments, secure element 116 can be operatively connected to mobile electronic device 110 without being embedded or plugged into the mobile electronic device 20. For example, secure element 116 may be wirelessly connected to mobile electronic device 110 via any appropriate wireless communication means (e.g., Bluetooth, WiFi, RF, etc.) Once secure element 116 is operatively connected to mobile electronic device 110 using any of the above means, NFC transactions can be conducted which can provide access to data stored on secure element 116 in accordance with embodiments of the invention.

25 Mobile electronic device 110 can also include user interface (UI) 117. In some embodiments, UI 117 can be displayed on a touchscreen or other display operatively coupled to an input device (not shown). A user can input information, such as an account identifier and/or an access identifier (e.g. a password, pin-code, or gesture), through UI 117 to enable access to the e-document containing the user's personal identification information, as will be discussed in detail below. In some embodiments, the contents of the e-document can be independently verified and the e-document can be configured so as to be inaccessible without the user first providing an associated account identifier and/or access identifier. Duplicates of the e-document can be stored both in secure element 116 and on secure wallet server 120, each copy acting as a secure backup of the other.

System 100 also includes at least one of an active NFC transceiver 142 and a passive NFC transceiver 144 associated with a service provider, which is operatively connected to service provider server 140, and which can communicate with user NFC transceiver 114 of mobile electronic device 110. Passive and/or active service provider NFC transceivers 142, 144, can be integrated in other mobile devices, tags, or readers, and/or located at a kiosk or other point-of-sale as required. In some embodiments, a SP may use a NFC enabled mobile device or kiosk to communicate directly with wireless network 130 in lieu of accessing wireless network 130 via service provider server 140. Similarly, TSM 150, which can act as a neutral contact point for business and technical connections between Mobile Network Operators, device manufacturers, and/or other entities requiring access to a user's secure element in a NFC transaction, can enable service providers to communicate with the secure element in NFC-enabled handsets in lieu of the service providers communicating directly with mobile electronic device 110. Of course, a trusted service manager may not be required depending on the type of service provider involved in a given NFC transaction.

Turning to Fig. 2, a high-level flow diagram illustrating elements of a method for providing secure digital identification according to embodiments of the invention is provided. Method 200, which can be employed, for example, using system 100, starts at step 205 when personal ID information is provided and recorded in a secure e-document. At step 210, the personal ID information (e-document) is stored in secure element 116 and on secure wallet server 120. As explained above, in some embodiments the information in the e-document can be independently verified prior to storage. In some embodiments, the user provides the personal ID information directly to mobile digital wallet 115, which can create the secure e-document. Mobile digital wallet 115 can then store the e-document in secure element 116, and send a copy of the e-document to secure wallet server 120 via wireless network 130 for storage there. In other embodiments, the e-document can be created by the user or a third party via other means, such as through a web portal or web application accessed over the Internet, and the e-document can be uploaded first to secure wallet server 120 using security controls appropriate to maintaining data integrity, as understood by those having ordinary skill in the art. Mobile digital wallet 115 can then download a copy of the e-document via wireless transceiver 113, and store it in secure element 116.

At step 215, mobile digital wallet 115 receives a request from a service provider for access to a subset of the personal ID information recorded in the e-document, in

order for the service provider to provide a service to the user. For example, a rental car company may request a user's driver license information prior to renting the user a car, or a liquor store owner may want to verify that a potential alcohol purchaser is above the mandated age restriction. In accordance with embodiments of the invention, a verbal or otherwise non-digital request can be made by a service provider to the user, requesting that the user begin a NFC connection with the service provider. As explained in detail above, this can be an active communication mode connection wherein user NFC transceiver 114 generates a RF field and modulates the field toward SP active NFC transceiver 144, which then replies with a RF field of its own. Alternatively, the NFC connection can be a passive communication mode connection wherein user NFC transceiver 114 generates a RF field and modulates the field toward SP passive NFC transceiver 142, which then responds by modulating the received RF field back to user NFC transceiver 114.

In both of the forgoing embodiments, user NFC transceiver 114 acts as the initiator and either SP passive NFC transceiver 142 or SP active NFC transceiver 144 acts as the target. In some embodiments, while the user is the initiator of the NFC connection, the response received by the user from the target NFC device of the SP can contain the request in digital form. For example, a user can bring MED 110 within the required proximity to a service provider's NFC-enabled device to start an NFC connection, at which time the service provider's NFC-enabled device can digitally request the desired subset of the user's personal ID information from MED 110. In other embodiments, SP active NFC transceiver 144 can act as the initiator, and user NFC transceiver 114 can act as the target. The request from the service provider can then be defined as the transmission of the RF field from SP active NFC transceiver 144 toward user NFC transceiver 114, rather than the request being in response to receiving a transmission from user NFC transceiver 114. In summary, a request from a SP can be in digital form as part of a NFC connection with a user's NFC enabled device, in lieu of a verbal or otherwise non-digital request to begin a NFC connection.

In some embodiments, the access request can comprise a request to connect via NFC, wherein the underlying purpose of the NFC connection is for the SP to receive the user's personal ID information. Furthermore, it should be understood that the access request can additionally or alternatively include a request for the service provider to retrieve the requested information from a predefined location, an unspecified location, and/or a location specified by the SP or user. Alternatively and/or additionally to the

request to retrieve information, the access request can include a request for the user to provide the requested information to the SP (i.e., for the SP to receive the requested information) from a predefined location, an unspecified location, and/or a location specified by the SP or user.

5 In some embodiments, the SP request to initiate a NFC connection can be in the form of an electronic notification (other than an NFC transmission) received at MED 110. For example, an electronic notification can be an e-mail, text message, multimedia message, IM, "tweet", ping, or any other appropriate form of digital message sent by the SP and received at MED 110 via wireless transceiver 113,
10 requesting a NFC connection with the user. This may be necessary, for example, when user NFC transceiver 114 is not actively enabled for NFC connection, or when an NFC-enabled device of the SP does not detect a RF field of the user.

 At step 220, mobile digital wallet 115 acquires an account identifier and/or an access identifier from the user via UI 117. An account identifier may be required, for
15 example, if more than one e-document is stored in secure element 116 and secure wallet server 120, or if more than one profile (set of information) has been created. In this instance, an account identifier can identify the desired e-document or profile. In some embodiments, an account identifier may not be required if there is only one e-document or profile, or if a default e-document or profile has been previously defined. The
20 access identifier may be any form of password, pin-code, or user-defined gesture, etc., typically known only to the user, which can be provided to mobile digital wallet 115 to enable mobile digital wallet 115 to manage access to the user's personal ID information. At step 225, mobile digital wallet 115 verifies the accuracy of the acquired account identifier and/or access identifier. If the inputted account identifier
25 and/or access identifier fails to match a previously defined account identifier and/or access identifier, access is denied at step 230, and the user is again requested to provide the account identifier and/or access identifier. In some embodiments, if an incorrect account identifier and/or access identifier is provided a predefined number of times, an alternative action can be taken, such as a notification being sent to the user, an account manager, and/or the SP indicating, for example, that incorrect information has been
30 provided and access has been denied. If the inputted account identifier and access identifier are correct, then access is granted for the specified account (e-document or profile), and the method continues.

In accordance with embodiments of the invention, at step 235 mobile digital wallet 115 determines, using code executing in the processor, a minimum-required-subset of the set of personal ID information necessary to satisfy the subset of personal ID information requested by the SP. For example, a request may simply ask that user provide identifying information to the SP. There are many types of information that can identify a user, such as a driver license, passport, social security number, etc. In different instances and situations, service providers may require different types of information. For example, to pass a security checkpoint a driver license may be requested, whereas to check in at a hospital a social security card may be requested. Mobile digital wallet 115 can therefore determine a subset of all the personal information stored in the e-document which is sufficient to satisfy the request. To make this determination, mobile digital wallet 115 can, for example, analyze characteristics of the service provider, such as the type of service provided, the location of the service provider, etc.

In some embodiments the subset may require a particular form of identification, or multiple forms of identification, in order to satisfy the request. However, in other embodiments the subset may require less information than is provided by any one particular form of identification, or may require some information from one form of identification and some information from another form of identification. For example, to enter a nightclub with a 21+ age restriction, a driver license may be requested by the nightclub. However, a driver license typically includes a photo of the cardholder, a home address, driver license number, date of birth, hair and eye colors, etc. All the nightclub security actually wants to confirm is whether or not patrons to the nightclub are 21+ years old. However, providing a driver license exposes to strangers more personal information than is necessary to make that confirmation. In such a circumstance, mobile digital wallet 115 can determine which personal information is required, and provide only that information. In this instance, for example, mobile digital wallet 115 can determine that the only information that must be provided from the verified e-document is a date of birth of the patron, and a digital photograph of the patron to confirm the person providing the personal ID information is the same person associated with the personal ID information.

By way of another example, to receive special education services for a child from a school district, a parent may be requested to provide two forms of identification proving the parent resides in that school district. Both a driver license and passport

contain the address of the parent, but both also contain other information which the parent may not desire to share, and which are not necessary for proving where the parent lives. Mobile digital wallet 115 can determine which information is required from the two forms of identification, and that subset can be provided to the service provider, in this case the school district, without exposing unnecessary private data.

Once mobile digital wallet 115 determines the minimum-required-subset of personal ID information to provide to the SP, at step 240 mobile digital wallet 115 analyzes, using code executing in the processor, whether to provide the minimum-required-subset of the personal ID information from secure element 116 via user NFC transceiver 114 at step 245, or from secure wallet server 120 via wireless network 130 at step 250. As explained in detail above, the user's personal ID information is stored both in secure element 116 and on secure wallet server 120. Depending on the situation, after receiving the request, mobile digital wallet 115 may determine that it is preferable to provide the information from one source over another. For example, a user at an NFC-enabled airline check-in kiosk may receive a request via the NFC-enabled kiosk in any of the manners described in step 215. Mobile digital wallet 115 can then direct secure wallet server 120 to provide the necessary information directly to the airline's server. In other embodiments, mobile digital wallet 115 can provide the information from secure element 116 to a NFC-enabled device of the service provider via NFC transceiver 114.

At step 255, once the minimum-required-subset of the personal ID information is provided to the service provider, either from secure element 116 via user NFC transceiver 114 or from secure wallet server 120 via wireless network 130, the service provider can confirm that the subset of information provided by mobile digital wallet 115 does in fact satisfy the request. If the provided information fails to satisfy the request, the method can return to step 235, where mobile digital wallet 115 can revise the determined minimum-required-subset. In some embodiments, if mobile digital wallet 115 fails to determine a minimum-required-subset after a predefined number of attempts, an alternative action can be taken, such as a notification being sent to the user, an account manager, and/or the SP, indicating, for example, mobile digital wallet 115 has failed to determine a minimum-required-subset that satisfies the request, and/or indicating that the user should provide the personal ID information manually. If the provided information is sufficient to satisfy the access request, then at step 260 the desired service can be provided to the user and the method ends.

Turning now to Fig. 3A and Fig. 3B, flow diagrams illustrating detailed elements of method 200 of Fig. 2 are provided according to embodiments of the invention. In particular, Fig. 3A and Fig. 3B provide steps that can be taken depending on what roles the user and the SP play in the NFC transaction, initiator or target, in accordance with embodiments of the invention. In the flow diagram of Fig. 3A, MED 110 receives an electronic notification comprising the request at step 305. As explained above, electronic notification can be an e-mail, text message, multimedia message, IM, "tweet," ping, or any other appropriate form of digital message containing the request. Use of an electronic notification comprising the request can be useful, for example, in situations where user NFC transceiver 114 is not initially activated. As such, the electronic notification can inform the user to activate the NFC feature of MED 110. Alternatively or additionally, the electronic notification can also include other information relating to the request, such as coupons, offers, instructions, directions, etc., in conjunction with the request for personal ID information.

At step 310, mobile digital wallet 115 can activate user NFC transceiver 114, which can then act as initiator and send a RF communication to a NFC-enabled target device of the service provider, such as SP passive NFC transceiver 142 or SP active NFC transceiver 144, at step 315. This can be performed, for example, by waving or tapping MED 110 near or against the SP's NFC-enabled device to prompt the SP to connect via NFC. At step 320, a response from the service provider target is received at user NFC transceiver 114, and then at step 325 personal ID information can be provided in accordance with the further steps of method 200 described in Fig. 2.

In alternative embodiments, as shown in the flow diagram of Fig. 3B, at step 330 mobile digital wallet 115 can activate user NFC transceiver 114 as a target. User NFC transceiver 114 can remain in a target mode until it receives an initiating RF communication via NFC from a NFC-enabled device of a service provider, such as SP active NFC transceiver 144, at step 335. The initiating RF communication can include the request for personal ID information, or simply a request to connect via NFC, with the actual request being sent subsequently during the NFC connection. At step 340, user NFC transceiver 114 responds to the initiator RF communication, and at step 345 personal ID information can be provided in accordance with the further steps of method 200 described in Fig. 2.

Fig. 4 is a high-level diagram illustrating a further exemplary configuration of a system for providing secure digital identification according to embodiments of the

invention. Similar to system 100 of Fig. 1, system 400 includes MED 410, secure wallet server 420, wireless network 430, service provider A server 440, and service provider B server 450. MED 410 can be any hand-held device capable of providing a NFC connection, and can include a processor, memory, wireless transceiver (all not shown), and a user NFC transceiver 414. In embodiments of the invention, code stored in the memory implements in the processor a mobile digital wallet 415. Mobile digital wallet 415 is an application which manages access to a user's personal information, as is explained in further detail below. MED 410 also includes secure element 416, which, in embodiments of the present invention, is implemented by a SIM card for a cell phone or a secure memory card, such as a micro-SD card.

System 400 also includes third-party NFC transceiver 460. Third-party NFC transceiver 460 as described herein can refer to any NFC-enabled device capable of sharing with MED 410 information relating to a service provider via NFC. Third-party NFC transceiver 460 can be part of another user's mobile device, can be a stand-alone kiosk, tag, or reader etc. In some embodiments, third-party NFC transceiver 460 can be owned by or associated with a particular service provider or a plurality of service providers. For example, third-party NFC transceiver 460 can be a NFC-enabled kiosk in a mall or supermarket, etc.

It should be noted that while in the exemplary embodiment of systems 100, 400, one or two server providers are referenced, in other embodiments more or less service providers, and service provider servers, may be included. Furthermore, while in system 400 SP servers are shown in communication with MED 410 and secure wallet server 420 directly over wireless network 430, in other embodiments one or more service provider servers may communicate indirectly via a TSM (not shown). As described above, a service provider can be, for example, a retailer, a financial institution, a transportation system, or a restaurant chain, etc.

Many service providers prefer or require a user to complete a registration or "sign-up" process prior to providing service. The sign-up process can be in relation to a rewards program, membership, account, etc., and typically requires the user to provide at least some personal ID information to the SP. Employing the systems and methods described herein, a streamlined instant sign-up can be achieved. In accordance with embodiments of the invention, a secure application associated with a particular service provider can be provided to the user to be stored in the secure element. Furthermore, a widget lifecycle management platform, and a distribution and

transaction system for NFC services, such as is described in detail in U.S. Non-Provisional Application Serial No. 13/ 934,726 (filed on July 3, 2013 which is hereby incorporated by reference), can be employed to provide service provider widgets to MED 410. Users can access SP widgets on a virtual machine 418 to enable
5 NFC transactions using the associated secure application stored in secure element 416. As will be explained below, mobile digital wallet 415 can play an integral role in the rapid deployment of such systems to MED 410, as well as the other features described herein.

Briefly, as is explained in detail in U.S. Pub. No. US 2011/0143663, published
10 June 16, 2011, in certain embodiments, an integrated distribution and transaction system for at least one mobile electronic device can comprise a server having a widget generator for creating at least one widget having a certificate. A widget is an independent application that is developed using an SDK and that can be run on a virtual machine of the mobile electronic device. The widget may display multimedia content
15 associated with a secure application installed on the mobile electronic device.

In some embodiments, the integrated distribution and transaction system can further include a communication interface for distributing the widget and retrieving widget information associated with NFC transactions, and at least one mobile electronic device having a transaction terminal and a virtual machine. The transaction
20 terminal can include an NFC modem and at least one secure element divided into a plurality of secure domains. The virtual machine can authenticate the certificate, manage the widgets received from the communication interface, and change the widget information, while enabling the mobile electronic device to perform at least one NFC transaction using the corresponding secure application.

According to another broad aspect of the invention that can be used in certain
25 embodiments, a distribution system can be installed on a mobile electronic device, and can be operatively coupled to a secure element having one or more secure applications. In some embodiments, the system can further include a virtual machine configured to execute in a processor to provide a runtime environment capable of running a plurality
30 of widgets. The virtual machine can be configured to enable the widgets to be operable on any of a plurality of mobile operating systems, including the particular mobile operating system on which it is installed. The system can further include a secure element manager configured to enable the widgets to read from or write to the secure element. This can be accomplished, for example, by providing the widgets

with access to corresponding secure applications stored in the secure element. The system can enable the mobile electronic device to perform NFC transactions using the corresponding secure applications.

Turning now to Fig. 5, a high-level flow diagram illustrating elements of a further method for providing secure digital identification is provided according to embodiments of the invention. Method 500 starts at step 505 when a request is received by MED 410. As described in detail above, the request can include the request for the user to provide personal ID information that the service provider requires in order to provide a service to the user. For example, a user at a NFC-enabled kiosk in a mall may desire to sign up for a membership card prior to engaging a service provider for services. In this example, a request can be provided via third party NFC transceiver 460, on behalf of the service provider, for the user to provide personal ID information. As another example, while a user is in the process of completing a NFC transaction at a retail store, a request may ask the user if the user would be interested in a rewards program, for which personal ID information must be provided.

At step 510, the user can provide an account identifier and/or an access identifier to mobile digital wallet 415, allowing mobile digital wallet 415 to provide personal ID information recorded in a verified e-document to a service provider in accordance with the methods described herein. At step 515, mobile digital wallet 415 can verify the provided account identifier and/or access identifier, after which the service provider can be notified, at step 520, that the user has been verified. At step 525, the personal ID information can be provided to the service provider by the mobile digital wallet 415. This can include, for example, using one or more of the steps of method 200 outlined in Fig. 2, including determining a minimum-required-subset of the personal ID information required to satisfy the request, analyzing from where to provide the minimum-required-subset to a server of the service provider, and/or sending the information either from secure element 416 via user NFC transceiver 414 or from secure wallet server 420 via wireless network 430.

In accordance with embodiments of the invention, once the user's personal ID information has been provided to the service provider, SP widgets and secure applications for NFC transactions can be pushed over-the-air to MED 410 at step 530 from servers associated with service provider. Finally, at step 535, the user can complete a NFC transaction using the SP widgets and secure application. Thus,

employing the systems and methods described herein, a user can quickly and seamlessly complete a sign-up process with a service provider.

At this juncture, it should be noted that although much of the foregoing description has been directed to systems and methods for providing secure digital identification, the systems and methods disclosed herein can be similarly deployed and/or implemented in scenarios, situations, and settings far beyond the referenced scenarios. It is to be understood that like numerals in the drawings represent like elements through the several figures, and that not all components and/or steps described and illustrated with reference to the figures are required for all embodiments or arrangements.

Thus, illustrative embodiments and arrangements of the present systems and methods provide a computer implemented method, computer system, and computer program product for providing secure digital identification. The flowchart and block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments and arrangements. In this regard, each block in the flowchart or block diagrams can represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

The functions describe herein can be implemented by hardware and or hardware executing code (also known as programs, software, or software applications) which include machine instructions for a programmable processor, and can be implemented in a high-level procedural and/or object-oriented programming language, and/or in assembly/machine language. As used herein, the terms machine-readable storage medium and computer-readable storage medium refer to any computer program product, apparatus and/or device (e.g., magnetic discs, optical disks, memory,

Programmable Logic Devices (PLDs)) used to provide machine instructions and/or data to a programmable processor, including a machine-readable storage medium that receives machine instructions as a machine-readable signal. The term machine-readable signal refers to any signal used to provide machine instructions and/or data to a programmable processor. A machine-readable storage medium does not include a machine-readable signal.

The systems and techniques described here can be implemented in a computing system that includes a back end component (e.g., as a data server), or that includes a middleware component (e.g., an application server), or that includes a front end component (e.g., a client computer having a graphical user interface or a Web browser through which a user can interact with an implementation of the systems and techniques described here), or any combination of such back end, middleware, or front end components. The components of the system can be interconnected by any form or medium of digital data communication (e.g., a communication network). Examples of communication networks include a local area network (LAN), a wide area network (WAN), and the Internet. A wireless network can include both wired and wireless connections.

The computing system can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

While this specification contains many specific implementation details, these should not be construed as limitations on the scope of any implementation or of what may be claimed, but rather as descriptions of features that may be specific to particular embodiments of particular implementations. Certain features that are described in this specification in the context of separate embodiments can also be implemented in combination in a single embodiment. Conversely, various features that are described in the context of a single embodiment can also be implemented in multiple embodiments separately or in any suitable subcombination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a subcombination or variation of a subcombination.

Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Moreover, the separation of various system components in the embodiments described above should not be understood as requiring such separation in all embodiments, and it should be understood that the described program components and systems can generally be integrated together in a single software product or packaged into multiple software products.

The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising", when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

It should be noted that use of ordinal terms such as "first," "second," "third," etc., in the claims to modify a claim element does not by itself connote any priority, precedence, or order of one claim element over another or the temporal order in which acts of a method are performed, but are used merely as labels to distinguish one claim element having a certain name from another element having a same name (but for use of the ordinal term) to distinguish the claim elements. Also, the phraseology and terminology used herein is for the purpose of description and should not be regarded as limiting. The use of "including," "comprising," or "having," "containing," "involving," and variations thereof herein, is meant to encompass the items listed thereafter and equivalents thereof as well as additional items.

Particular embodiments of the subject matter described in this specification have been described. Other embodiments are within the scope of the following claims. For example, the actions recited in the claims can be performed in a different order and still achieve desirable results. As one example, the processes depicted in the accompanying figures do not necessarily require the particular order shown, or sequential order, to achieve desirable results. In certain implementations, multitasking and parallel processing may be advantageous.

WHAT IS CLAIMED IS:

What is claimed is:

1. A method for providing a mobile digital wallet identification (ID) system for use with a mobile electronic device having a processor, memory, code in the memory for implementing in the processor a mobile digital wallet, and an NFC transceiver, the mobile electronic device being operatively coupled to a secure element and being in wireless communication with a secure wallet server over at least one wireless network, the method comprising:
 - receiving at the mobile digital wallet a service provider request which requests access to a subset of a set of personal ID information to enable the service provider to provide a service, the set of personal ID information being stored both in the secure element and at the secure wallet server;
 - determining by the mobile digital wallet, using code executing in the processor, a minimum-required-subset of the set of personal ID information necessary to satisfy the access request to the requested subset of the set of personal ID information;
 - analyzing, by the mobile digital wallet, using code executing in the processor, whether to provide the minimum-required-subset of the personal ID information from the secure element via the NFC transceiver or from the secure wallet server via the wireless network; and
 - causing the minimum-required-subset of the set of personal ID information to be provided to the service provider in response to the analyzing step having concluded to provide the minimum-required-subset of the set of personal ID information.
2. The method of claim 1, further comprising, initializing a wireless download of at least one of a widget and a secure application over the wireless network from a server of the service provider subsequent to the service provider receiving the minimum-required-subset of the set of personal ID information as a result of the causing step.
3. The method of claim 1, further comprising, prior to the causing step, acquiring by the mobile digital wallet an account identifier and an access identifier from the user, the account identifier being associated with an account comprising the

set of personal ID information and the access identifier indicating a right of the user to access the account.

4. The method of claim 3, wherein the access identifier is at least one of a numeric code, an alphabetical code, an alphanumeric code, and a gesture, and wherein the access identifier is acquired via a User Interface (UI) of the mobile electronic device and detected by the mobile digital wallet.
5. The method of claim 1, wherein the service provider request is an initiator request generated by a service provider-NFC transceiver, and wherein the mobile electronic device is a target of the initiator request.
6. The method of claim 1, wherein the service provider request is a response generated by a target service provider-NFC transceiver in response to an initiator request sent from the NFC transceiver of the mobile electronic device.
7. The method of claim 1, further comprising activating the NFC transceiver for radio frequency (RF) communication prior to the receiving step, enabling the receiving of the service provider request.
8. The method of claim 1, the receiving step further comprising receiving at the mobile digital wallet an electronic notification comprising the service provider request.
9. The method of claim 8, wherein the electronic notification is one of a text message, multimedia message, instant message, and e-mail, notifying the user of a desire of the service provider to access the subset of the set of personal ID information.
10. The method of claim 1, wherein the set of personal ID information includes at least one of the user's government-issued ID information, identifying image, biometric data, secure login credentials, membership information, address, and contact information.

11. A mobile digital wallet identification (ID) system comprising:

a mobile electronic device having a processor, memory, code in the memory for implementing in the processor a mobile digital wallet, and an NFC transceiver;

5 a secure element, the mobile electronic device being operatively coupled to the secure element; and

a secure wallet server, the mobile electronic device being in wireless communication with the secure wallet server over at least one wireless network;

10 wherein the code in the memory for implementing in the processor the mobile digital wallet is executable in the processor of the mobile electronic device which, when executed, configures the processor to:

receive at the mobile digital wallet a service provider request which requests access to a subset of a set of personal ID information to enable the service provider to provide a service, the set of personal ID information being stored both in the secure element and at the secure wallet server;

15 determine by the mobile digital wallet, using code executing in the processor, a minimum-required-subset of the set of personal ID information necessary to satisfy the access request to the requested subset of the set of personal ID information;

20 analyze, by the mobile digital wallet, using code executing in the processor, whether to provide the minimum-required-subset of the personal ID information from the secure element via the NFC transceiver or from the secure wallet server via the wireless network; and

25 cause the minimum-required-subset of the set of personal ID information to be provided to the service provider in response to the analyzing step having concluded to provide the minimum-required-subset of the set of personal ID

30

12. The system of claim 11, further configured to initialize a wireless download of at least one of a widget and a secure application over the wireless network from a server of the service provider subsequent to the service provider receiving the

minimum-required-subset of the set of personal ID information as a result of the causing operation.

- 5 13. The system of claim 11, the processor further configured to acquire by the mobile digital wallet, prior to the causing operation, an account identifier and an access identifier from the user, the account identifier being associated with an account comprising the set of personal ID information and the access identifier indicating a right of the user to access the account.
- 10 14. The system of claim 13, wherein the access identifier is at least one of a numeric code, an alphabetical code, an alphanumeric code, and a gesture, and wherein the access identifier is acquired via a User Interface (UI) of the mobile electronic device and detected by the mobile digital wallet.
- 15 15. The system of claim 11, wherein the service provider request is an initiator request generated by a service provider-NFC transceiver, and wherein the mobile electronic device is a target of the initiator request.
- 20 16. The system of claim 11, wherein the service provider request is a response generated by a target service provider-NFC transceiver in response to an initiator request sent from the NFC transceiver of the mobile electronic device.
- 25 17. The system of claim 11, further configured to activate the NFC transceiver for radio frequency (RF) communication prior to the receiving step, enabling the receiving of the service provider request.
- 30 18. The system of claim 11, the processor further configured to receive at the mobile digital wallet an electronic notification comprising the service provider request.
19. The system of claim 18, wherein the electronic notification is one of a text message, multimedia message, instant message, and e-mail, notifying the user of a desire of the service provider to access the subset of the set of personal ID information.

20. The system of claim 1, wherein the set of personal ID information includes at least one of the user's government-issued ID information, identifying image, biometric data, secure login credentials, membership information, address, and contact information.

1/5

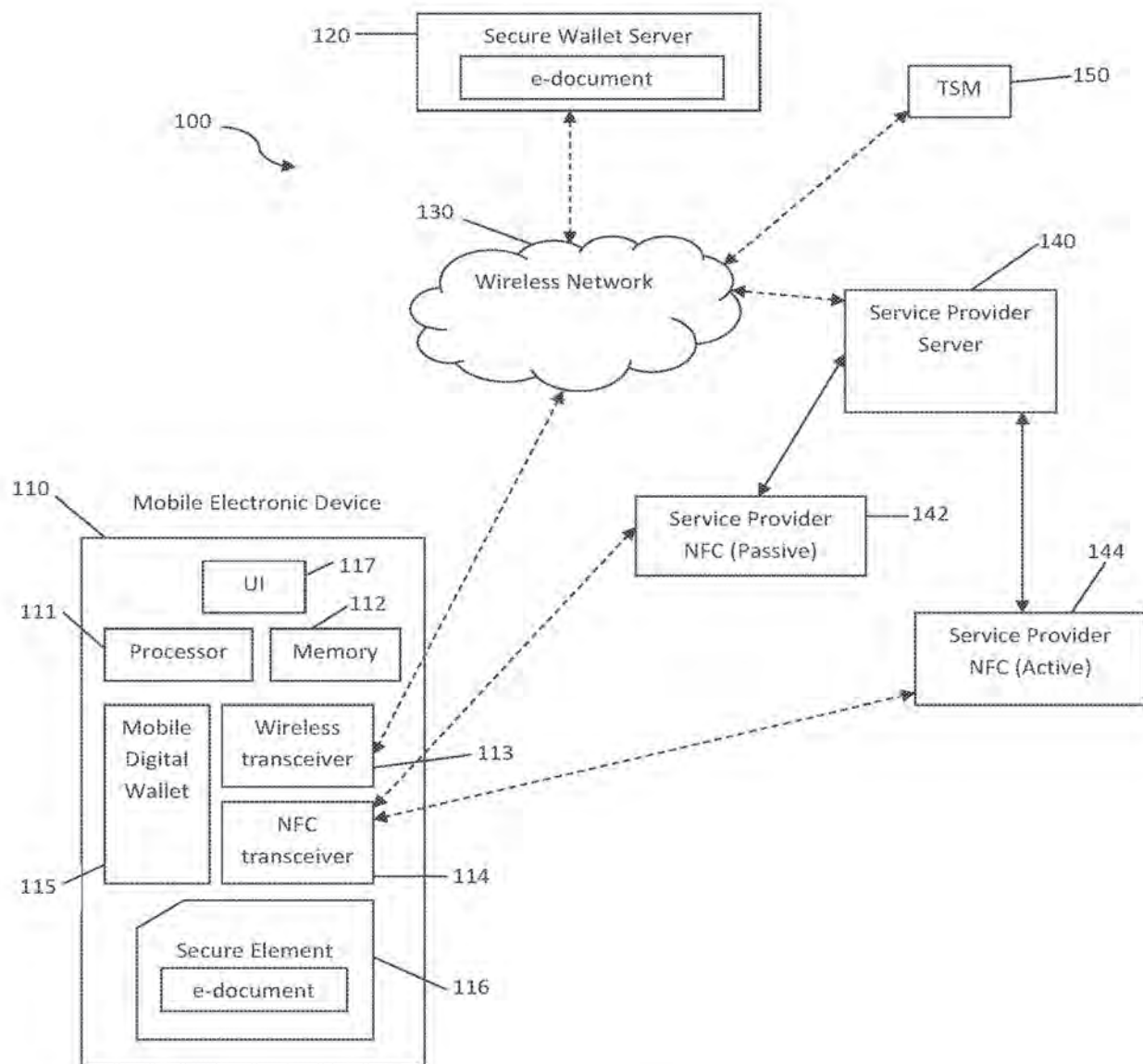
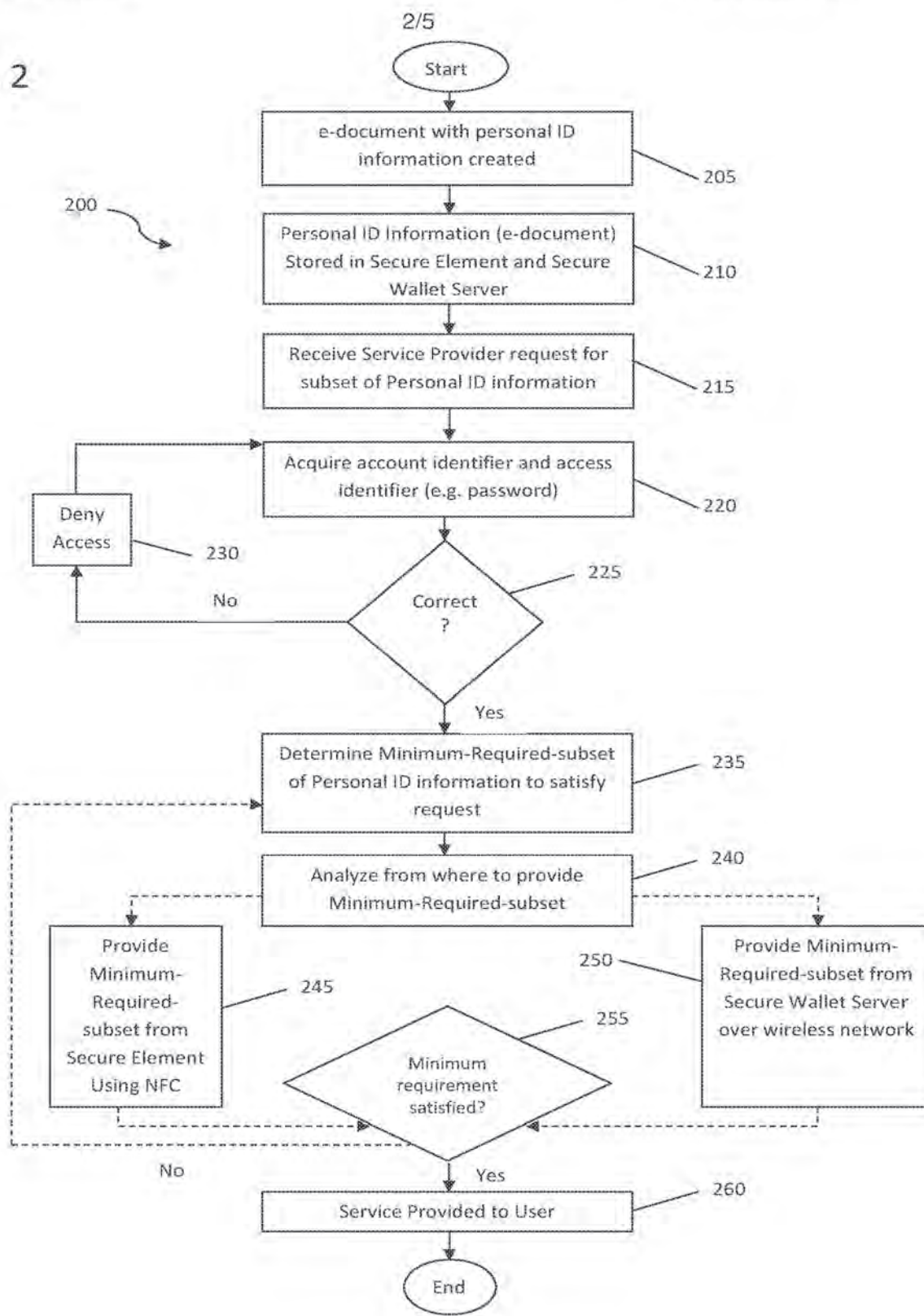


Fig. 1

Fig. 2



3/5

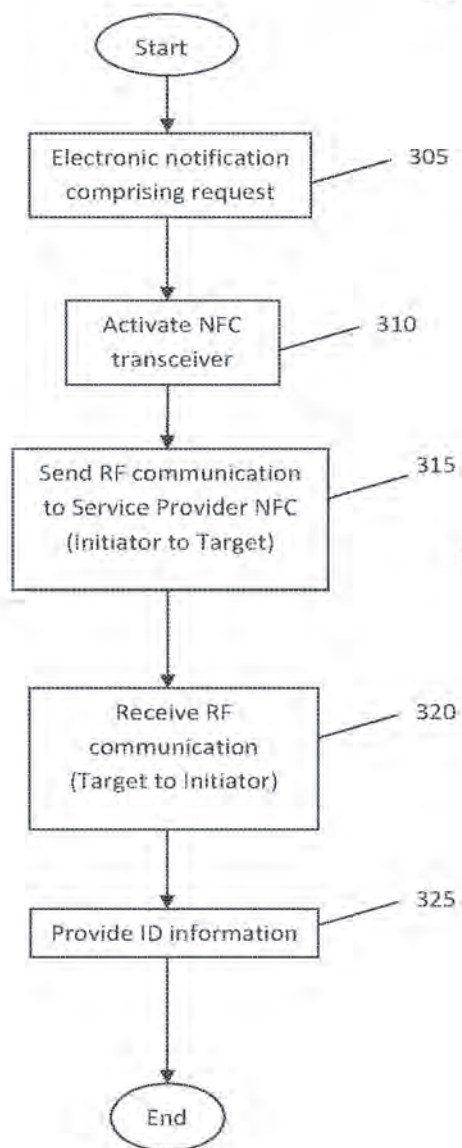


Fig. 3A

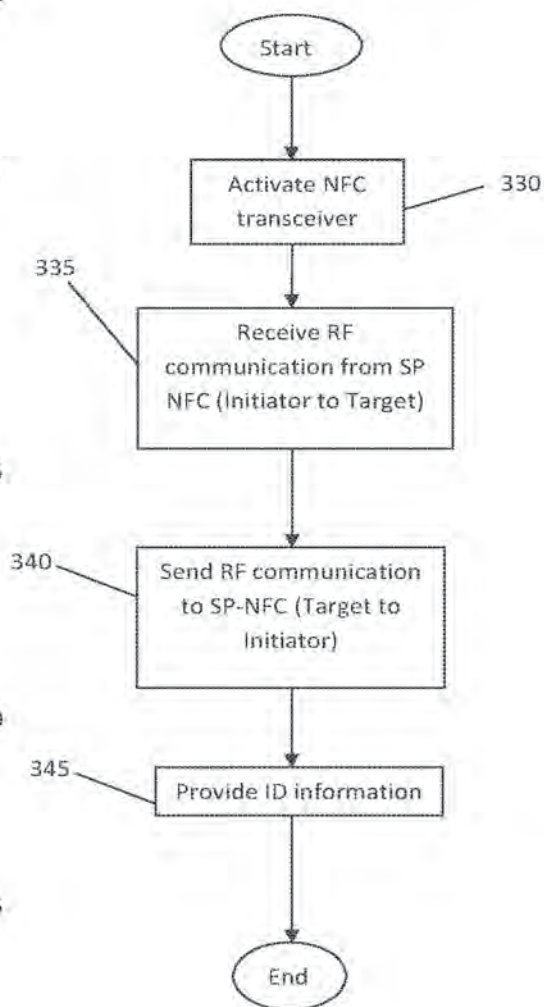


Fig. 3B

4/5

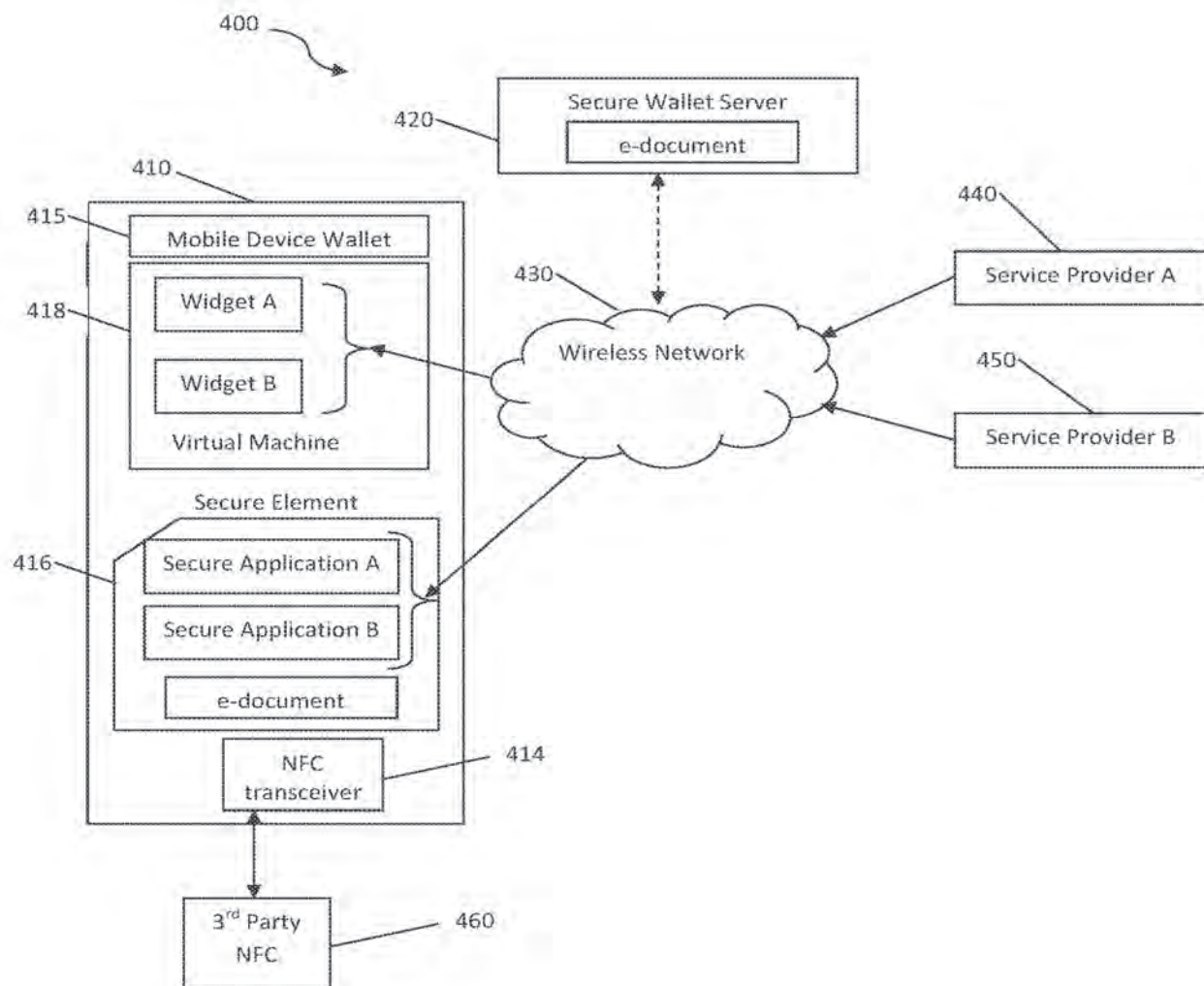


Fig. 4

5/5

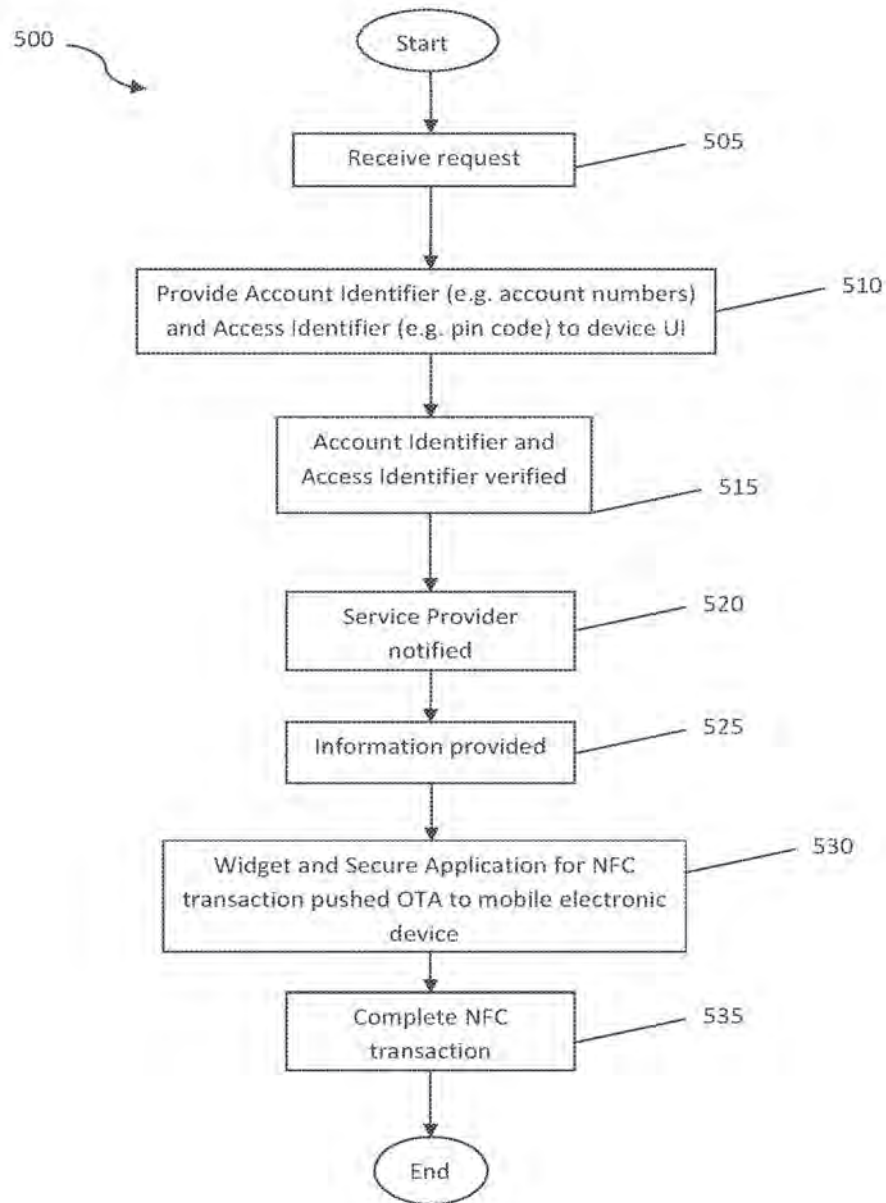


Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IB2014/064439

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W; G06F; H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS,CNABS,CNTXT,CNKI,VEN: identify, identity, identification, ID, digital, wallet, verify, authentication, personal, service, provid+, protect+, privacy, near field communication, NFC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101707772 A (YULONG COMPUTER TELECOM TECHNOLOGY SHENZ) 12 May 2010 (2010-05-12) the whole document	1-20
A	US 2011197267 A1 (GRAVEL VIVIANNE ET AL.) 11 August 2011 (2011-08-11) the whole document	1-20
A	US 2011126010 A1 (ELECTRONICS&TELECOM RES. INST. ET AL.) 26 May 2011 (2011-05-26) the whole document	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

21 January 2015

Date of mailing of the international search report

28 January 2015

Name and mailing address of the ISA/CN

**STATE INTELLECTUAL PROPERTY OFFICE OF THE
P.R.CHINA(ISA/CN)
6,Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088 China**

Facsimile No. (86-10)62019451

Authorized officer

ZHANG,Xin

Telephone No. (86-10)62089567

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/IB2014/064439

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	101707772	A	12 May 2010	None			
US	2011197267	A1	11 August 2011	WO	2011094869	A1	11 August 2011
US	2011126010	A1	26 May 2011	KR	20110056997	A	31 May 2011
				KR	101276201	B1	18 June 2013

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:
 Lotaut, Yacine
 Thales Dis France SA
 Intellectual Property Department
 5 Rue de la Verrerie
 92190 Melun
 FRANCE

REÇU LE
 24 NOV. 2020
 SERVICE INTELLECTUELLE

NOTIFICATION OF TRANSMITTAL OF
 THE INTERNATIONAL SEARCH REPORT AND
 THE WRITTEN OPINION OF THE INTERNATIONAL
 SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing (day/month/year)	20 November 2020 (20-11-2020)
Applicant's or agent's reference GMT4119 WO/YL / 51	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/EP2020/076905	International filing date (day/month/year) 25 September 2020 (25-09-2020)
Applicant THALES DIS FRANCE SA	

- ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.
Filing of amendments and statement under Article 19:
 The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 40).
When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.
How? Directly to the International Bureau preferably through ePCT, or on paper to:
 The International Bureau of WIPO, 34 chemin des Colombettes, 1211 Geneva 20, Switzerland
 For more detailed instructions, see the *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.
- ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.
- ☐ With regard to any protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:
 - ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices;
 - ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.
- Reminders**
 The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. These comments will be made available to the public after international publication. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established.
 Shortly after the expiration of 18 months from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90bis.1 and 90bis.3).
 Within 19 months from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later); otherwise, the applicant must, within 28 months from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices; in respect of other designated Offices, the time limit of 30 months (or later) will apply even if no demand is filed within 19 months. For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.
 Within 22 months from the priority date, the applicant may request that a supplementary international search be carried out by a different International Searching Authority that offers this service (Rule 45bis.1). The procedure for requesting supplementary international search is described in the *PCT Applicant's Guide*, International Phase, paragraphs 8.006-8.032.

Name and mailing address of the International Searching Authority  European Patent Office, P.B. 5618 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	Authorized officer BERTHON, Claude Tel. +31 (0)70 340-1001
---	--

Form PCT/ISA/220 (revised January 2020)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference GMT4110 WO/YL	FOR FURTHER ACTION see Form PCT/SA/220 as well as, where applicable, item 5 below.	
International application No. PCT/EP2020/076906	International filing date (day/month/year) 25 September 2020 (25-09-2020)	(Earliest) Priority Date (day/month/year) 18 October 2019 (18-10-2019)
Applicant THALES DIS FRANCE SA		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the **language**, the international search was carried out on the basis of:

- ☒ the international application in the language in which it was filed
☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c. ☐ With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2. ☐ Certain claims were found unsearchable (See Box No. II)

3. ☐ Unity of invention is lacking (see Box No. III)

4. With regard to the title,

- ☒ the text is approved as submitted by the applicant
☐ the text has been established by this Authority to read as follows:

5. With regard to the abstract,

- ☒ the text is approved as submitted by the applicant
☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

- a. the figure of the drawings to be published with the abstract is Figure No. 6a
☒ as suggested by the applicant
☐ as selected by this Authority, because the applicant failed to suggest a figure
☐ as selected by this Authority, because this figure better characterizes the invention
b. ☐ none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2020/076906

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06Q50/26 G06Q20/32 G06Q20/36
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q G07G

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPD-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2016/294831 A1 (BORUNDA ADRIAN [US] ET AL) 5 October 2016 (2016-10-06) paragraph [0005] - paragraph [0008] paragraph [0021] - paragraph [0034] figures 1-2	1-16
X	WO 2015/036957 A1 (TORO DEV LTD [CN]) 19 March 2015 (2015-03-19) abstract page 1, line 25 - page 3, line 18 page 6, line 28 - page 13, line 32 figures 1, 2, 3A, 3B	1-16

-/--

☒ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent, but published on or after the international filing date

"L" document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"Z" document member of the same patent family

Date of the actual completion of the international search

12 November 2020

Date of mailing of the international search report

20/11/2020

Name and mailing address of the ISA/

European Patent Office, P.B. 5518 Patentleer 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Nicolì, Félix

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2020/076906

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016/156386 A1 (VAN NIEUWENHUYZE OLIVIER [BE] ET AL) 2 June 2016 (2016-06-02) paragraph [0005] - paragraph [0007] paragraph [0050] - paragraph [0065]; figure 4	1-16
A	EMVCO: "EMV '96 Integrated Circuit Card Application Specification for Payment Systems", EMV, EMVCO vol. 3.1.1 ; Contact 1 July 2006 (2006-07-01), pages 1-62, XP061034511, Retrieved from the Internet: URL:https://www.emvco.com/wp-content/uploads/documents/Emvapp_20090126073328.pdf [retrieved on 2020-01-06] page 15 - page 16	1-16
A	Anonymous: "Thales lance son nouveau portefeuille d'identité numérique - vos documents d'identité accessibles où que vous soyez Thales Group", 29 July 2019 (2019-07-29), pages 1-7, XP055689283, Retrieved from the Internet: URL:https://www.thalesgroup.com/fr/group/journaliste/press_release/thales-lance-son-nouveau-portefeuille-didentite-numerique-vos [retrieved on 2020-04-24] the whole document	1-16

Form PCT/IS/A/210 (continuation of second sheet) (April 2005)

page 2 of 2

INTERNATIONAL SEARCH REPORT

information on patent family members

International application No.

PCT/EP2020/076906

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016294831 A1	06-10-2016	AU 2016242966 A1	26-10-2017
		CA 2981659 A1	06-10-2016
		EP 3278248 A1	07-02-2018
		US 2016294831 A1	06-10-2016
		WO 2016161272 A1	06-10-2016
WO 2015036957 A1	19-03-2015	EP 3044902 A1	20-07-2016
		US 2015081538 A1	19-03-2015
		WO 2015036957 A1	19-03-2015
US 2016156386 A1	02-06-2016	CN 105657637 A	08-06-2016
		CN 205029877 U	10-02-2016
		FR 3029324 A1	03-06-2016
		US 2016156386 A1	02-06-2016

TITLE: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON
MOBILE DEVICES

APPLICANT: THALES DIS FRANCE SA

IPC CLASSIFICATION: G06Q50/26, G06Q20/32, G06Q20/36

EXAMINER: Nicoli, Félix

CONSULTED DATABASES: WPI, NPL

CLASSIFICATION SYMBOLS DEFINING EXTENT OF THE SEARCH:

IPC:

CPC: G06Q20/3227, G06Q20/363, G06Q50/265

FI/F-TERMS:

KEYWORDS OR OTHER ELEMENTS FEATURING THE INVENTION:

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43bis.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.
PCT/EP2020/076906

International filing date (day/month/year)
25.09.2020

Priority date (day/month/year)
18.10.2019

International Patent Classification (IPC) or both national classification and IPC
INV. G06Q50/26 G06Q20/32 G06Q20/36

Applicant
THALES DIS FRANCE SA

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1 bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:



European Patent Office
P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk - Pays Bas
Tel. +31 70 340 - 2040
Fax: +31 70 340 - 3016

Date of completion of
this opinion

see form
PCT/ISA/210

Authorized Officer:

Nicoll, Félix

Telephone No. +31 70 340-0



WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/EP2020/076906

Box No. 1 Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:
 - ☒ the international application in the language in which it was filed.
 - ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).
2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:
 - a. ☐ forming part of the international application as filed:
 - ☐ in the form of an Annex C/ST.25 text file.
 - ☐ on paper or in the form of an image file.
 - b. ☐ furnished together with the international application under PCT Rule 13ter.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.
 - c. ☐ furnished subsequent to the international filing date for the purposes of international search only:
 - ☐ in the form of an Annex C/ST.25 text file (Rule 13ter.1(a)).
 - ☐ on paper or in the form of an image file (Rule 13ter.1(b) and Administrative Instructions, Section 713).
4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/EP2020/076906

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	<u>1-16</u>
	No: Claims	
Inventive step (IS)	Yes: Claims	
	No: Claims	<u>1-16</u>
Industrial applicability (IA)	Yes: Claims	<u>1-16</u>
	No: Claims	

2. Citations and explanations

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

1 Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1.1 Reference is made to the following documents:

D1 US 2016/294831 A1 (BORUNDA ADRIAN [US] ET AL) 6 October 2016 (2016-10-06)

D2 WO 2015/036957 A1 (TORO DEV LTD [CN]) 19 March 2015 (2015-03-19)

D3 US 2016/158386 A1 (VAN NIEUWENHUYZE OLIVIER [BE] ET AL) 2 June 2016 (2016-06-02)

EMVCO: "EMV '96 Integrated Circuit Card Application Specification for Payment Systems",
EMV, EMVCO

D4 vol. 3.1.1 ; Contact 1 July 2006 (2006-07-01), pages 1-62, XP061034511,
Retrieved from the Internet:
URL:https://www.emvco.com/wp-content/uploads/documents/Emvapp_20090126073328.pdf
[retrieved on 2020-01-06]

Anonymous: "Thales lance son nouveau portefeuille d'identité numérique - vos documents d'identité accessibles où que vous soyez | Thales Group",
, 29 July 2019 (2019-07-29), pages 1-7, XP055689283,
D5 Retrieved from the Internet:
URL:https://www.thalesgroup.com/fr/group/journaliste/press_release/thales-lance-son-nouveau-portefeuille-didentite-numerique-vos
[retrieved on 2020-04-24]

2 The subject-matter of claim 16 not deemed to be inventive in the sense of Article 33(3) PCT for the following reasons:

2.1 Claim 16 reads:

2.2 A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

associating a security policy with each of a plurality of supported namespaces on a mobile device;

transmitting the security policy of each of the plurality of supported namespaces to a read-

er connected to a verifier;

selecting, by the reader, at least one of the namespaces as candidate namespaces, and transmitting from the reader to the mobile device, a list containing the candidate namespaces;

transmitting to the reader by the mobile device, the security policy associated with each of the selected candidate namespaces;

operating the reader to:

determine for which of the candidate namespaces the reader can satisfy the security policy of the namespace; and

if the verifier can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the verifier terminal can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the mobile device; if the verifier cannot satisfy the security policy of any of the candidate namespaces, rejecting access to the data item; and

upon successful demonstration by the reader to the mobile device of satisfaction of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

2.2.1 The scheme underlying present claim 16 is as follows:

A method for managing security policies for data items of a user, comprising:

associating a security policy with each of a plurality of supported namespaces on a mobile device;

transmitting the security policy of each of the plurality of supported namespaces to a service provider

selecting, by the service provider, at least one of the namespaces as candidate namespaces, and transmitting from service provider to the user, a list containing the candidate namespaces;

transmitting to the service by the user, the security policy associated with each of the selected candidate namespaces;

the service provider performs the following steps:

determines for which of the candidate namespaces the reader can satisfy the security policy of the namespace; and

if the service can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the service provider can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the user;

if the verifier cannot satisfy the security policy of any of the candidate namespaces, abandoning access to the data and

upon successful demonstration by the service provider to the user of satisfaction of the security policy of the selected namespace, granting access to the data item by the user to the service provider.

Basically, a user wishes to access a service for which he/she needs to provide identification information. The user can provide several sorts of identification information but each information needs an accreditation level to be consulted. The service provider aware of its own level of accreditation selects the user identification information it may use to check for allowing or disallowing access to the requested service. If the service provider does not have a sufficient level of accreditation level for any of the user identification information, it abandons its request and the user cannot access to the initially requested service.

A security policy is understood as a required level of accreditation and a namespace as a category/kind of user identification information.

Thus, such a scheme is deemed to be an administrative scheme for checking the legitimacy of a user to access a service (Is he/she old enough to buy alcohol ? for example); such a scheme is not relevant for assessing inventive step.

- 2.2.2 When considering the wording of this claim, the only technical features appear to be a mobile device with a digital wallet in communication with a reader. Any other feature is deemed to relate to an administrative step. The non-technical features do not interact with the identified technical features to produce a further technical effect.
- 2.3 In view of the claim, the closest prior art appears to be a mobile phone including a digital wallet storing personal user information which can be accessed by a reader. Such a system was well-known in art at the priority date of the application as this is shown for instance in D1 and D2 (see the citations in the search report).
- 2.4 The only apparent technical problem appears then to reside in the implementation of the considered administrative scheme (see item 2.2.1) when starting from the identified closest prior art (see item 2.3). The skilled person made aware of such a scheme would implement it as a routine activity at the level defined in the claims.
- 2.5 Hence, claim 16 is not inventive, Article 33(3) PCT.
- 3 The subject-matter of claims 1-10 corresponds to a large extent to the subject-matter of claim 16 such that the objections, under Article 33(3) PCT, raised against claim 16 also apply to present claims 1-10. Claims 1-10 are not inventive in the sense of Article 33(3) PCT for the following reasons:
- 3.1 Claims 1 and 5 are not inventive for the reasons raised against claim 16.

It is also noted that the concept of namespace used to characterize a family of information is also a well-known principle. The use of such a principle for user identity information cannot be deemed to be inventive.

- 3.2 The definition of level confidence for namespaces is an administrative step which appears merely to define, for instance, that a passport may be more trustworthy than a club member card. The use of blacklists or whitelists for expressing such a confidence cannot be deemed inventive. The overhead associated with a security policy is understood as the capacity of a service provider to demonstrate a sufficient level of accreditation; this is also at such level of definition an administrative criteria. Thus, claims 2 and 9 are not inventive, Article 33(3) PCT.
- 3.3 Manual selection of a namespace by a user representing the service provider is a mere matter of choice. The use of a user interface for that purpose is obvious to the skilled person. Thus, claim 3 is not inventive, Article 33(3) PCT.
- 3.4 The filtering out of namespaces merely materialises that the user selects which identity information she/he accepts to disclose for a given purpose. This is a non-technical choice which would be implemented as a routine activity at the level of definition of the claim 4. Thus, claim 4 is not inventive, Article 33(3) PCT.
- 3.5 Claims 6 and 7 are mere implementation choices relating the provision of policy information and the required authentication levels from a service provider. Thus, claims 6 and 7 are not inventive, Article 33(3) PCT.
- 3.6 Claim 10 defines obvious implementation choices. Thus, claim 10 is not inventive, Article 33(3) PCT.
- 3.7 Thus, claims 1-10 are not deemed to be inventive, Article 33(3) PCT.
- 4 Claim 11, 13-15 are not inventive in the sense of Article 33(3) PCT for substantially the reasons raised against claims 1, 4-6.
- 4.1 Claim 12 appears to define that the service provider may request to be made aware of the nature of the identity information that may be used from the wallet. It is noted that such a disclosure of wallet possibilities is a well-known principle as this is exemplified by digital wallets including payment applications which are communicated to a reader -see D4 (see the citations in the search report). The mere use of such a well-known principle for a digital wallet including user identity information cannot be deemed to be inventive. Thus, claim 12 is not inventive, Article 33(3) PCT.

5 Re Item VII

Certain defects in the international application

- 5.1 It appears that all features of claim 1 are included in present claim 16 such that claim 16 should be made dependent on claim 1, Rule 6 PCT.

6 **Re Item VIII**

Certain observations on the international application

6.1 The application does not meet the requirements of Article 6 PCT, because claims 2-4, 7, 8 and 10 are not clear for the following reasons:

6.1.1 Claim 2 depends on claim 1 and defines "the verifier module" and "the verifier"; no antecedent for these features can be found in claim 1.

A similar objection also applies to claims 3, 4, 8 and 10 which may all depend on claim 1 and define features such as "the verifier module", "the verifier", the "verifier terminal" which cannot be found in claim 1.

6.1.2 Claim 7 depends on claim 1 and defines "the required authentication"; no antecedent for this feature can be found in claim 1.

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO/ISA)

General information

For all international applications, the competent International Searching Authority (ISA) will establish an international search report (ISR) accompanied by a written opinion of the International Searching Authority (WO/ISA). The WO/ISA may be responded to by

- filing informal comments with the International Bureau of WIPO (IB) (where no demand for international preliminary examination (demand) is filed)
- filing amendments under Art. 19 PCT (this can be done whether or not a demand is filed)
- filing amendments under Art. 34 PCT and/or formal observations in response to objections raised in the WO/ISA (where a demand is actually filed)

This document explains these possibilities.

Filing informal comments

After receipt of the ISR and WO/ISA, the applicant may file informal comments on the WO/ISA, directly with the IB (see International Search and Preliminary Examination Guidelines 2.15). These will be communicated to the designated/elected Offices, together with the International Preliminary Report on Patentability (IPRP) at 30 months from the priority date.

Amending claims under Art. 19 PCT

The applicant may file amended claims under Art. 19 PCT, directly with the IB by the later of the following dates:

- 2 months from the date of mailing of the ISR and the WO/ISA
- 16 months from the priority date

However, any such amendment received by the IB after the expiration of the applicable time limit shall be **considered to have been received on time** by the IB, if it reaches it **before** the technical preparations for international publication have been completed (the 15th day prior to the date of publication, see PCT Applicant's Guide, International Phase, 9.013).

For further information, please see Rule 46 PCT as well as form PCT/ISA/220.

Please also note that, when filing amended claims under Art. 19 PCT, such amendments shall be **accompanied by a letter** identifying the amendments made and also the basis for the amendments in the application as originally filed (Rule 46.5(b) PCT). Where a **demand** is filed, failure to comply with this requirement may result in the amendments being ignored in the International Preliminary Examination Report (IPER), see Rule 70.2(c-bis) PCT.

Bitte beachten Sie, dass angeführte Nichtpatentliteratur (wie z. B. wissenschaftliche oder technische Dokumente) je nach geltendem Recht dem Urheberrechtsschutz und/oder anderen Schutzarten für schriftliche Werke unterliegen könnte. Die Vervielfältigung urheberrechtlich geschützter Texte, ihre Verwendung in anderen elektronischen oder gedruckten Publikationen und ihre Weitergabe an Dritte ist ohne ausdrückliche Zustimmung des Rechtsinhabers nicht gestattet.

Veuillez noter que les ouvrages de la littérature non-brevets qui sont cités, par exemple les documents scientifiques ou techniques, etc., peuvent être protégés par des droits d'auteur et/ou toute autre protection des écrits prévue par les législations applicables. Les textes ainsi protégés ne peuvent être reproduits ni utilisés dans d'autres publications électroniques ou imprimées, ni rediffusés sans l'autorisation expresse du titulaire du droit d'auteur.

Please be aware that cited works of non-patent literature such as scientific or technical documents or the like may be subject to copyright protection and/or any other protection of written works as appropriate based on applicable laws. Copyrighted texts may not be copied or used in other electronic or printed publications or re-distributed without the express permission of the copyright holder.

XS CPRTENRDE

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92*bis*.1 and
Administrative Instructions, Section 422)

To:

LOTAUT, Yacine
THALES DIS FRANCE SAS
Intellectual Property Department
6 Rue de la Verrerie
92190 MEUDON
FRANCE

Date of mailing (<i>day/month/year</i>) 28 October 2021 (28.10.2021)													
Applicant's or agent's file reference GMT4110 WO/YL		IMPORTANT NOTIFICATION											
International application No. PCT/EP2020/076906		International filing date (<i>day/month/year</i>) 25 September 2020 (25.09.2020)											
1. The following indications appeared on record concerning: ☒ the applicant ☐ the inventor ☐ the agent ☐ the common representative													
Name and Address THALES DIS FRANCE SA 6, rue de la Verrerie 92190 MEUDON FRANCE		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px; text-align: center;">State of Nationality FR</td> <td style="width: 50%; padding: 5px; text-align: center;">State of Residence FR</td> </tr> <tr> <td colspan="2" style="padding: 5px;">Telephone No.</td> </tr> <tr> <td colspan="2" style="padding: 5px;">Facsimile No.</td> </tr> <tr> <td colspan="2" style="padding: 5px;">E-mail address</td> </tr> </table>		State of Nationality FR	State of Residence FR	Telephone No.		Facsimile No.		E-mail address			
State of Nationality FR	State of Residence FR												
Telephone No.													
Facsimile No.													
E-mail address													
2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning: ☒ the person ☐ the name ☐ the address ☐ the nationality ☐ the residence													
Name and Address THALES DIS FRANCE SAS 6, rue de la Verrerie 92190 MEUDON FRANCE		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px; text-align: center;">State of Nationality FR</td> <td style="width: 50%; padding: 5px; text-align: center;">State of Residence FR</td> </tr> <tr> <td colspan="2" style="padding: 5px;">Telephone No.</td> </tr> <tr> <td colspan="2" style="padding: 5px;">Facsimile No.</td> </tr> <tr> <td colspan="2" style="padding: 5px;">E-mail address</td> </tr> <tr> <td colspan="2" style="padding: 5px;"> ☐ Notifications by e-mail authorized </td> </tr> </table>		State of Nationality FR	State of Residence FR	Telephone No.		Facsimile No.		E-mail address		☐ Notifications by e-mail authorized	
State of Nationality FR	State of Residence FR												
Telephone No.													
Facsimile No.													
E-mail address													
☐ Notifications by e-mail authorized													
3. Further observations, if necessary:													
4. A copy of this notification has been sent to: <div style="display: flex; justify-content: space-between;"> <div> ☒ the receiving Office ☐ the International Searching Authority ☐ the Authority (ies) specified for supplementary search </div> <div> ☐ the International Preliminary Examining Authority ☒ the designated Offices concerned ☐ the elected Offices concerned ☐ other: </div> </div>													
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland		Authorized officer: <div style="text-align: right; font-weight: bold;">Blanc Veronique</div> e-mail pct.team5@wipo.int Telephone No. +41 22 338 74 05											

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		
First Named Inventor/Applicant Name:		Mourad FAHER		
Filer:		Marc Andre Boillot/GHEZALI Djouher		
Attorney Docket Number:		GMT4110US/WO MQ/MB		
Filed as Large Entity				
Filing Fees for U.S. National Stage under 35 USC 371				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
NATIONAL STAGE FEE	1631	1	320	320
NATL STAGE SEARCH FEE - REPORT PROVIDED	1642	1	540	540
NATIONAL STAGE EXAM - ALL OTHER CASES	1633	1	800	800
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1660

Electronic Acknowledgement Receipt	
EFS ID:	45415500
Application Number:	17767153
International Application Number:	PCT/EP2020/076906
Confirmation Number:	2044
Title of Invention:	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
First Named Inventor/Applicant Name:	Mourad FAHER
Customer Number:	180929
Filer:	Marc Andre Bollot/GHEZALI Djouher
Filer Authorized By:	Marc Andre Boillot
Attorney Docket Number:	GMT4110US/WO MQ/MB
Receipt Date:	07-APR-2022
Filing Date:	
Time Stamp:	12:35:52
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	\$1660
RAM confirmation Number	E202247C36281394
Deposit Account	604092
Authorized User	GHEZALI Djouher
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <p>37 CFR 1.21 (Miscellaneous fees and charges)</p> <p>37 CFR 1.492 (National application filing, search, and examination fees)</p>	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	GMT4110US_APP_TRANS_371.pdf	339694	no	4
			60494a6c1e211057060f35971c3a80de625f630a3b		
Warnings:					
Information:					
2	Application Data Sheet	GMT4110US_APPL_ADSh.pdf	1256410	no	8
			26726a9921c089a4c379228f1064a3380a4e7c16		
Warnings:					
Information:					
3	Internet Communications Authorized	GMT4110US_APPL_AUTH_INTERNET_COM.pdf	90621	no	2
			0ce8c62f030f0a7c7e8a39c614b0d15aa0f63276		
Warnings:					
Information:					
4	Authorization for Extension of Time all replies	GMT4110US_Gen_Auth_Petition_Extension.pdf	51381	no	1
			91c5ef0a37e0074cc0d5ec35b050a03e0e9871		
Warnings:					
Information:					
5	Power of Attorney	GMT4110US_APPL_GEN_POA.pdf	366805	no	3
			9200518f05f3d076f44baff54039d0345120135		
Warnings:					
Information:					
6	Oath or Declaration filed	GMT4110US_Signed_Comb_Decl_Assignment.pdf	3720746	no	6
			f0ac87110a935c8615925d01375bcbdc39dc0401		
Warnings:					
Information:					

7	Assignee showing of ownership per 37 CFR 3.73	GMT4110US_STATE_37CFR.pdf	124602 b1d336983d5647ea11c9945cd182d2c0106c19	no	3
Warnings:					
Information:					
8		GMT4110US_Preliminary_Amendment.pdf	51180 62031a20ac571a70ba026c985355c13f9917c0f94c	yes	10
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Preliminary Amendment		1	1	
	Claims		2	6	
	Preliminary Amendment		7	8	
	Abstract		9	9	
	Applicant Arguments/Remarks Made in an Amendment		10	10	
Warnings:					
Information:					
9	Specification	GMT4110US_Specification.pdf	98020 8bec531c760c22a048f7d9031172ae00cc1919c05	no	17
Warnings:					
Information:					
10	Drawings-only black and white line drawings	GMT4110_Drawings.pdf	570473 d10f02c0d187a622bec0996f6c9e1b0b0d2b83b00	no	9
Warnings:					
Information:					
11	Documents submitted with 371 (National Stage) Applications	GMT4110WO_Intl_Publication.pdf	1608622 18011f1a60141f0c5d60b29eac747162d511485c0	no	34
Warnings:					
Information:					

12	Information Disclosure Statement (IDS) Form (SB08)	GMT4110US_APPL_IDS.pdf	1035384	no	4
			7947.0b60240f5f96c1ba2d90480907d6603ed1		
Warnings:					
Information:					
13	Foreign Reference	D2_WO2015036957A1.pdf	1438259	no	32
			1415ae5f2a669903a16840b6459692c765ff0f801		
Warnings:					
Information:					
14	Non Patent Literature	D4_XP061034511.pdf	2118067	no	62
			59c54054c09b05601113d089c6088ce112b0a76		
Warnings:					
Information:					
15	Non Patent Literature	D5_XP055689283.pdf	370989	no	7
			ac3be13f662b779d84789f171aeed42bfe2f10064b		
Warnings:					
Information:					
16	Documents submitted with 371 (National Stage) Applications	GMT4110WO_ISR.pdf	950434	no	16
			7a1ec110c1b286a1c9945c5e971c2a1d6158109e2		
Warnings:					
Information:					
17	Documents submitted with 371 (National Stage) Applications	GMT4110WO_PCT_FormI8306.pdf	41911	no	1
			4534d355e113e9498f57c023ee1c1b3ae628f0d80		
Warnings:					
Information:					
18	Fee Worksheet (SB06)	fee-info.pdf	44317	no	2
			5a1ff103b08990d09c20019ed221e02afdea72ed		
Warnings:					
Information:					
Total Files Size (in bytes):			14277915		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371		Attorney Docket No. GMT4110US/WO MQ/MB
		U.S. Application No. (if known, see 37 CFR 1.5)
International Application No. PCT/EP2020/076906	International Filing Date September 25 2020	Priority Date Claimed October 18 2019
Title of Invention SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		
First Named Inventor Mourad FAHER		
<p>Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information.</p> <p>1. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). NOTE: The express request under 35 U.S.C. 371(f) will not be effective unless the requirements under 35 U.S.C. 371(c)(1), (2), and (4) for payment of the basic national fee, copy of the International Application and English translation thereof (if required), and the oath or declaration of the inventor(s) have been received.</p> <p>2. ☒ A copy of the International Application (35 U.S.C. 371(c)(2)) is attached hereto (not required if the International Application was previously communicated by the International Bureau or was filed in the United States Receiving Office (RO/US)).</p> <p>3. An English language translation of the International Application (35 U.S.C. 371(c)(2))</p> <p>a. ☐ is attached hereto.</p> <p>b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).</p> <p>4. An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4))</p> <p>a. ☒ is attached.</p> <p>b. ☐ was previously filed in the international phase under PCT Rule 4.17(iv).</p> <p>Items 5 to 8 below concern amendments made in the international phase.</p> <p><u>PCT Article 19 and 34 amendments</u></p> <p>5. ☐ Amendments to the claims under PCT Article 19 are attached (not required if communicated by the International Bureau) (35 U.S.C. 371(c)(3)).</p> <p>6. ☐ English translation of the PCT Article 19 amendment is attached (35 U.S.C. 371(c)(3)).</p> <p>7. ☐ English translation of annexes (Article 19 and/or 34 amendments only) of the International Preliminary Examination Report is attached (35 U.S.C. 371(c)(5)).</p> <p><u>Cancellation of amendments made in the international phase</u></p> <p>8a. ☐ Do not enter the amendment made in the international phase under PCT Article 19.</p> <p>8b. ☐ Do not enter the amendment made in the international phase under PCT Article 34.</p> <p>NOTE: A proper amendment made in English under Article 19 or 34 will be entered in the U.S. national phase application absent a clear instruction from applicant not to enter the amendment(s).</p> <p>The following items 9 to 17 concern a document(s) or information included.</p> <p>9. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.</p> <p>10. ☒ A preliminary amendment.</p> <p>11. ☒ An Application Data Sheet under 37 CFR 1.76.</p> <p>12. ☐ A substitute specification. NOTE: A substitute specification cannot include claims. See 37 CFR 1.125(b).</p> <p>13. ☒ A power of attorney and/or change of address letter.</p> <p>14. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.3 and 37 CFR 1.821-1.825 (not required if sequence listing in text format was indicated on the PCT Request as part of the International Application and the sequence listing was published as part of the international application).</p> <p>15. ☒ Assignment papers (cover sheet and document(s)). Name of Assignee: <u>THALES DIS FRANCE SAS</u></p> <p>16. ☒ 37 CFR 3.73(c) Statement (when there is an Assignee).</p>		

This collection of information is required by 37 CFR 1.414 and 1.491-1.492. The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 15 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

U.S. APPLN. No. (if known – see 37 CFR 1.5)		INTERNATIONAL APPLICATION No. PCT/EP2020/076906		ATTORNEY DOCKET No. GMT4110US/WO MQ/MB	
17. ☐ Other items or information:					
The following fees have been submitted.					CALCULATIONS
18. ☒ Basic national fee (37 CFR 1.492(a))					\$ 320
19. ☒ Examination fee (37 CFR 1.492(c))					\$ 800
• If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4).....					\$ 0
• All other situations					\$ 800
20. ☒ Search fee (37 CFR 1.492(b))					\$ 540
• If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4).....					\$ 0
• Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority					\$ 140
• International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB.....					\$ 540
• All other situations					\$ 700
TOTAL OF 18, 19, and 20 =					\$ 1660
☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing in compliance with 37 CFR 1.821(c) or (e) in an electronic medium or computer program listing in an electronic medium) (37 CFR 1.492(j)).					\$ 0
Fee for each additional 50 sheets of paper or fraction thereof					\$ 420
Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof (round up to a whole number)		RATE	
44	-100 = 0	/ 50 = 0		x \$420	
Surcharge for furnishing any of the search fee, examination fee, or the oath or declaration after the date of commencement of the national stage (37 CFR 1.492(h)).....					\$ 160
CLAIMS		NUMBER FILED	NUMBER EXTRA	RATE	
Total claims		16	- 20 = 0	x \$100	
Independent claims		3	- 3 = 0	x \$480	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)				+ \$860	
Fee for submission of Sequence Listing text file of 300 MB to 800 MB (37 CFR 1.21(o)(1)).....					\$ 1,060
Fee for submission of Sequence Listing text file of more than 800 MB (37 CFR 1.21(o)(2)).....					\$ 10,500
Processing fee for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(i)).....					\$ 140 +
TOTAL OF ABOVE CALCULATIONS =					\$
☐ Applicant asserts small entity status. See 37 CFR 1.27. Fees above are reduced by 1/3.					
☐ Applicant certifies micro entity status. See 37 CFR 1.29. Fees above are reduced by 3/4. Applicant must attach form PTO/SB/15A or B or equivalent.					
TOTAL NATIONAL FEE =					\$
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31).....					\$ 50.00 per property +
TOTAL FEES ENCLOSED =					\$ 1660

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

- a. ☐ A check in the amount of \$ _____ to cover the above fees is enclosed.
- b. ☒ Please charge my Deposit Account No. 604092 in the amount of \$ 1660 to cover the above fees.
- c. ☒ The Director is hereby authorized to charge additional fees which may be required, or credit any overpayment, to Deposit Account No. 604092 as follows:
- i. ☒ any required fee.
- ii. ☐ any required fee except for excess claims fees required under 37 CFR 1.492(d) and (e) and multiple dependent claim fee required under 37 CFR 1.492(f).
- d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.
- ADVISORY:** If filing by EFS-Web, do NOT attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is not recommended and by doing so your credit card information may be displayed via PAIR. To protect your information, it is recommended to pay fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

- ☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013, and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE 1: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

NOTE 2: A U.S. national stage application may not claim priority to the international application of which it is the national phase. The filing date of a U.S. national stage application is the international filing date. See 35 U.S.C. 363.

Correspondence Address

- ☐ The address associated with Customer Number: 180929 OR ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country				Telephone	
Email					

Signature	/Marc BOILLLOT/	Date	April 7 2022
Name (Print/Type)	Marc BOILLLOT	Registration No. (Attorney/Agent)	56164

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	GMT4110US/WO MQ/MB
		Application Number	
Title of Invention	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.</p> <p>This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor	1				Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	Mourad		FAHER			
Residence Information (Select One) US Residency ☐ Non US Residency Active US Military Service						
City	MARLY LE ROI		Country of Residence ⁱ	FR		
Mailing Address of Inventor:						
Address 1		THALES DIS FRANCE SAS - IP Department				
Address 2		6, rue de la Verrerie				
City	MEUDON		State/Province			
Postal Code	92190		Country ⁱ	FR		
Inventor	2				Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	Carole		BAYLE			
Residence Information (Select One) US Residency ☒ Non US Residency Active US Military Service						
City	MARSEILLE		Country of Residence ⁱ	FR		
Mailing Address of Inventor:						
Address 1		THALES DIS FRANCE SAS - IP Department				
Address 2		6, rue de la Verrerie				
City	MEUDON		State/Province			
Postal Code	92190		Country ⁱ	FR		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.						
Add						

Correspondence Information:

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	GMT4110US/WO MQ/MB
		Application Number	
Title of Invention	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ An Address is being provided for the correspondence information of this application.

Customer Number	180929		
Email Address	us.intellectualproperty@thalesgroup.com	Add Email	Remove Email
Email Address	marc.boillot@thalesgroup.com	Add Email	Remove Email

Application Information:

Title of the Invention	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		
Attorney Docket Number	GMT4110US/WO MQ/MB	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	9	Suggested Figure for Publication (if any)	6a

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
--------------------	--	--	---

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	GMT4110US/WO MQ/MB
		Application Number	
Title of Invention	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		
Customer Number	180929		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78. When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	a 371 of international	PCT/EP2020/076906	2020-09-25
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Remove
19306357.5	EP	2019-10-18	Access Code ⁱ (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	GMT4110US/WO MQ/MB
		Application Number	
Title of Invention	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	GMT4110US/WO MQ/MB
		Application Number	
Title of Invention	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.			
Applicant	1		<input type="button" value="Remove"/>
<p>If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.</p>			
		<input type="button" value="Clear"/>	
☒ Assignee	Legal Representative under 35 U.S.C. 117		Joint Inventor
Person to whom the inventor is obligated to assign.		Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
<div> <div></div> <div></div> </div>			
Name of the Deceased or Legally Incapacitated Inventor: <input type="text"/>			
If the Applicant is an Organization check here. ☒			
Organization Name	THALES DIS FRANCE SAS		
Mailing Address Information For Applicant:			
Address 1	6, rue de la Verrerie		
Address 2			
City	MEUDON	State/Province	
Country	FR	Postal Code	92190
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button. <input type="button" value="Add"/>			

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	GMT4110US/WO MQ/MB
		Application Number	
Title of Invention	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		

Assignee	1		
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.			
			<input type="button" value="Remove"/>
If the Assignee or Non-Applicant Assignee is an Organization check here.			☒
Organization Name	THALES DIS FRANCE SAS		
Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1	6, rue de la Verrerie		
Address 2			
City	MEUDON	State/Province	
Country i	FR	Postal Code	92190
Phone Number		Fax Number	
Email Address			
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). However, if this Application Data Sheet is submitted with the **INITIAL** filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Marc BOILLOT/		Date (YYYY-MM-DD)	2022-04-07	
First Name	Marc	Last Name	BOILLOT	Registration Number	56164
Additional Signature may be generated within this form by selecting the Add button.				<input type="button" value="Add"/>	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	GMT4110US/WO MQ/MB
		Application Number	
Title of Invention	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: ECOMM.AUTH/ECOMM.WTDW

Doc Description: Internet Communications Authorized/Internet Communications Authorization Withdrawn

PTO/SB/439 (11-15)

AUTHORIZATION FOR INTERNET COMMUNICATIONS IN A PATENT APPLICATION OR REQUEST TO WITHDRAW AUTHORIZATION FOR INTERNET COMMUNICATIONS	Application No.	
	Filing Date	
	First Named Inventor	Mourad FAHER
	Art Unit	
	Examiner Name	
	Practitioner Docket No.	GMT4110US/WO MQ/MB

To: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I. To authorize permission for Internet Communications.

☒ Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with the undersigned and practitioners in accordance with 37 CFR 1.33 and 37 CFR 1.34 concerning any subject matter of this application via video conferencing, instant messaging, or electronic mail. I understand that a copy of these communications will be made of record in the application file. (MPEP 502.03)

II. To withdraw authorization for Internet Communications.

☐ The authorization given on _____, to the USPTO to communicate with the undersigned and any practitioner in accordance with 37 CFR 1.33 and 37 CFR 1.34 concerning any subject matter of this application via Internet communications such as video conferencing, instant messaging, or electronic mail is hereby withdrawn. I understand that the withdrawal is effective when approved rather than when received.

I am the

- ☐ applicant.
- ☒ attorney or agent of record. Registration number 56164
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number _____

/Marc BOILLOT/
Signature

April 7 2022
Date

Marc BOILLOT
Typed or printed name

954-658-0418
Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Juristic entities must be represented by a patent practitioner (see 37 CFR 1.31, which is applicable to any paper filed on or after September 16, 2012, that is presented on behalf of a juristic entity, regardless of application filing date). Submit multiple forms if more than one signature is required, see below*.

☒ * Total of 1 forms are submitted.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



Attorney Docket No. GMT4110US/WO MQ/MB

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

First named Inventor: Mourad FAHER

Application No.: Unassigned

Filing Date: On Even Date Herewith

Title: SECURITY MECANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

**GENERAL AUTHORIZATION FOR PETITIONS
FOR EXTENSIONS OF TIME AND PAYMENT OF FEES**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

The U.S. Patent and Trademark Office is hereby provided with a general authorization to treat any concurrent or future reply requiring a petition for an extension of time for its timely submission, as containing a request therefor for the appropriate length of time, in accordance with 37 C.F.R. § 1.136(a)(3),

The Commissioner is hereby authorized to charge any appropriate fees that may be required by this paper, or any other submissions in this application, and to credit any overpayment, to Deposit Account No.604092.

Respectfully submitted,

Marc BOILLOT

Date: April 7 2022

By: /Marc BOILLOT/
Marc BOILLOT
Registration No. 56164

Customer No. 180929

www.thalesgroup.com

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA/82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	
Filing Date	
First Named Inventor	Mourad FAHER
Title	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
Art Unit	
Examiner Name	
Attorney Docket Number	GMT4110US/WO MQ/MB

SIGNATURE of Applicant or Patent Practitioner

Signature	/Marc BOILLOT/	Date (Optional)	April 7 2022
Name	Marc BOILLOT	Registration Number	56164
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)	THALES DIS FRANCE SAS		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.



*Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

☒ Practitioners associated With Customer Number: 180929

OR

☒ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number
Marc BOILLOT	56164

Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

☐ The address associated with Customer Number:

OR

☐ Firm or individual name		
Address		
City	State	Zip
Country		
Telephone		Email

Assignee name and address: THALES DIS FRANCE SAS - 6, rue de la Verrerie - 92190 MEUDON-FRANCE

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of the practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee.

Signature	Date January 18 2022
Name Benoît JOUFFREY	Telephone
Title Chief Technical Officer (CTO)	

This collection of information is required by 37 CFR 1.31, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public, which is to update (and by the USPTO to process) the file of a patent or reexamination proceeding. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 18 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

COMBINED DECLARATION AND ASSIGNMENT

As the below named inventor(s), I (we) hereby declare that this Combined Declaration and Assignment is directed to:

Case Reference Number	Patent Application Data Official Title	Inventor(s)
GMT4110	<p>US Patent Application N° Filed on</p> <p>and its corresponding International Application pursuant to the PCT/EP2020/076906 filed on September 25, 2020 and based on the priority EP19306357.5 filed on October 18, 2019</p> <p>SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES</p>	<p>BAYLE Carole FAHER Mourad</p>

DECLARATION

- As the below named inventor, I further declare that:
- The above-identified application was made or authorized to be made by me.
- I believe that I am the original inventor of a claimed invention in the application.
- I have reviewed and understand the contents of the above-identified specification, including the claims.
- I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.
- I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

ASSIGNMENT

THIS ASSIGNMENT is made by and between the undersigned inventor (hereinafter referred to as "the Assignor"), and **THALES DIS FRANCE SAS** (hereinafter referred to as "the Assignee"), a corporation duly organized under and pursuant to the laws of France and having a principal place of business at: 6 rue de La Verrerie - 92190 Meudon - France

MF

4/5

WHEREAS, the Assignor has invented certain new and useful improvements set forth in the application for Letters Patent of the United States identified above;

WHEREAS, the Assignee is desirous of acquiring the entire right, title, and interest in and to said inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications, including provisional applications for Letters Patent of the United States or other countries claiming priority to said application, and in and to any Letters Patent or Patents, United States or foreign, to be obtained therefore and thereon.

NOW, THEREFORE, for good and sufficient consideration, the receipt of which is hereby acknowledged, the Assignor has sold, assigned, transferred, and set over, and by these presents does sell, assign, transfer, and set over, unto the Assignee, its successors, legal representatives, and assigns the entire right, title, and interest in and to the above-mentioned inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications for Letters Patent of the United States or other countries claiming priority to said applications, and any and all Letters Patent or Patents of the United States of America and all foreign countries that may be granted therefore and thereon, and in and to any and all applications claiming priority to said applications, divisions, continuations, and continuations-in-part of said applications, and reissues, and re-examinations and extensions of said Letters Patent or Patents, and all rights under the International Convention for the Protection of Industrial Property, the same to be held and enjoyed by the Assignee, for its own use and benefit and the use and benefit of its successors, legal representatives, and assigns, to the full end of the term or terms for which Letters Patent or Patents may be granted as fully and entirely as the same would have been held and enjoyed by the Assignor had this sale and assignment not been made;

AND for the same consideration, the Assignor hereby covenants and agrees to and with the Assignee, its successors, legal representatives, and assigns, that, at the time of execution and delivery of these presents, the Assignor is the sole and lawful owner of the entire right, title, and interest in and to the inventions set forth in said applications and said applications, including provisional applications, above-mentioned, and that the same are unencumbered, and that the Assignor has good and full right and lawful authority to sell and convey the same in the manner herein set forth;

AND for the same consideration, the Assignor hereby covenants and agrees to and with the Assignee, its successors, legal representatives, and assigns that the Assignor will, whenever counsel of the Assignee, or the counsel of its successors, legal representatives, and assigns, shall advise that any proceeding in connection with said inventions or said applications for Letters Patent or Patents, or any proceeding in connection with Letters Patent or Patents for said inventions in any country, including interference proceedings, is lawful and desirable, or that any application claiming priority to said application, division, continuation, or continuation-in-part of any applications for Letters Patent or Patents, or any reissue or extension of any Letters Patent or Patents to be obtained thereon, is lawful and desirable, sign all papers and documents, take all lawful oaths, and do all acts necessary or

MS

21

required to be done for the procurement, maintenance, enforcement, and defense of Letters Patent or Patents for said inventions, without charge to the Assignee, its successors, legal representatives, and assigns, but at the cost and expense of the Assignee, its successors, legal representatives, and assigns;

AND the Assignor hereby requests the Commissioner of Patents to issue any and all said Letters Patent of the United States to the Assignee as the Assignee of said inventions, the Letters Patent to be issued for the sole use and benefit of the Assignee, its successors, legal representatives, and assigns.

INVENTOR(S):

April 4th, 2022
Date

FAHER, Mourad
Name


Signature

Date

BAYLE, Carole
Name

Signature

MF

3/7/2022

COMBINED DECLARATION AND ASSIGNMENT

As the below named inventor(s), I(we) hereby declare that this Combined Declaration and Assignment is directed to:

Case Reference Number	Patent Application Data Official Title	Inventor(s)
GMT4110	US Patent Application N° Filed on and its corresponding International Application pursuant to the PCT/EP2020/076906 filed on September 25, 2020 and based on the priority EP19306357.5 filed on October 18, 2019 SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES	BAYLE Carole FAHER Mourad

DECLARATION

- As the below named inventor, I further declare that:
- The above-identified application was made or authorized to be made by me.
- I believe that I am the original inventor of a claimed invention in the application.
- I have reviewed and understand the contents of the above-identified specification, including the claims.
- I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.
- I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

ASSIGNMENT

THIS ASSIGNMENT is made by and between the undersigned inventor (hereinafter referred to as "the Assignor"), and **THALES DIS FRANCE SAS** (hereinafter referred to as "the Assignee"), a corporation duly organized under and pursuant to the laws of France and having a principal place of business at: 6 rue de La Verrerie - 92190 Meudon - France

WHEREAS, the Assignor has invented certain new and useful improvements set forth in the application for Letters Patent of the United States identified above;

WHEREAS, the Assignee is desirous of acquiring the entire right, title, and interest in and to said inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications, including provisional applications for Letters Patent of the United States or other countries claiming priority to said application, and in and to any Letters Patent or Patents, United States or foreign, to be obtained therefore and thereon.

NOW, THEREFORE, for good and sufficient consideration, the receipt of which is hereby acknowledged, the Assignor has sold, assigned, transferred, and set over, and by these presents does sell, assign, transfer, and set over, unto the Assignee, its successors, legal representatives, and assigns the entire right, title, and interest in and to the above-mentioned inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications for Letters Patent of the United States or other countries claiming priority to said applications, and any and all Letters Patent or Patents of the United States of America and all foreign countries that may be granted therefore and thereon, and in and to any and all applications claiming priority to said applications, divisions, continuations, and continuations-in-part of said applications, and reissues, and re-examinations and extensions of said Letters Patent or Patents, and all rights under the International Convention for the Protection of Industrial Property, the same to be held and enjoyed by the Assignee, for its own use and benefit and the use and benefit of its successors, legal representatives, and assigns, to the full end of the term or terms for which Letters Patent or Patents may be granted as fully and entirely as the same would have been held and enjoyed by the Assignor had this sale and assignment not been made;

AND for the same consideration, the Assignor hereby covenants and agrees to and with the Assignee, its successors, legal representatives, and assigns, that, at the time of execution and delivery of these presents, the Assignor is the sole and lawful owner of the entire right, title, and interest in and to the inventions set forth in said applications and said applications, including provisional applications, above-mentioned, and that the same are unencumbered, and that the Assignor has good and full right and lawful authority to sell and convey the same in the manner herein set forth;

AND for the same consideration, the Assignor hereby covenants and agrees to and with the Assignee, its successors, legal representatives, and assigns that the Assignor will, whenever counsel of the Assignee, or the counsel of its successors, legal representatives, and assigns, shall advise that any proceeding in connection with said inventions or said applications for Letters Patent or Patents, or any proceeding in connection with Letters Patent or Patents for said inventions in any country, including interference proceedings, is lawful and desirable, or that any application claiming priority to said application, division, continuation, or continuation-in-part of any applications for Letters Patent or Patents, or any reissue or extension of any Letters Patent or Patents to be obtained thereon, is lawful and desirable, sign all papers and documents, take all lawful oaths, and do all acts necessary or

required to be done for the procurement, maintenance, enforcement, and defense of Letters Patent or Patents for said inventions, without charge to the Assignee, its successors, legal representatives, and assigns, but at the cost and expense of the Assignee, its successors, legal representatives, and assigns;

AND the Assignor hereby requests the Commissioner of Patents to issue any and all said Letters Patent of the United States to the Assignee as the Assignee of said inventions, the Letters Patent to be issued for the sole use and benefit of the Assignee, its successors, legal representatives, and assigns.

INVENTOR(S):

	FAHER, Mourad	
_____	_____	_____
Date	Name	Signature

	BAYLE, Carole	
_____	_____	_____
Date	Name	Signature

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: THALES DIS FRANCE SAS

Application No./Patent No.: _____ Filed/Issue Date: _____

Titled: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
THALES DIS FRANCE SAS, a Corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.
- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Marc BOILLOT

Signature

/Marc BOILLOT/

Printed or Typed Name

April 7 2022

Date

N°56164

Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

SCORE Placeholder Sheet for IFW Content

Application Number: 17767153

Document Date: 04/07/2022

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access SCORE content via DAV or via the SCORE web page.
- External customers may access SCORE content via PAIR using the Supplemental Content tab.

PCT REQUEST

(Original in Electronic Form)

0	For receiving Office use only	
0-1	International Application No.	PCT/EP2020/076906
0-2	International Filing Date	25 SEP 2020 (25.09.2020)
0-3	Name of receiving Office and "PCT International Application"	RO/EP
0-4	Form PCT/RO/101 PCT Request	
0-4-1	Prepared Using	PCT Online Filing Version 3.51.000.268e MT/FOP 20141031/0.20.5.24
0-5	Petition The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	Receiving Office (specified by the applicant)	European Patent Office (EPO) (RO/EP)
0-7	Applicant's or agent's file reference	GMT4110 WO/YL
I	Title of Invention	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
II	Applicant	
II-1	This person is	Applicant only
II-2	Applicant for	All designated States
II-4	Name	THALES DIS FRANCE SA
II-5	Address	6, rue de la Verrerie 92190 MEUDON France
II-6	State of nationality	FR
II-7	State of residence	FR
III-1	Applicant and/or inventor	
III-1-1	This person is	Inventor only
III-1-3	Inventor for	All designated States
III-1-4	Name (LAST, First)	FAHER, Mourad
III-1-5	Address	THALES DIS FRANCE SA Intellectual Property Department 6 Rue de la Verrerie 92190 MEUDON France

PCT REQUEST

(Original in Electronic Form)

III-2	Applicant and/or inventor	
III-2-1	This person is	Inventor only
III-2-3	Inventor for	All designated States
III-2-4	Name (LAST, First)	BAYLE, Carole
III-2-5	Address	THALES DIS FRANCE SA Intellectual Property Department 6 Rue de la Verrerie 92190 MEUDON France
IV-1	Agent or common representative; or address for correspondence	
	The person identified below is hereby/ has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	Agent
IV-1-1	Name (LAST, First)	LOTAUT, Yacine
IV-1-2	Address	THALES DIS FRANCE SA Intellectual Property Department 6 Rue de la Verrerie 92190 MEUDON France
IV-1-3	Telephone No.	+33 1 55 01 63 98
IV-1-5	e-mail	intellectual.property@thalesgroup.com
IV-1-5(a)	E-mail authorization The receiving Office, the International Searching Authority, the International Bureau and the International Preliminary Examining Authority are authorized to use this e-mail address, if the Office or Authority so wishes, to send notifications issued in respect of this international application:	exclusively in electronic form (no paper notifications will be sent)
V	DESIGNATIONS	
V-1	The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.	
VI-1	Priority claim of earlier regional application	
VI-1-1	Filing date	18 October 2019 (18.10.2019)
VI-1-2	Number	19306357.5
VI-1-3	Regional Office	EP
VI-2	Priority document request	
	The International Bureau is requested to obtain from a digital library a certified copy of the earlier application(s) identified above as item(s), using, where applicable, the access code(s) indicated:	VI-1 Access code: 3977
VI-3	Incorporation by reference : where an element of the international application referred to in Article 11(1)(iii)(d) or (e) or a part of the description, claims or drawings referred to in Rule 20.5(a), or an element or part of the description, claims or drawings referred to in Rule 20.5bis(a) is not otherwise contained in this international application but is completely contained in an earlier application whose priority is claimed on the date on which one or more elements referred to in Article 11(1)(iii) were first received by the receiving Office, that element or part is, subject to confirmation under Rule 20.6, incorporated by reference in this international application for the purposes of Rule 20.6.	

PCT REQUEST

(Original in Electronic Form)

VII-1	International Searching Authority Chosen	European Patent Office (EPO) (ISA/EP)	
VII-2	Request to use results of earlier search; reference to that search		
VII-2-1	Filing date	18 October 2019 (18.10.2019)	
VII-2-2	Application Number	19306357.5	
VII-2-3	Country (or regional Office)	EP	
VII-2-4	Statement (Rule 4.12(ii)):	This international application is the same, or substantially the same, as the application in respect of which the earlier search was carried out except, where applicable, that it is filed in a different language.	
VII-2-6	The applicant requests the receiving Office to prepare and transmit to the ISA a copy of the earlier search results (Rule 12bis.1(b) and (d)).		
VIII	Declarations	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	—	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	—	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	—	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	—	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	—	
IX	Check list	Number of sheets	Electronic file(s) attached
IX-1	Request (including declaration sheets)	4	✓
IX-2	Description	17	✓
IX-3	Claims	4	✓
IX-4	Abstract	1	✓
IX-5	Drawings	9	✓
IX-6a	Sequence listing part of the description (also to be used for the purposes of international search)	—	—
IX-7	TOTAL	35	
	Accompanying items	Paper document(s) attached	Electronic file(s) attached
IX-8	Fee calculation sheet	—	✓
IX-20	Figure of the drawings which should accompany the abstract	6a	
IX-21	Language of filing of the international application	English	

PCT REQUEST

(Original in Electronic Form)

X-1	Signature of applicant, agent or common representative	(PKCS7 Digital Signature)
X-1-1	Name (LAST, First)	LOTAUT, Yacine
X-1-3	Capacity (if such capacity is not obvious from reading the request)	(Representative)

FOR RECEIVING OFFICE USE ONLY

10-1	Date of actual receipt of the purported international application	25 SEP 2020 (25.09.2020)
10-2	Drawings:	✓
10-2-1	Received	
10-2-2	Not received	
10-3	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application	
10-4	Date of timely receipt of the required corrections under PCT Article 11(2)	
10-5	International Searching Authority	ISA/EP
10-6	Transmittal of search copy delayed until search fee is paid	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	Date of receipt of the record copy by the International Bureau	
-------------	--	--



(51) International Patent Classification:

G06Q 50/26 (2012.01) G06Q 20/36 (2012.01)
G06Q 20/32 (2012.01)

(21) International Application Number:

PCT/EP2020/076906

(22) International Filing Date:

25 September 2020 (25.09.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

19306357.5 18 October 2019 (18.10.2019) EP

(71) Applicant: **THALES DIS FRANCE SA** [FR/FR]; 6, rue de la Verrerie, 92190 MEUDON (FR).

(72) Inventors: **FAHER, Mourad**; THALES DIS FRANCE SA, Intellectual Property Department, 6 Rue de la Verrerie, 92190 MEUDON (FR). **BAYLE, Carole**; THALES DIS FRANCE SA, Intellectual Property Department, 6 Rue de la Verrerie, 92190 MEUDON (FR).

(74) Agent: **LOTAUT, Yacine**; THALES DIS FRANCE SA, Intellectual Property Department, 6 Rue de la Verrerie, 92190 MEUDON (FR).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

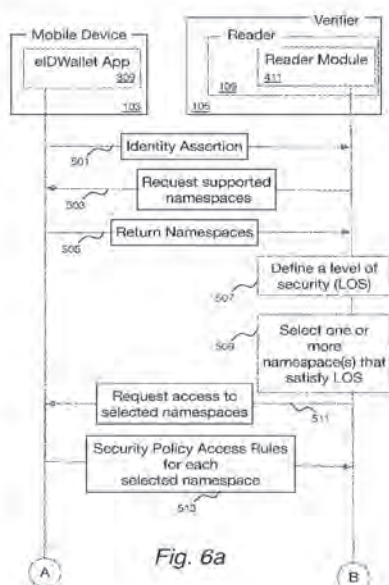


Fig. 6a

(57) Abstract: A system, mobile device, and method for managing security policies for data items stored in an electronic identification (eID) wallet on the mobile device. Security policies are associated with each of a plurality of supported namespaces on a mobile device and a verifier terminal operates to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.

CLAIMS

1. A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

associating security policies with each of a plurality of supported namespaces on a mobile device; and

operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.

2. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device of Claim 1, comprising:

transmitting a list of supported namespaces to the verifier module executing on the verifier; and

selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.

3. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims, comprising:

transmitting a list of supported namespaces to the verifier module; and

selecting, by the verifier module, at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

4. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims further comprising:

prior to transmitting a list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

5. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims, comprising:

transmitting the security policy of each of the plurality of supported namespaces from the mobile device to the reader.

6. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

7. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims wherein the required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

8. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims further comprises operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier associates with each namespace in the plurality of supported namespaces.

9. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims further comprises operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

10. The method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims wherein the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory, the method further comprising operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.

11. A mobile device comprising:
a processor; and
a memory for storing instructions executable by the processor and for storing electronic identity (eID) data, the memory including an eID wallet application having instructions to cause the processor to:
receive a list of selected namespaces from a reader;
in response to receiving the list of selected namespaces from the reader, transmitting security rules associated with each selected namespace according to a defined bytestring template.

12. The mobile device of claim 10, wherein the eID wallet application further comprises instruction to cause the processor to;
receive a request for supported namespaces from a reader;
transmit a list of supported name spaces to the reader.

13. The mobile device according to claims 11 to 12, wherein the eID wallet application further comprises instruction to cause the processor to;
prior transmitting a list of supported namespaces to a reader, filter out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the reader.

14. The mobile device according to claims 11 to 13, wherein the eID wallet application further comprises instruction to cause the processor to;
transmit the security policy of each of the plurality of supported namespaces to a reader connected to a verifier.

15. The mobile device according to claims 11 to 12, wherein the eID wallet application wherein the security policy is transmitted as a sequence of bytes

having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

16. A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

- associating a security policy with each of a plurality of supported namespaces on a mobile device;

- transmitting the security policy of each of the plurality of supported namespaces to a reader connected to a verifier;

- selecting, by the reader, at least one of the namespaces as candidate namespaces, and transmitting from the reader to the mobile device, a list containing the candidate namespaces;

- transmitting to the reader by the mobile device, the security policy associated with each of the selected candidate namespaces;

- operating the reader to:

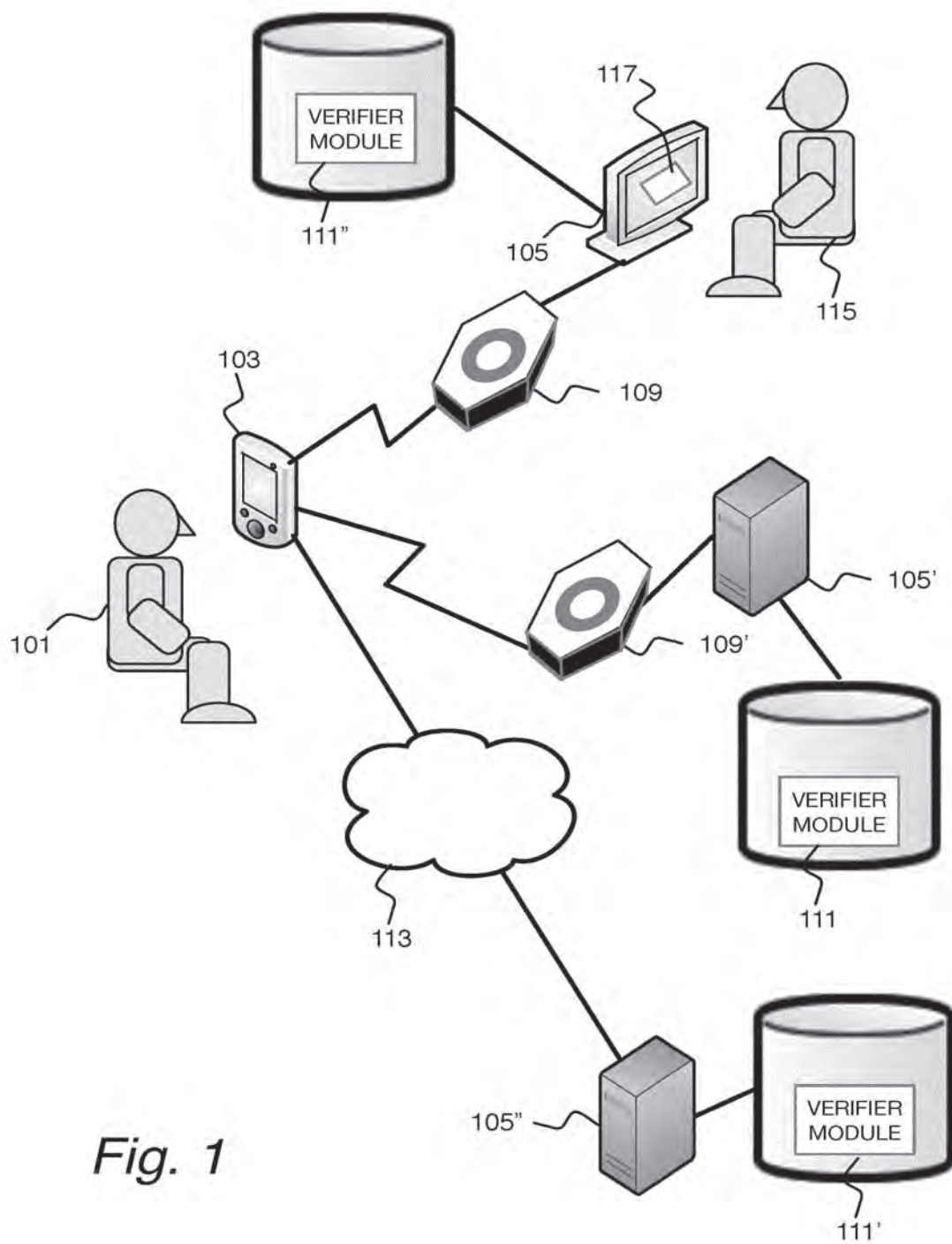
- determine for which of the candidate namespaces the reader can satisfy the security policy of the namespace; and

- if the verifier can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the verifier terminal can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the mobile device;

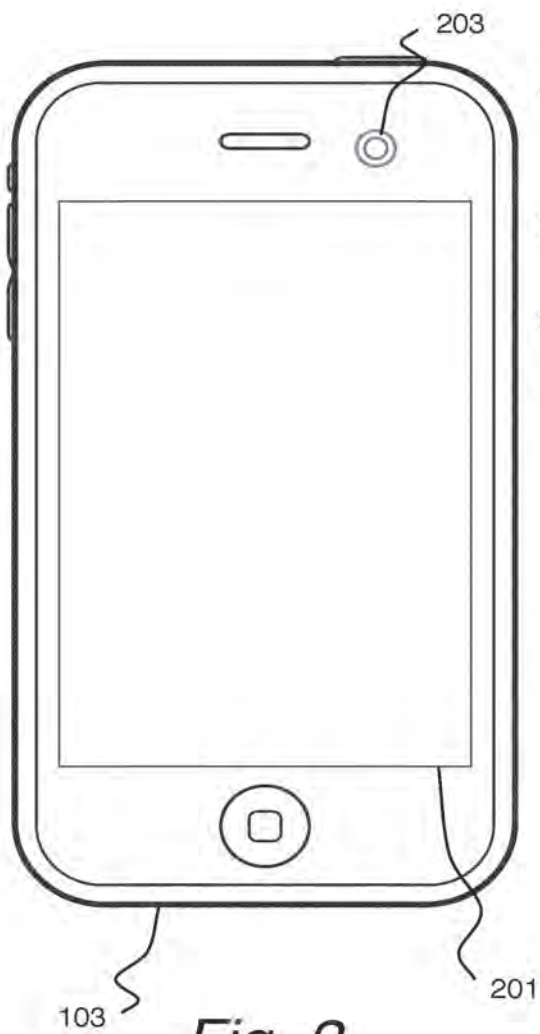
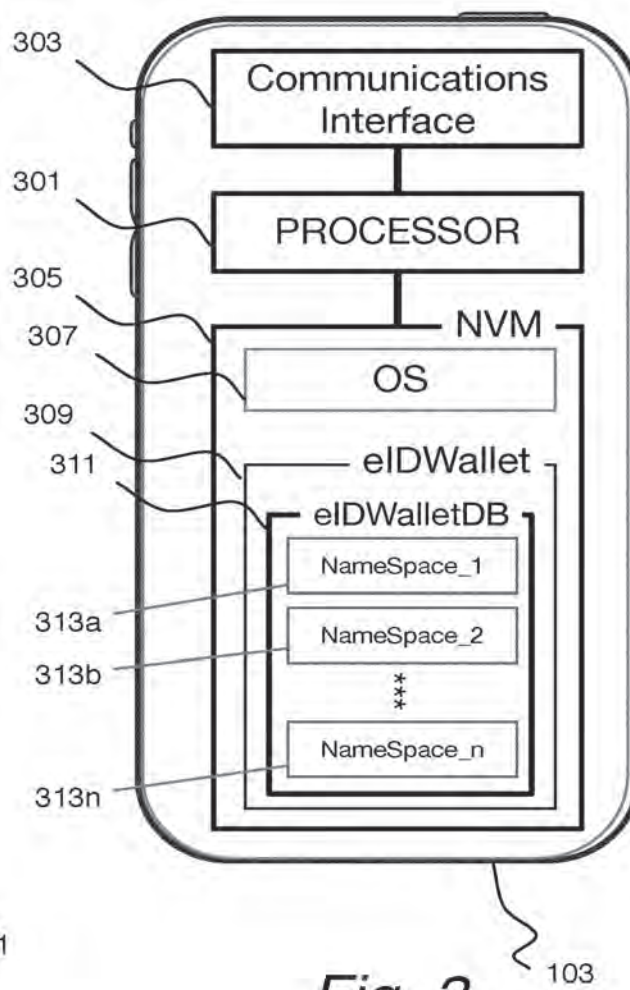
- if the verifier cannot satisfy the security policy of any of the candidate namespaces, rejecting access to the data item; and

- upon successful demonstration by the reader to the mobile device of satisfaction of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

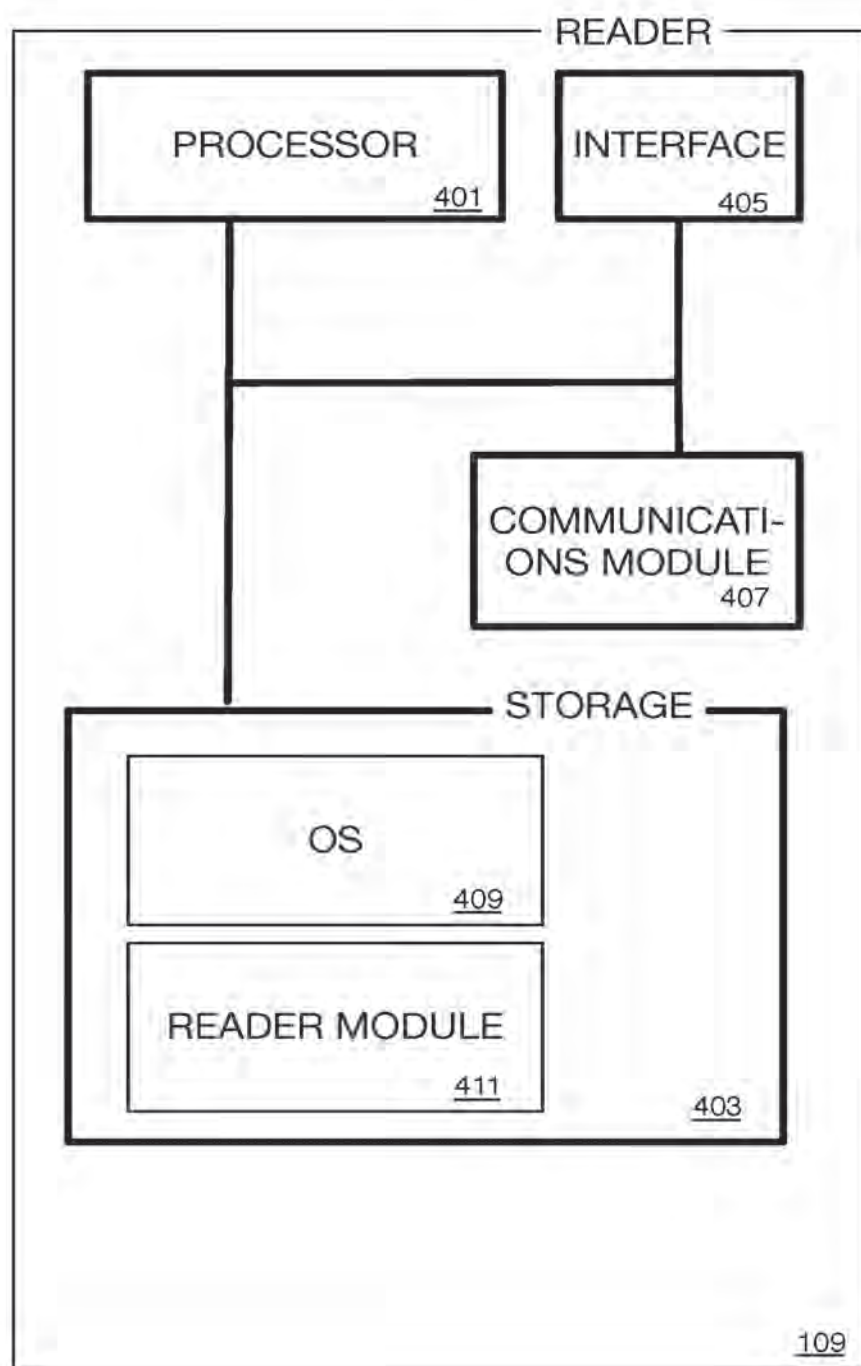
1/9

*Fig. 1*

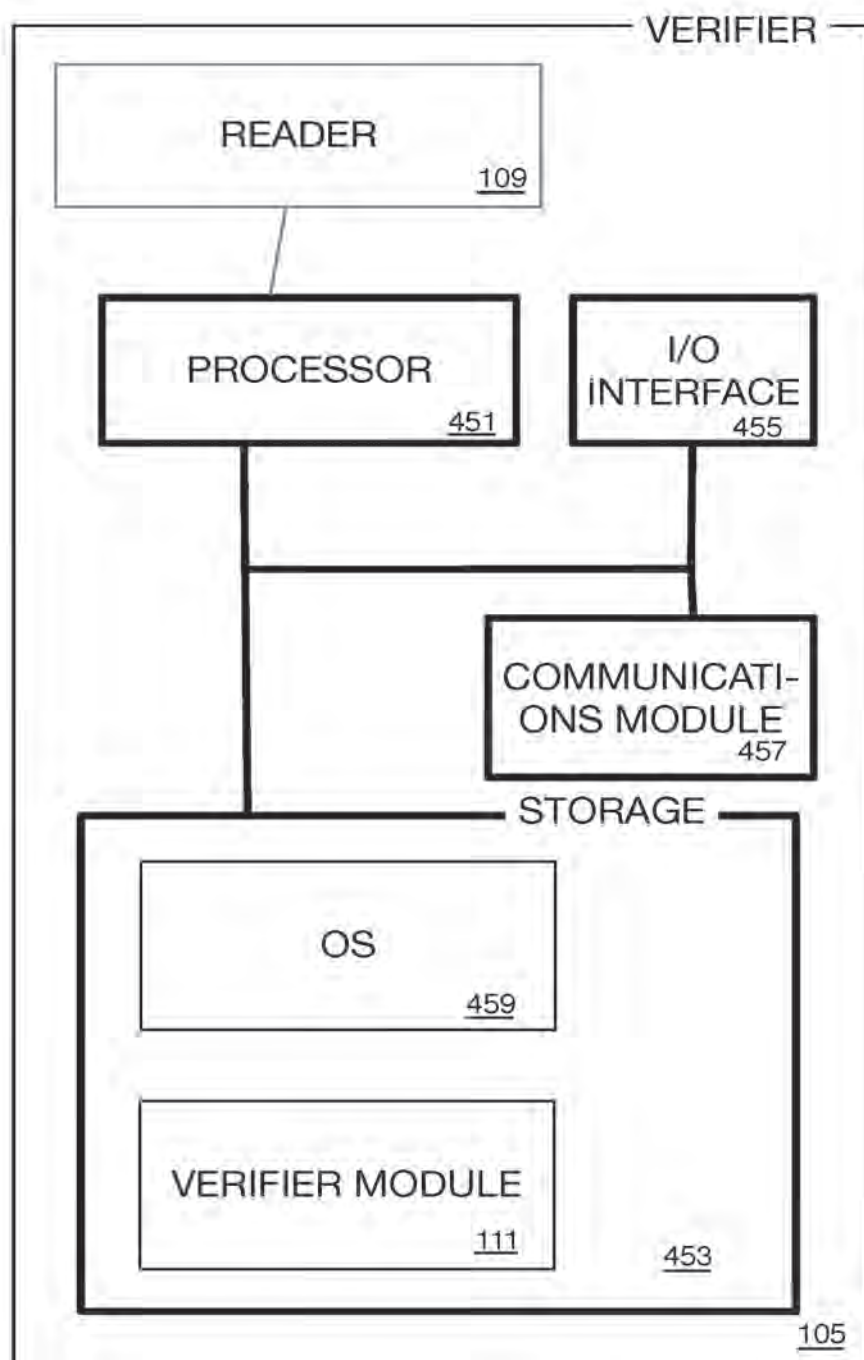
2/9

*Fig. 2**Fig. 3*

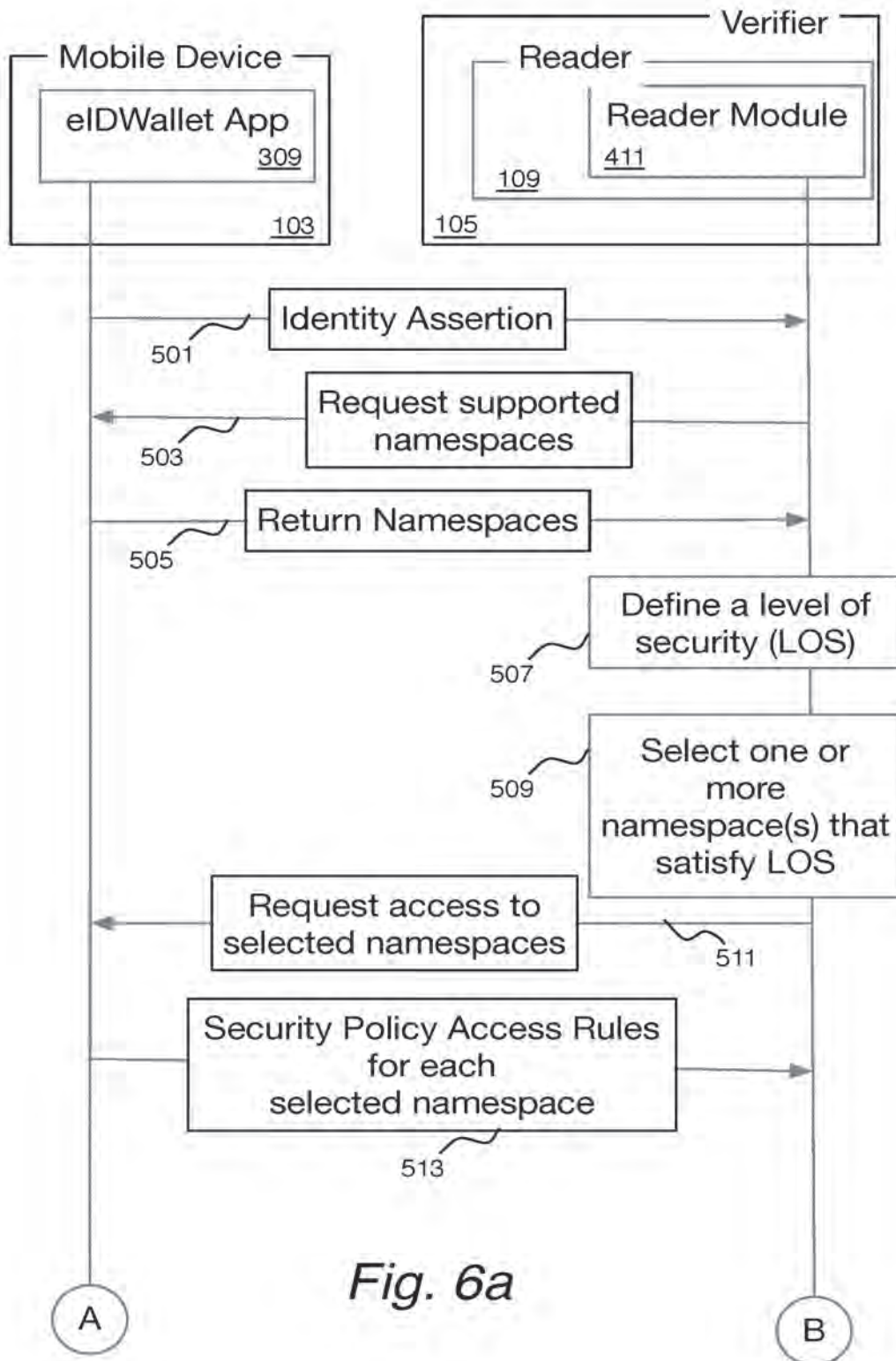
3/9

*Fig. 4*

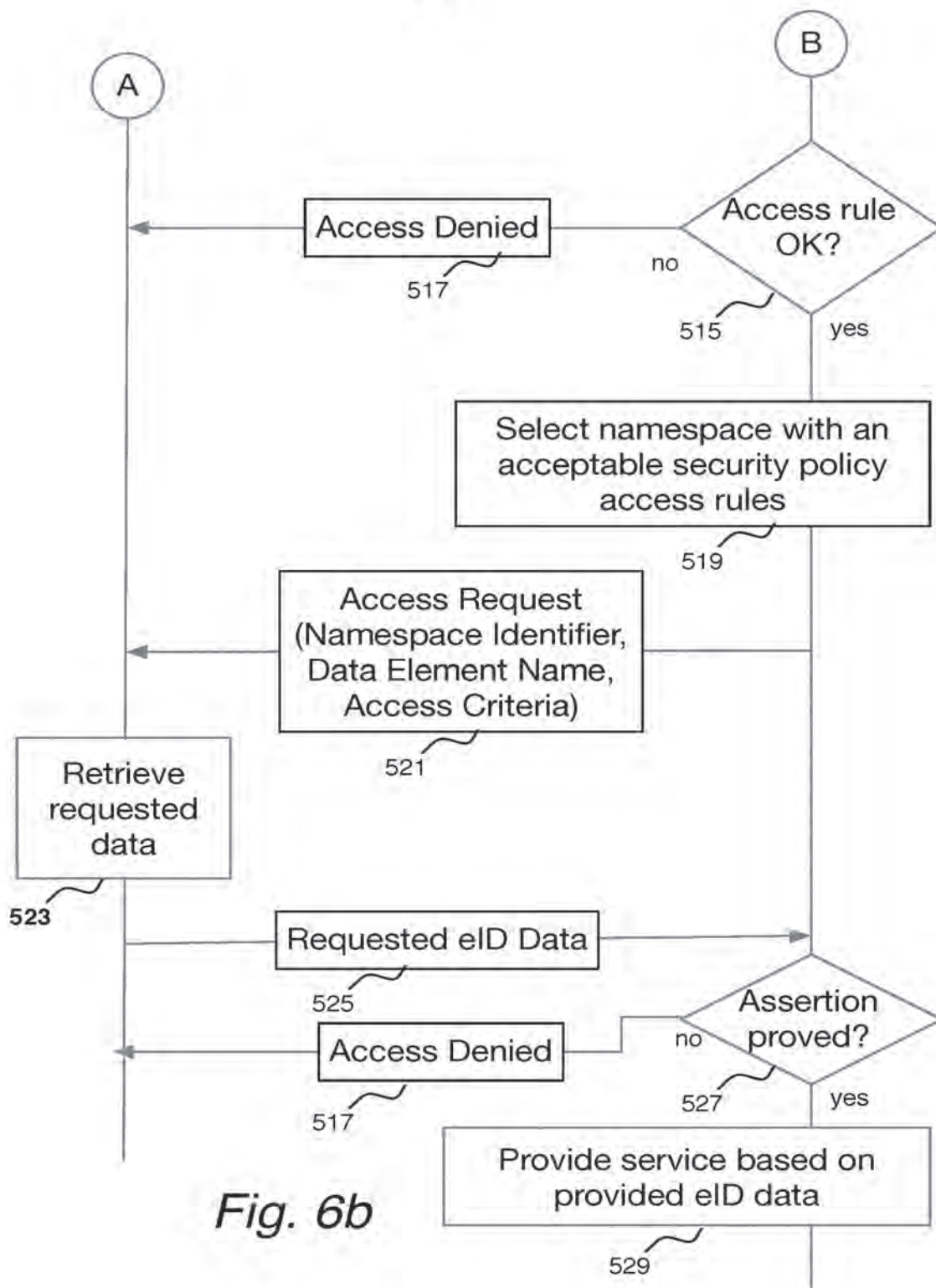
4/9

*Fig. 5*

5/9



6/9



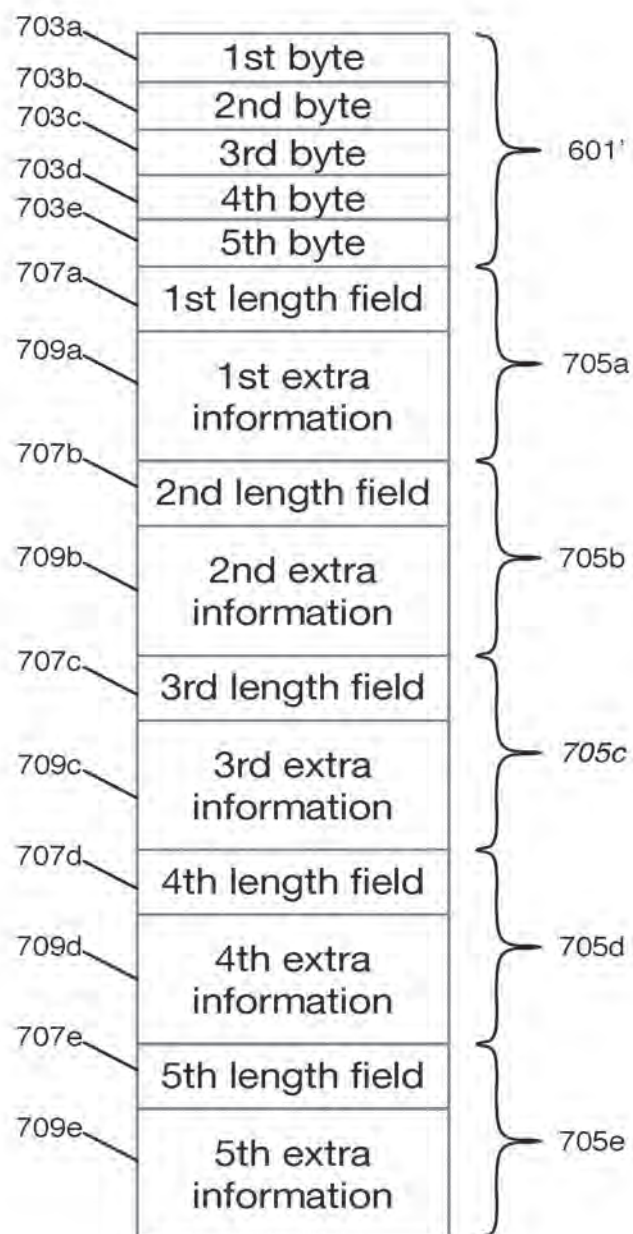
7/9

First byte								
b8	b7	b6	b5	b4	b3	b2	b1	
								Value determining the version of this template (for extensibility and interoperability)
Second byte								
b8	b7	b6	b5	b4	b3	b2	b1	value denoting the authentication protocol required
								e.g. digital signature
								e.g. reader authentication
								e.g. certificate verification
								e.g. secure messaging
								e.g. role authentication
								e.g. user consent ...
Third byte								NOTE: could be a coded over a nibble of the first byte if allowed
b8	b7	b6	b5	b4	b3	b2	b1	value denoting the HASH type
								e.g. SHA-256
								e.g. SHA-384
								e.g. SHA-512
								...
Fourth byte								
b8	b7	b6	b5	b4	b3	b2	b1	value denoting the signature scheme
								e.g. RSA
								e.g. ECDSA
								...
Fifth byte								
b8	b7	b6	b5	b4	b3	b2	b1	value denoting secure messaging options
								e.g. AES 128 bits - CMAC
								e.g. AES 128 bits - EMAC
								e.g. AES-GCM ...

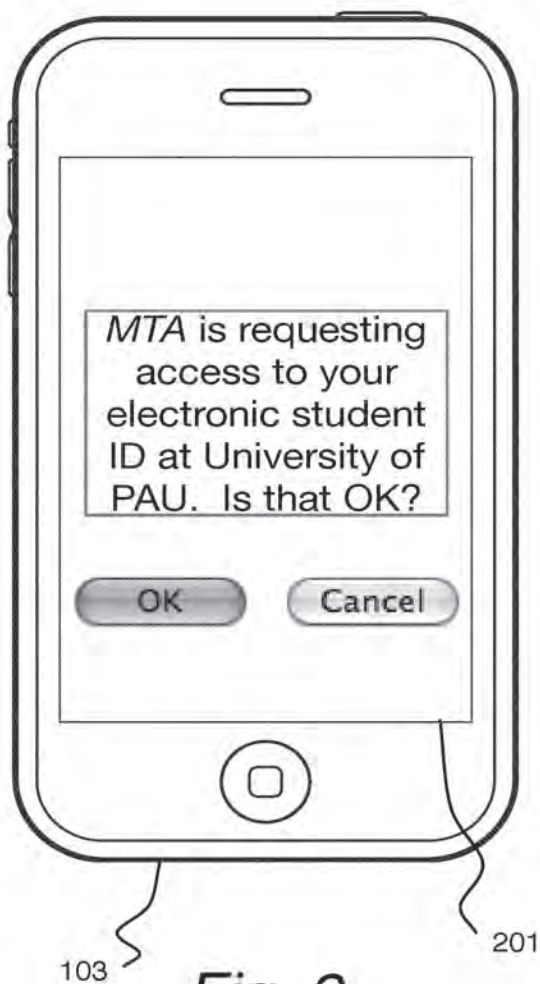
601

Fig. 7

8/9

*Fig. 8*

9/9

*Fig. 9*

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
 Stylesheet Version v1.2

EPAS ID: PAT7274090

SUBMISSION TYPE:	NEW ASSIGNMENT	
NATURE OF CONVEYANCE:	ASSIGNMENT	
CONVEYING PARTY DATA		
	Name	Execution Date
	FAHER MOURAD	04/04/2022
	CAROLE BAYLE	04/04/2022
RECEIVING PARTY DATA		
Name:	THALES DIS FRANCE SAS	
Street Address:	6, RUE DE LA VERRERIE	
City:	MEUDON	
State/Country:	FRANCE	
Postal Code:	92190	
PROPERTY NUMBERS Total: 1		
	Property Type	Number
	Application Number:	17767153
CORRESPONDENCE DATA		
Fax Number:		
<i>Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.</i>		
Phone:	954-658-0418	
Email:	us.intellectualproperty@thalesgroup.com	
Correspondent Name:	THALES DIS CPL USA, INC.	
Address Line 1:	900 SOUTH PINE ISLAND ROAD - SUITE 710	
Address Line 4:	PLANTATION, FLORIDA 33324	
ATTORNEY DOCKET NUMBER:	GMT4110US/WO MQ/MB	
NAME OF SUBMITTER:	MARC BOILLOT	
SIGNATURE:	/Marc BOILLOT/	
DATE SIGNED:	04/12/2022	
	This document serves as an Oath/Declaration (37 CFR 1.63).	
Total Attachments: 6		
source=GMT4110US_Signed_Comb_Decl_Assignment#page1.tif		
source=GMT4110US_Signed_Comb_Decl_Assignment#page2.tif		
source=GMT4110US_Signed_Comb_Decl_Assignment#page3.tif		
source=GMT4110US_Signed_Comb_Decl_Assignment#page4.tif		

source=GMT4110US_Signed_Comb_Decl_Assignment#page5.tif
source=GMT4110US_Signed_Comb_Decl_Assignment#page6.tif

COMBINED DECLARATION AND ASSIGNMENT

As the below named inventor(s), I/(we) hereby declare that this Combined Declaration and Assignment is directed to:

Case Reference Number	Patent Application Data Official Title	Inventor(s)
GMT4110	<p>US Patent Application N° Filed on</p> <p>and its corresponding International Application pursuant to the PCT/EP2020/076906 filed on September 25, 2020 and based on the priority EP19306357.5 filed on October 18, 2019</p> <p>SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES</p>	<p>BAYLE Carole FAHER Mourad</p>

DECLARATION

- As the below named inventor, I further declare that:
- The above-identified application was made or authorized to be made by me.
- I believe that I am the original inventor of a claimed invention in the application.
- I have reviewed and understand the contents of the above-identified specification, including the claims.
- I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.
- I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

ASSIGNMENT

THIS ASSIGNMENT is made by and between the undersigned inventor (hereinafter referred to as "the Assignor"), and **THALES DIS FRANCE SAS** (hereinafter referred to as "the Assignee"), a corporation duly organized under and pursuant to the laws of France and having a principal place of business at: 6 rue de La Verrerie - 92190 Meudon - France

MF

1/1/2021

WHEREAS, the Assignor has invented certain new and useful improvements set forth in the application for Letters Patent of the United States identified above;

WHEREAS, the Assignee is desirous of acquiring the entire right, title, and interest in and to said inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications, including provisional applications for Letters Patent of the United States or other countries claiming priority to said application, and in and to any Letters Patent or Patents, United States or foreign, to be obtained therefore and thereon.

NOW, THEREFORE, for good and sufficient consideration, the receipt of which is hereby acknowledged, the Assignor has sold, assigned, transferred, and set over, and by these presents does sell, assign, transfer, and set over, unto the Assignee, its successors, legal representatives, and assigns the entire right, title, and interest in and to the above-mentioned inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications for Letters Patent of the United States or other countries claiming priority to said applications, and any and all Letters Patent or Patents of the United States of America and all foreign countries that may be granted therefore and thereon, and in and to any and all applications claiming priority to said applications, divisions, continuations, and continuations-in-part of said applications, and reissues, and re-examinations and extensions of said Letters Patent or Patents, and all rights under the international Convention for the Protection of Industrial Property, the same to be held and enjoyed by the Assignee, for its own use and benefit and the use and benefit of its successors, legal representatives, and assigns, to the full end of the term or terms for which Letters Patent or Patents may be granted as fully and entirely as the same would have been held and enjoyed by the Assignor had this sale and assignment not been made;

AND for the same consideration, the Assignor hereby covenants and agrees to and with the Assignee, its successors, legal representatives, and assigns, that, at the time of execution and delivery of these presents, the Assignor is the sole and lawful owner of the entire right, title, and interest in and to the inventions set forth in said applications and said applications, including provisional applications, above-mentioned, and that the same are unencumbered, and that the Assignor has good and full right and lawful authority to sell and convey the same in the manner herein set forth;

AND for the same consideration, the Assignor hereby covenants and agrees to and with the Assignee, its successors, legal representatives, and assigns that the Assignor will, whenever counsel of the Assignee, or the counsel of its successors, legal representatives, and assigns, shall advise that any proceeding in connection with said inventions or said applications for Letters Patent or Patents, or any proceeding in connection with Letters Patent or Patents for said inventions in any country, including interference proceedings, is lawful and desirable, or that any application claiming priority to said application, division, continuation, or continuation-in-part of any applications for Letters Patent or Patents, or any reissue or extension of any Letters Patent or Patents to be obtained thereon, is lawful and desirable, sign all papers and documents, take all lawful oaths, and do all acts necessary or

MF 21

required to be done for the procurement, maintenance, enforcement, and defense of Letters Patent or Patents for said inventions, without charge to the Assignee, its successors, legal representatives, and assigns, but at the cost and expense of the Assignee, its successors, legal representatives, and assigns;

AND the Assignor hereby requests the Commissioner of Patents to issue any and all said Letters Patent of the United States to the Assignee as the Assignee of said inventions, the Letters Patent to be issued for the sole use and benefit of the Assignee, its successors, legal representatives, and assigns.

INVENTOR(S):

April 4th, 2022
Date

FAHER, Mourad
Name


Signature

Date

BAYLE, Carole
Name

Signature

MF

3 | Page

COMBINED DECLARATION AND ASSIGNMENT

As the below named inventor(s), I(we) hereby declare that this Combined Declaration and Assignment is directed to:

Case Reference Number	Patent Application Data Official Title	Inventor(s)
GMT4110	US Patent Application N° Filed on and its corresponding International Application pursuant to the PCT/EP2020/076906 filed on September 25, 2020 and based on the priority EP19306357.5 filed on October 18, 2019 SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES	BAYLE Carole FAHER Mourad

DECLARATION

- As the below named inventor, I further declare that:
- The above-identified application was made or authorized to be made by me.
- I believe that I am the original inventor of a claimed invention in the application.
- I have reviewed and understand the contents of the above-identified specification, including the claims.
- I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.
- I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

ASSIGNMENT

THIS ASSIGNMENT is made by and between the undersigned inventor (hereinafter referred to as "the Assignor"), and **THALES DIS FRANCE SAS** (hereinafter referred to as "the Assignee"), a corporation duly organized under and pursuant to the laws of France and having a principal place of business at: 6 rue de La Verrerie - 92190 Meudon - France

WHEREAS, the Assignor has invented certain new and useful improvements set forth in the application for Letters Patent of the United States identified above;

WHEREAS, the Assignee is desirous of acquiring the entire right, title, and interest in and to said inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications, including provisional applications for Letters Patent of the United States or other countries claiming priority to said application, and in and to any Letters Patent or Patents, United States or foreign, to be obtained therefore and thereon.

NOW, THEREFORE, for good and sufficient consideration, the receipt of which is hereby acknowledged, the Assignor has sold, assigned, transferred, and set over, and by these presents does sell, assign, transfer, and set over, unto the Assignee, its successors, legal representatives, and assigns the entire right, title, and interest in and to the above-mentioned inventions, the right to file applications on said inventions and the entire right, title and interest in and to any applications for Letters Patent of the United States or other countries claiming priority to said applications, and any and all Letters Patent or Patents of the United States of America and all foreign countries that may be granted therefore and thereon, and in and to any and all applications claiming priority to said applications, divisions, continuations, and continuations-in-part of said applications, and reissues, and re-examinations and extensions of said Letters Patent or Patents, and all rights under the International Convention for the Protection of Industrial Property, the same to be held and enjoyed by the Assignee, for its own use and benefit and the use and benefit of its successors, legal representatives, and assigns, to the full end of the term or terms for which Letters Patent or Patents may be granted as fully and entirely as the same would have been held and enjoyed by the Assignor had this sale and assignment not been made;

AND for the same consideration, the Assignor hereby covenants and agrees to and with the Assignee, its successors, legal representatives, and assigns, that, at the time of execution and delivery of these presents, the Assignor is the sole and lawful owner of the entire right, title, and interest in and to the inventions set forth in said applications and said applications, including provisional applications, above-mentioned, and that the same are unencumbered, and that the Assignor has good and full right and lawful authority to sell and convey the same in the manner herein set forth;

AND for the same consideration, the Assignor hereby covenants and agrees to and with the Assignee, its successors, legal representatives, and assigns that the Assignor will, whenever counsel of the Assignee, or the counsel of its successors, legal representatives, and assigns, shall advise that any proceeding in connection with said inventions or said applications for Letters Patent or Patents, or any proceeding in connection with Letters Patent or Patents for said inventions in any country, including interference proceedings, is lawful and desirable, or that any application claiming priority to said application, division, continuation, or continuation-in-part of any applications for Letters Patent or Patents, or any reissue or extension of any Letters Patent or Patents to be obtained thereon, is lawful and desirable, sign all papers and documents, take all lawful oaths, and do all acts necessary or

required to be done for the procurement, maintenance, enforcement, and defense of Letters Patent or Patents for said inventions, without charge to the Assignee, its successors, legal representatives, and assigns, but at the cost and expense of the Assignee, its successors, legal representatives, and assigns;

AND the Assignor hereby requests the Commissioner of Patents to issue any and all said Letters Patent of the United States to the Assignee as the Assignee of said inventions, the Letters Patent to be issued for the sole use and benefit of the Assignee, its successors, legal representatives, and assigns.

INVENTOR(S):

	FAHER, Mourad	
_____	_____	_____
Date	Name	Signature

	BAYLE, Carole	
06/25/2011	_____	
Date	Name	Signature



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1459
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GR/PART UNIT	FIL. FEE REC'D	ATTY. DOCKET NO.	TOT. CLAIMS	IND. CLAIMS
17/767,153	04/07/2022		1660	GMT4110US/WO MQ/MB	16	3

CONFIRMATION NO. 2044

FILING RECEIPT



180929
THALES DIS CPL USA, INC.
Marc BOILLOT
900 South Pine Island Road – Suite 710
PLANTATION, FL 33324

Date Mailed: 08/16/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Mourad FAHER, MARLY LE ROI, FRANCE;
Carole BAYLE, MARSEILLE, FRANCE;

Applicant(s)

THALES DIS FRANCE SAS, MEUDON, FRANCE;

Assignment For Published Patent Application

THALES DIS FRANCE SAS, MEUDON, FRANCE

Power of Attorney: The patent practitioners associated with Customer Number 180929

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/EP2020/076906 09/25/2020

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.)

EUROPEAN PATENT OFFICE (EPO) 19306357.5 10/18/2019

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 08/12/2022

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/767,153**

Projected Publication Date: 11/24/2022

Non-Publication Request: No

Early Publication Request: No
Title

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON
MOBILE DEVICES

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

U.S. APPLICATION NO.	FIRST NAMED INVENTOR	ATTY. DOCKET NO.
17/767,153	Mourad FAHER	GMT4110US/WO MQ/MB
180929 THALES DIS CPL USA, INC. Marc BOILLOT 900 South Pine Island Road – Suite 710 PLANTATION, FL 33324		INTERNATIONAL APPLICATION NO. PCT/EP2020/076906
		LA. FILING DATE 09/25/2020
		PRIORITY DATE 10/18/2019

CONFIRMATION NO. 2044
371 ACCEPTANCE LETTER



Date Mailed: 08/16/2022

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office, in its capacity as a Designated / Elected Office (37 CFR 1.495), has ACCEPTED the above identified international application for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above. A Filing Receipt will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE "FILING DATE or 371(c) DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1) and (c)(2) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN BELOW.** The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363)

04/07/2022

DATE OF RECEIPT OF 35 U.S.C.
371(c)(1) and (c)(2) REQUIREMENTS

The following items have been received:

- Copy of the International Application filed on 04/07/2022
- Copy of the International Search Report filed on 04/07/2022
- Preliminary Amendments filed on 04/07/2022
- Information Disclosure Statements filed on 04/07/2022
- Inventor's Oath or Declaration filed on 04/07/2022
- U.S. Basic National Fees filed on 04/07/2022
- Assignee Statement for PGPUB filed on 04/07/2022
- Authorize Access to Search Results filed on 04/07/2022
- Priority Documents filed on 04/07/2022
- Power of Attorney filed on 04/07/2022
- Authorization to Permit Access filed on 04/07/2022
- Application Data Sheet (37 CFR 1.76) filed on 04/07/2022

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

TONI M HOOD

Telephone: (571) 272-3654

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 17/767,153			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)		
BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A			N/A	320		
SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A			N/A	540		
EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A			N/A	800		
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	16	minus 20 =				x 100 =	0.00		
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	3	minus 3 =				x 480 =	0.00		
APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00		
MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>							0.00		
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL		TOTAL	1660		
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total <small>(37 CFR 1.16(ii))</small>	* Minus **	=	x =			x =		
	Independent <small>(37 CFR 1.16(h))</small>	* Minus ***	=	x =			x =		
	Application Size Fee <small>(37 CFR 1.16(s))</small>								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>								
TOTAL ADD'L FEE						TOTAL ADD'L FEE			
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total <small>(37 CFR 1.16(ii))</small>	* Minus **	=	x =			x =		
	Independent <small>(37 CFR 1.16(h))</small>	* Minus ***	=	x =			x =		
	Application Size Fee <small>(37 CFR 1.16(s))</small>								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>								
TOTAL ADD'L FEE						TOTAL ADD'L FEE			
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.									

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET Substitute for Form PTO-1360 (For use with Form PTO/SB/06)							Application Number 17767153		Filing Date		
							Applicant(s) Mourad FAHER				
							* May be used for additional claims or amendments				
CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT						
	Indep	Depend	Indep	Depend	Indep	Depend		Indep	Depend	Indep	Depend
1	1		1								
2		1		1							
3		2		1							
4		(1)		1							
5		(1)		1							
6		(1)		1							
7		(1)		1							
8		(1)		1							
9		(1)		1							
10		(1)		1							
11	3		1								
12		1		(1)							
13		2		(1)							
14		(1)		(1)							
15		2		(1)							
16	1		1								
17											
18											
19											
20											
21											
22											
23											
24											
25											
26											
27											
28											
29											
30											
31											
32											
33											
34											
35											
36											
37											
38											
39											
40											
41											
42											
43											
44											
45											
46											
47											
48											
49											
50											
Total Indep	3		3		0						
Total Depend	16	↙	13	↙	0	↙					
Total Claims	19		16		0						

51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/767,153	04/07/2022	Mourad FAHER	GMT4110US/WO MQ/MB CONFIRMATION NO. 2044

180929

THALES DIS CPL USA, INC.
Marc BOILLOT - Adam LEWENTAL
900 South Pine Island Road ? Suite 710
PLANTATION, FL 33324

PUBLICATION NOTICE



Title: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Publication No. US-2022-0374533-A1

Publication Date: 11/24/2022

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publicly available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <https://portal.uspto.gov/pair/PublicPair>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Notice of References Cited	Application/Control No. 17/767,153	Applicant(s)/Patent Under Reexamination FAHER et al.	
	Examiner RICHARD G KEEHN	Art Unit 2444	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Name	CPC Classification	US Classification
*	A	US-20220374533-A1	2022-11-24	FAHER; Mourad	G06Q20/326	1/1
*	B	US-20160055248-A1	2016-02-25	Goel; Samir	G06F21/6218	707/770
*	C	US-20150040180-A1	2015-02-05	Jacobson; Van L.	G06F21/62	726/1
*	D	US-20120159195-A1	2012-06-21	von Behren; Rob	G06F21/62	713/193
*	E	US-20090006642-A1	2009-01-01	Dickens; Christopher Scott	H04L65/611	709/231
*	F	US-20060265508-A1	2006-11-23	Angel; Franklin J.	H04L61/2567	709/230
*	G	US-11973758-B2	2024-04-30	Baryshnikov; Boris V.	H04L63/10	1/1
*	H	US-10922386-B1	2021-02-16	Li; Ching-Yi	G06F21/53	1/1
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable; Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in YYYY-MM-DD format are publication dates. Classifications may be US or foreign.

<i>Search Notes</i> 	Application/Control No. 17/767,153	Applicant(s)/Patent Under Reexamination FAHER et al.
	Examiner RICHARD G KEEHN	Art Unit 2444

CPC - Searched*		
Symbol	Date	Examiner
G06F21/62	05/07/2024	rkeehn
H04L63/101	05/07/2024	rkeehn
H04L63/20	05/07/2024	rkeehn
G06Q50/265	05/07/2024	rkeehn
G06Q20/3227,326,363,367,3825,3827,4014	05/07/2024	rkeehn

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor/Applicant search.	05/07/2024	rkeehn
Prior-art searches in PE2E-Search and Innovation Q+.	05/07/2024	rkeehn

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

--	--

Bibliographic Data

Application No: 17/767,153

Foreign Priority claimed: ☒ Yes ☐ No

35 USC 119 (a-d) conditions met: ☒ Yes ☐ No ☐ Met After Allowance

Verified and Acknowledged: /RICHARD G KEEHN/

Examiner's Signature

Initials

Title:

SECURITY MECHANISM FOR NAMESPACES USED IN
ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
04/07/2022	726	2444	
RULE			

APPLICANTS

THALES DIS FRANCE SAS, MEUDON, FRANCE

INVENTORS

Mourad FAHER, MARLY LE ROI, FRANCE

Carole BAYLE, MARSEILLE, FRANCE

CONTINUING DATA

This application is a 371 of PCT/EP2020/076906 09/25/2020

FOREIGN APPLICATIONS

EPO EP19306357.5 10/18/2019

IF REQUIRED, FOREIGN LICENSE GRANTED**

08/12/2022

STATE OR COUNTRY

FRANCE

ADDRESS

FILING FEE RECEIVED

\$1,660



Search History

17767153

Report Run Date: 2024-05-07 UTC

Searches: 3

Markers: 0

Search #	Timestamp	Results	Page
1	2024-05-07 19:43 UTC	25,544,135	3
2	2024-05-07 19:45 UTC	17,133,518	4
3	2024-05-07 20:37 UTC	15,424,105	4

Content: Patents + NPL (193)

US Patents | US Designs | US Applications | EPO Patents | EPO Applications | China Patents | China Applications | Japan Patents | Japan Applications | Korea Patents | Korea Applications | WIPO Applications | Argentina Patents | Argentina Applications | Brazil Patents | Brazil Applications | Canada Patents | Canada Applications | Chile Patents | Chile Applications | Colombia Applications | Costa Rica Applications | Cuba Patents | Cuba Applications | Dominican Republic Applications | Ecuador Patents | Ecuador Applications | El Salvador Applications | Guatemala Applications | Honduras Applications | Mexico Patents | Mexico Applications | Nicaragua Patents | Panama Applications | Peru Applications | Trinidad & Tobago Patents | Uruguay Applications | Austria Patents | Austria Applications | Belarus Patents | Belgium Patents | Belgium Applications | Bosnia & Herzegovina Patents | Bosnia & Herzegovina Applications | Bulgaria Patents | Bulgaria Applications | Croatia Patents | Croatia Applications | Czech Republic Patents | Czech Republic Applications | Czechoslovakia Patents | Czechoslovakia Applications | Denmark Patents | Denmark Applications | Estonia Patents | Estonia Applications | EUIPO Patents | Finland Patents | Finland Applications | France Patents | France Applications | Germany Patents | Germany Applications | Great Britain Patents | Great Britain Applications | Greece Patents | Greece Applications | Hungary Patents | Hungary Applications | Iceland Patents | Iceland Applications | Ireland Patents | Ireland Applications | Italy Patents | Italy Applications | Latvia Patents | Latvia Applications | Lithuania Patents | Lithuania Applications | Luxembourg Patents | Luxembourg Applications | Malta Patents | Monaco Patents | Montenegro Patents | Montenegro Applications | Netherlands Patents | Netherlands Applications | Norway Patents | Norway Applications | Poland Patents | Poland Applications | Portugal Patents | Portugal Applications | Republic of Moldova Patents | Republic of Moldova Applications | Romania Patents | Romania Applications | San Marino Patents | San Marino Applications | Serbia Patents | Serbia Applications | Slovakia Patents | Slovakia Applications | Slovenia Patents | Spain Patents | Spain Applications | Sweden Patents | Sweden Applications | Switzerland Patents | Switzerland Applications | Ukraine Patents | Yugoslavia/Serbia and Montenegro Patents | Yugoslavia/Serbia and Montenegro Applications | Armenia Patents | Australia Patents | Australia Applications | Cyprus Patents | Gulf Cooperation Council Patents | Hong Kong Patents | India Patents | India Applications | Indonesia Patents | Indonesia Applications | Israel Patents | Israel Applications | Jordan Patents | Jordan Applications | Kyrgyzstan Patents | Macao Applications | Malaysia Patents | Mongolia Patents | New Zealand Patents | Philippines Patents | Philippines Applications | Saudi Arabia Patents | Saudi Arabia Applications | Singapore Patents | Singapore Applications | Taiwan Patents | Taiwan Applications | Tajikistan Patents | Tajikistan Applications | Thailand Patents | Thailand Applications | Uzbekistan Patents | Vietnam Patents | Algeria Patents | ARIPO Patents | ARIPO Applications | Egypt Patents | Kenya Patents | Malawi Patents | Morocco Patents | Morocco Applications | OAPI Patents | South Africa Patents | Tunisia Applications | Zambia Patents | Zimbabwe Patents | EAPO Patents | EAPO Applications | Georgia Patents | Georgia Applications | Kazakhstan Patents | Kazakhstan Applications | Russia Patents | Russia Applications | Turkey Patents | Turkey Applications | IEEE Xplore Publications: IEEE Periodicals | IEEE Xplore Publications: IEEE Conferences | IEEE Xplore Publications: IEEE Standards | IEEE Xplore Publications: IEEE Early Access | IEEE Xplore Publications: SMPTE Periodicals | IEEE Xplore Publications: SMPTE Conferences | IEEE Xplore Publications: SMPTE Standards | IEEE Xplore Publications: MIT Press eBooks | IEEE Xplore Publications: Wiley-IEEE eBooks | IEEE Xplore Publications: IBM Periodicals | IEEE Xplore Publications: URSI Periodicals | IEEE Xplore Publications: VDE Conferences | IEEE Xplore Publications: Periodicals from China | IEEE Xplore Publications: Ericsson Technology Review | IP.com Prior Art Database: The IP.com Journal | IP.com Prior Art Database: Internet Society RFC | IP.com Prior Art Database: IBM TDB Archive | IP.com Prior Art Database: Legacy Journals | IP.com Prior Art Database: Software Patent Institute | OnePetro.org: Periodicals at OnePetro.org | OnePetro.org: Conferences at OnePetro.org | Other Literature: IBM Redbooks | Other Literature: PubMed Central | Other Literature: arXiv.org

1 2024-05-07 19:43 UTC | 25,544,135 results from 

De-Dup: None | Relevance Cut-off: None | Sort: Relevance

Main Concept: Text

A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile

device, comprising: associating security policies with each of a plurality of supported namespaces on a mobile device; and operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.

Concept Modifiers: None

Filters: None

2 2024-05-07 19:45 UTC | 17,133,518 results from 

De-Dup: None | **Relevance Cut-off:** None | **Sort:** Relevance

Main Concept: [Same as Search 1](#)

Concept Modifiers: None

Filters (1):

[Publication Date:](#) To 2019-10-18

3 2024-05-07 20:37 UTC | 15,424,105 results from 

De-Dup: None | **Relevance Cut-off:** None | **Sort:** Relevance

Main Concept: Text

A mobile device comprising: a processor; and a memory for storing instructions executable by the processor and for storing electronic identity (eID) data, the memory including an eID wallet application having instructions to cause the processor to: receive a list of selected namespaces from a reader; in response to receiving the list of selected namespaces from the reader, transmitting security rules associated with each selected namespace according to a defined bytestring template.

Concept Modifiers: None

Filters: [Same as Search 2](#)

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/09a (02-16)

Approved for use through 11/30/2020. OMB 0851-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	
	First Named Inventor	Mourad FAHER
	Art Unit	
	Examiner Name	
	Attorney Docket Number	GMT4110US/WO MQ/MB

U.S. PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S. PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
/R.G.K./	1	20160294831	A1	2016-10-06	BORUNDA ADRIAN [US] ET AL	paragraph [0005] - paragraph [0008] paragraph [0021] - paragraph [0034] figures 1-2		
/R.G.K./	2	20160156386	A1	2016-06-02	VAN NIEUWENHUYZE OLIVIER [BE] ET AL	paragraph [0005] - paragraph [0007] paragraph [0050] - paragraph [0065]; figure 4		
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
/R.G.K./	1	WO2015/036957	WO	A1	2015-03-19	TORO DEV LTD [CN]	abstract page 1, line 25-page 3, line 18 page 6, line 28-page 13, line 32	
If you wish to add additional Foreign Patent Document citation information please click the Add button.							Add	
NON-PATENT LITERATURE DOCUMENTS							Remove	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	Mourad FAHER
Art Unit	
Examiner Name	
Attorney Docket Number	GMT4110US/WO MQ/MB

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
/R.G.K./	1	International Search Report (PCT/ISA/210) and Written Opinion (PCT/ISA/237) mailed on November 20 2020, by the European Patent Office as the International Searching Authority for current International Application No. PCT/EP2020/076906 - [16 pages]	
/R.G.K./	2	EMVCO: "EMV '96 Integrated Circuit Card Application Specification for Payment Systems", EMV, EMVCO vol. 3.1.1 ; Contact, 1 July 2006 (2006-07-01), pages 1-62, XP061034511, Retrieved from the Internet: URL:https://www.emvco.com/wp-content/uploads/documents/Emvapp_20090126073328.pdf [retrieved on 2020-01-06] - page 15 - page 16	
/R.G.K./	3	Anonymous: "Thales lance son nouveau portefeuille d'identité numérique - vos documents d'identité accessibles où que vous soyez "Thales Group", 29 July 2019 (2019-07-29), pages 1-7, XP055689283, Retrieved from the Internet: URL:https://www.thalesgroup.com/fr/group/journaliste/press_release/thales-lance-son-nouveau-portefeuille-didentite-numerique-vos [retrieved on 2020-04-24] the whole document	
	4		
	5		

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/RICHARD G KEEHN/	Date Considered	05/03/2024
--------------------	-------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	Mourad FAHER
Art Unit	
Examiner Name	
Attorney Docket Number	GMT4110US/WO MQ/MB

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Marc BOILLOT/	Date (YYYY-MM-DD)	2022-04-07
Name/Print	Marc BOILLOT	Registration Number	56164

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	1	"20220374533"	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/03 12:39 PM
L2	136	((("THALES") near3 ("DIS") near3 ("FRANCE") near3 ("SAS"))).AS,AANM,	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:06 PM
L4	14	((("FAHER") near3 ("Mourad")) OR ((("BAYLE") near3 ("Carole"))).INV	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:07 PM
L5	147	2 4	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:07 PM
L6	2	5 AND wallet.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:08 PM
L7	1	6 AND eid.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:08 PM
L8	0	6 AND eid.clm.	(USPAT)	OR	ON	ON	2024/05/06 05:08 PM
L9	208115	(G06F21/62 OR H04L63/101 OR H04L63/20 OR G06Q50/265 OR G06Q20/3227,326,363,367,3825,3827,4014).c pc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/06 05:10 PM
L10	168211	9 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/06 05:11 PM
L11	476	(namespace "name space") WITH security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:42 PM
L12	2	(namespace "name space") WITH security WITH (rule policy procedure) WITH reader	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:42 PM
L13	19	(namespace "name space") WITH security WITH (rule policy procedure) WITH (select\$4 choos\$4)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:43 PM
L14	0	13 AND 10	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:43 PM
L15	3	13 AND (@ad	(US-PGPUB; USPAT;	OR	ON	ON	2024/05/07

		@prad)<20191018	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)				01:43 PM
L16	141	(EID "electronic identification") WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:46 PM
L17	11	11 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:47 PM
L18	0	17 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:47 PM
L19	4815	(namespace "name space") WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:47 PM
L20	11	19 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:48 PM
L21	0	20 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:48 PM
L22	262497	security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:48 PM
L23	11	16 WITH 22	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:49 PM
L24	0	23 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:49 PM
L25	476	(namespace "name space") WITH security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:49 PM
L26	476	22 AND 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:50 PM
L27	476	22 SAME 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:50 PM
L28	476	22 WITH 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	ON	2024/05/07 01:50 PM

L29	11	28 AND 16	JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:52 PM
L30	0	29 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:52 PM
L31	49	28 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:53 PM
L32	32	31 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:53 PM
L33	433	(select\$4 choos\$4) WITH namespace WITH access\$4	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:56 PM
L34	5841	namespace WITH (rule policy procedure check\$4 algorithm)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:57 PM
L35	159	33 AND 34	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:57 PM
L36	95	35 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:58 PM
L37	23024057	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:59 PM
L38	77	36 AND 37	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:59 PM
L39	77	38 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:00 PM
L40	19	38 AND (@ad @prad)<20191018 AND 9	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:00 PM
L41	1159	(mobile wireless portable cell cellular phone tablet ipad ipod	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2024/05/07 02:20 PM

L42	65	notebook radio) WITH namespace 41 AND wallet	IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:21 PM
L43	50	42 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:21 PM
L44	40942	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:51 PM
L45	1159	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH namespaces	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:52 PM
L46	51	44 AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:52 PM
L47	36	46 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:52 PM
L48	65	wallet AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:13 PM
L49	50	48 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:13 PM
L50	881	45 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:32 PM
L51	50	45 AND (@ad @prad)<20191018 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:32 PM
L52	66	45 AND (@ad @prad)<20191018 AND (eid wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:33 PM
L53	16	52 NOT 51	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:33 PM
L54	43457	(mobile wireless	(US-PGPUB; USPAT;	OR	ON	ON	2024/05/07

L55	40942	portable cell cellular phone tablet ipad ipod notebook radio) WITH (eid wallet)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	03:35 PM
L56	28	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH (wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:35 PM
L57	9	55 AND ((rule policy procedure safeguard) WITH namespace)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:36 PM
L58	8	56 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:36 PM
L59	3	((US-10922386-B1 OR US-11973758-B2).did. AND USPT.dbnm.) OR ((US-20090006642-A1 OR US-20160055248- A1 OR US- 20150040180-A1 OR US-20060265508-A1 OR US-20120159195- A1 OR US- 20220374533-A1).did. AND PGPB.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:40 PM
L60	289	58 AND 10	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:40 PM
L61	14	45 AND reader	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:54 PM
L61	14	45 AND (reader WITH wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	ON	2024/05/07 03:55 PM

L62	12	61 AND (@ad @prad)<20191018	JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:56 PM
L63	16	(list\$4 roster) WITH namespaces WITH (reader cardreader)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 05:46 PM
L64	10	(bytestring "byte string") WITH template WITH (rules policies)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 05:47 PM
L65	1	63 AND 64	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 05:47 PM
L66	0	65 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 05:47 PM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/767,153	04/07/2022	Mourad FAHER	GMT4110US/WO MQ/MB	2044
180929	7590	05/13/2024		
THALES DIS CPL USA, INC. Intellectual Property 900 South Pine Island Road Suite 710 PLANTATION, FL 33324			EXAMINER KEEHN, RICHARD G	
			ART UNIT 2444	PAPER NUMBER
			NOTIFICATION DATE 05/13/2024	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

adam.lewentel@thalesgroup.com
marc.boillot@thalesgroup.com
us.intellectualproperty@thalesgroup.com

DETAILED ACTION

- 1. Claims 1-16 are pending and have been examined.**

Notice of Pre-AIA or AIA Status

- 2. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.**

Claim Rejections - 35 USC § 112

- 3. The following is a quotation of 35 U.S.C. 112(b):**
(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

- 4. Claims 2, 3, 6-8, 10 and 12-16 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor (or for applications subject to pre-AIA 35 U.S.C. 112, the applicant), regards as the invention.**

a. Claim 2 recites the limitations "the verifier module" and "the verifier" in the first limitation. There is insufficient antecedent basis for this limitation in the claim.

b. Claim 3 recites the limitation "the verifier module" in the first limitation. There is insufficient antecedent basis for this limitation in the claim.

- c. Claim 6 recites the limitation "the security policy " in the first limitation. There are a plurality of security policies claimed in Claim 1. Which one of the plurality is THE security policy?
- d. Claim 7 recites the limitation "the required authentication" in the first limitation. There is insufficient antecedent basis for this limitation in the claim.
- e. Claim 8 recites the limitation "the verifier" in the first limitation. There is insufficient antecedent basis for this limitation in the claim.
- f. Claim 10 recites the limitation "the verifier terminal" in the first limitation. There is insufficient antecedent basis for this limitation in the claim.
- g. Claim 12 recites the limitation "the mobile device of claim 0" in the preamble. There is insufficient antecedent basis for this limitation in the claim. As such, Claims 13 and 15, which incorporate the unclear Claim 12, are also rejected.
- h. Claims 12 and 13 recite the limitation "the reader" in the second and first limitations respectively. It is unclear which reader is being referred to. Both Claims 11 and 12 recite "a reader". So is the claimed "the reader" the reader from Claim 11 or the reader from Claim 12? Claim 14, which incorporates Claim 13, is therefore rejected as well.
- i. Claim 15 recites "wherein the eID wallet application wherein the security policy" in the first limitation. This phrase makes no sense, and the claim is therefore unclear.
- j. Claim 16 recites the limitation "the verifier terminal" in the sixth limitation. There is insufficient antecedent basis for this limitation in the claim.

Allowable Subject Matter

5. Claims 1, 4, 5, 9 and 11 are allowed.

Interview Practice

USPTO Automated Interview Request (AIR)

The USPTO AIR is a new optional online interview scheduling tool that allows Applicants to request an interview with an Examiner for their pending patent application.

The USPTO AIR form is available on our website at:
<http://www.uspto.gov/patent/laws-and-regulations/interview-practice>.

By submitting this type of interview request, the pending patent application will be in compliance with the written authorization requirement for Internet communication in accordance with MPEP §502.03. This authorization will be in effect until the Applicant provides a written withdrawal of authorization to the Examiner of record.

If you have questions or need assistance with the USPTO AIR form or with interview practice at the USPTO, please contact an Interview Specialist at <http://www.uspto.gov/patent/laws-and-regulations/interview-practice/interview-specialist> or send an email to ExaminerInterviewPractice@USPTO.GOV.

Examiner Notes:

A) Prior to conducting any interview (whether using AIR or not), Applicant(s) must submit an agenda including the proposed date and time, all arguments in writing,

and proposed claim amendments (if applicable). Any proposed amendments or arguments not presented in the agenda will only be heard by the Examiner, but because the Examiner will not have heard them in advance and been given an equitable opportunity to consider them, no decision will be rendered, nor agreement made. ALL AGENDAS MUST BE RECEIVED BY THE EXAMINER AT LEAST 24 HOURS PRIOR TO THE START OF THE INTERVIEW, OR THE PREVIOUS BUSINESS DAY, WHICHEVER IS LONGER, or the interview may have to be rescheduled.

B) After-final interviews may be granted, but the agenda must be in compliance with MPEP 713.09 which limits the interview only to discussions of proposed amendments, or clarification for appeal. After-final interviews are not to be conducted for the purpose of rehashing previously made arguments. After seeing the agenda, Examiner will decide whether to grant or deny the interview.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See Form PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RICHARD G KEEHN whose telephone number is (571)270-5007. The examiner can normally be reached M-F 9:00am - 5:00pm Eastern.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/RICHARD G KEEHN/
Primary Examiner, Art Unit 2444

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 17/767,153		Filing Date 04/07/2022		☐ To be Mailed			
ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO											
APPLICATION AS FILED - PART I											
		(Column 1)	(Column 2)								
FOR		NUMBER FILED	NUMBER EXTRA		RATE (\$)		FEE (\$)				
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A		N/A						
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))		N/A	N/A		N/A						
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A		N/A						
TOTAL CLAIMS (37 CFR 1.16(j))		minus 20 =	*		x \$100 =						
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 =	*		x \$480 =						
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).									
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))											
* If the difference in column 1 is less than zero, enter "0" in column 2.					TOTAL						
APPLICATION AS AMENDED - PART II											
		(Column 1)	(Column 2)		(Column 3)						
AMENDMENT	08/12/2024	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR		PRESENT EXTRA		RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(g))	* 16	Minus	** 20		= 0		x \$100 =		0	
	Independent (37 CFR 1.16(h))	- 3	Minus	*** 3		= 0		x \$480 =		0	
	☐ Application Size Fee (37 CFR 1.16(s))										
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
								TOTAL ADD'L FEE		0	
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR		PRESENT EXTRA		RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(g))	*	Minus	**		=		x \$0 =			
	Independent (37 CFR 1.16(h))	*	Minus	***		=		x \$0 =			
	☐ Application Size Fee (37 CFR 1.16(s))										
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
								TOTAL ADD'L FEE			
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.								LIE			
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".								/TRACEY M YOUNG/			
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".											
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.											

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES
PATENT AND TRADEMARK OFFICE

Page 1 of 2
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION # 17/767,153	RECEIPT DATE / TIME 08/12/2024 01:58:02 PM Z ET	ATTORNEY DOCKET # GMT4110US/WO MQ/MB
------------------------------------	---	--

Title of Invention

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Application Information

APPLICATION TYPE	Utility - U.S. National Stage under 35 USC 371	PATENT #	-
CONFIRMATION #	2044	FILED BY	Marc Boillot
PATENT CENTER #	66747803	FILING DATE	04/07/2022
CUSTOMER #	180929	FIRST NAMED INVENTOR	Mourad FAHER
INTL. APPLICATION #	-	INTL. FILING DATE	-
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 3

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
GMT4110_ReplyTo_Non_Final_OA.pdf	7	-	63 KB
GMT4110_ReplyTo_Non_Final_OA-A....pdf (1-1)	1	Amendment/Request for Reconsideration-After Non-Final Rejection	30 KB
GMT4110_ReplyTo_Non_Final_OA-CLM.pdf (2-5)	4	Claims	45 KB
GMT4110_ReplyTo_Non_Final_OA-REM.pdf (6-7)	2	Applicant Arguments/Remarks Made in an Amendment	40 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
GMT4110_ReplyTo_Non_Final_OA.pdf	60FD95FA36D9EDEB9FBE833DDC25FD7297C0234199B90CFD8B351BEE1BF805B89F450E944DB640EC1711F6E7839872910F86538C3821BBF4379B03C71C7ED9F5
GMT4110_ReplyTo_Non_Final_OA-A....pdf	D0E22A4B1EC9C316B93E3C255AEF8CF7709A08C0295108B2D6346A91527C45EA73632564EDC0191F146D99A46E5459FFE0AE7EDF272926FE43EEFE5E3DF10AAA
GMT4110_ReplyTo_Non_Final_OA-CLM.pdf	87C69A31D4B6E70D8A80986A03F34B3A8398A31E19FFBF200678EA7C5939D1E03037678F3906B395643AFEF84DC1E64966477ECA18030C42A4F8D3ED44F21B44
GMT4110_ReplyTo_Non_Final_OA-REM.pdf	D55021707BDDF640E47DABCF89605FA4493E9B8DD5F5AE8834B4BA474EDF098A613423CB8A1A384F52D033A5B5F06B87754A82FFCE27B7D49A1A987449074097

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the immediate application:

Listing of Claims:

1. (Original) A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:
 - associating security policies with each of a plurality of supported namespaces on a mobile device; and
 - operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.
2. (Currently Amended) The method of claim 1 for managing security policies for data items stored in the electronic identification (eID) wallet on the mobile device, comprising:
 - transmitting a list of supported namespaces to ~~[[the]]~~ a verifier module executing on ~~[[the]]~~ a verifier ~~terminal~~; and
 - selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier ~~terminal~~ assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying a ~~[[the]]~~ security policy of ~~[[a]]~~ the namespace from the security policies associated with the plurality of supported namespaces on the mobile device.
3. (Currently Amended) The method of claim 1 for managing security policies for data items stored in the electronic identification (eID) wallet on the mobile device, comprising:
 - transmitting a list of supported namespaces to ~~[[the]]~~ a verifier module; and
 - selecting, by the verifier module, at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.
4. (Currently Amended) The method of claim 1 for managing security policies for data items stored in the electronic identification (eID) wallet on the mobile device further comprising:

prior to transmitting a list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

5. (Previously Presented) The method of claim 1 for managing security policies for data items stored in the electronic identification (eID) wallet on the mobile device, comprising:

transmitting the security policy of each of the plurality of supported namespaces from the mobile device to the reader.

6. (Currently Amended) The method of claim 1 for managing security policies for data items stored in the electronic identification (eID) wallet on the mobile device,

wherein a ~~[[the]]~~ security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options,

wherein the security policy is one of the security policies associated with the plurality of supported namespaces on the mobile device.

7. (Currently Amended) The method of claim 1 for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device ,

wherein ~~[[the]]~~ a required authentication ~~[[may be]]~~ is selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

8. (Currently Amended) The method of claim ~~[[1]]~~ 2 for managing security policies for data items stored in the electronic identification (eID) wallet on the mobile device further comprises

operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier terminal associates with each namespace in the plurality of supported namespaces.

9. (Currently Amended) The method of claim 1 for managing security policies for data items stored in an electronic identification (eID) wallet on ~~[[a]]~~ the mobile device, further comprises

operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

10. (Currently Amended) The method of claim [[1]] 2 for managing security policies for data items stored in an electronic identification (eID) wallet on [[a]] the mobile device,

wherein the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory, the method further comprising operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.

11. (Original) A mobile device comprising:

a processor; and

a memory for storing instructions executable by the processor and for storing electronic identity (eID) data, the memory including an eID wallet application having instructions to cause the processor to:

receive a list of selected namespaces from a reader;

in response to receiving the list of selected namespaces from the reader, transmitting security rules associated with each selected namespace according to a defined bytestring template.

12. (Currently Amended) The mobile device of claim [[10]] 11, wherein the eID wallet application further comprises instruction to cause the processor to:

receive a request for supported namespaces from [[a]] the reader;

transmit a list of supported name spaces to the reader.

13. (Currently Amended) The mobile device according to claim 12, wherein the eID wallet application further comprises instruction to cause the processor to:

prior transmitting a list of supported namespaces to [[a]] the reader, filter out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the reader.

14. (Currently Amended) The mobile device according to claim 13, wherein the eID wallet application further comprises instruction to cause the processor to:

transmit ~~[[the]]~~ a security policy of each of the plurality of supported namespaces to ~~[[a]] the~~ reader connected to a verifier.

15. (Currently Amended) The mobile device according to claim ~~[[12]]~~ 14, ~~wherein the eID wallet application~~ wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.

16. (Currently Amended) A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

associating a security policy with each of a plurality of supported namespaces on a mobile device;

transmitting the security policy of each of the plurality of supported namespaces to a reader connected to a verifier;

selecting, by the reader, at least one of the namespaces as candidate namespaces, and transmitting from the reader to the mobile device, a list containing the candidate namespaces;

transmitting to the reader by the mobile device, the security policy associated with each of the selected candidate namespaces;

operating the reader to:

determine for which of the candidate namespaces the reader can satisfy the security policy of the namespace; and

if the verifier can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the verifier ~~terminal~~ can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the mobile device;

if the verifier cannot satisfy the security policy of any of the candidate namespaces, rejecting access to the data item; and

upon successful demonstration by the reader to the mobile device of satisfaction of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

U.S. Appln. No.	: 17/767,153	Confirmation No.	2044
First Inventor	: Mourad FAHER		
Filed	: 04/07/2022		
TC/A.U.	: 2444		
Examiner	: Keehn, Richard G.		
Thales Docket No.	: GMT4110 EG/MB		

RESPONSE TO NON-FINAL OFFICE ACTION

MAIL STOP Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Date: August 12, 2024

Applicant provides the present Amendment to address the issues raised in the non-final Office Action mailed May 13, 2024 (hereinafter "Office Action").

This response is being filed within the three months period ending August 13, 2024. Accordingly, no extension of time fee is believed due.

Any additional fees however believed to be due in connection with this paper may be charged to Deposit Account No. **60-4092**.

Amendments to the Claims begin on page **2** of this submission; and

Remarks/Arguments begin on page **6** of this submission.

Application No. : 17/767,153
Reply to Office Action mailed: May 13, 2024
Amendment dated: August 12, 2024
Docket No.: GMT4110US EG/MB

REMARKS/ARGUMENTS

These remarks are in response to the final Office Action mailed May 13, 2024 **Error! Reference source not found.**("Office Action") and within the three-month shortened statutory period ending August 13, 2024. Accordingly, no extension of time fees are believed due.

Reconsideration and allowance of the present application are respectfully requested in view of the foregoing Amendments and following Remarks.

No new subject matter has been added.

Response to Claim Rejections under 35 USC § 112

On pages 2-3 of the Office Action, Claims 2, 3, 6-8, 10 and 12-16 were rejected under 35 U.S.C. 112(b) or 35 U.S.C.112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor (or for applications subject to pre-AI A 35 U.S.C. 112, the applicant), regards as the invention. Applicant has amended the claims for consistency and to overcome the rejections:

- a. Claim 2 now recites: overhead associated with satisfying a ~~[[the]]~~ security policy of ~~[[a]] the namespace from the security policies associated with the plurality of supported namespaces on the mobile device;~~
- b. Claim 3 now recites: transmitting a list of supported namespaces to ~~[[the]]~~ a verifier module;
- c. Claim 6 now recites: wherein the security policy is one of the security policies associated with the plurality of supported namespaces on the mobile device.
- d. Claim 7 now recites: wherein ~~[[the]]~~ a required authentication ~~[[may be]]~~ is selected
- e. Claim 8 now recites: method of claim ~~[[1]]~~ 2 to provide antecedent basis support of "a reader", where claim 2 introduces "a verifier module" and "a verifier terminal".
- f. Claim 10 now recites: method of claim ~~[[1]]~~ 2 to provide antecedent basis support for "the verifier terminal".

Application No. : 17/767,153
Reply to Office Action mailed: May 13, 2024
Amendment dated: August 12, 2024
Docket No.: GMT4110US EG/MB

- g. Claim 12 now recites: mobile device of claim [[10]] 11 to provide antecedent basis for "the" reader. Claims 13 and 15 have their claim dependency correct now.
- h. Claims 12 and 13 have their claim dependency correct now with reference to "the" reader which is common to both. Claim 14 is amended for consistency
- i. Claim 15 is corrected for clarification and to depend on claim 14 for support of "the" security policy.
- j. Claim 16 is amended for antecedent basis consistency with respect to "verifier".

Response to Allowable Subject Matter

On page 4 of the Office Action, Claims 1, 4, 5, 9 and 11 were indicated as allowable.

CONCLUSION

With the amendments to Claims 2, 3, 6-8, 10 and 12-16 to address and overcome the 35 U.S.C. 112(b) rejections, and their dependence on certain allowed claims, Applicant believes all the claims of this application are now in full condition for allowance. The Applicant respectfully requests that the Examiner please call the undersigned if clarification is needed on any matter within this Response.

Respectfully submitted,

Date: August 12, 2024

Customer No.: 180929

/Marc Boillot/
Marc A. Boillot
USPTO Reg. No.: 56,164
Telephone: (954) 658-0418

Search Notes 	Application/Control No. 17/767,153	Applicant(s)/Patent Under Reexamination FAHER et al.
	Examiner RICHARD G KEEHN	Art Unit 2444

CPC - Searched*		
Symbol	Date	Examiner
G06F21/62	05/07/2024	rkeehn
H04L63/101	05/07/2024	rkeehn
H04L63/20	05/07/2024	rkeehn
G06Q50/265	05/07/2024	rkeehn
G06Q20/3227,326,363,367,3825,3827,4014	05/07/2024	rkeehn

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor/Applicant search.	05/07/2024	rkeehn
Prior-art searches in PE2E-Search and Innovation Q+.	05/07/2024	rkeehn
Updated and interference searches.	08/19/2024	rkeehn

/RICHARD G KEEHN/ Primary Examiner, Art Unit 2444	
--	--

<i>Search Notes</i> 	Application/Control No. 17/767,153	Applicant(s)/Patent Under Reexamination FAHER et al.
	Examiner RICHARD G KEEHN	Art Unit 2444

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
G06F21	62	08/19/2024	rkeehn
H04L63	101	08/19/2024	rkeehn
H04L63	20	08/19/2024	rkeehn
G06Q50	265	08/19/2024	rkeehn
G06Q20	3227,326,363,367,3825,3827,4014	08/19/2024	rkeehn

/RICHARD G KEEHN/ Primary Examiner, Art Unit 2444	
--	--

Issue Classification 	Application/Control No. 17/767,153	Applicant(s)/Patent Under Reexamination FAHER et al.
	Examiner RICHARD G KEEHN	Art Unit 2444

CPC						
Symbol					Type	Version
G06F	/	21	/	62	F	2013-01-01
H04L	/	63	/	101	I	2013-01-01
H04L	/	63	/	20	I	2013-01-01
G06Q	/	50	/	265	A	2013-01-01

CPC Combination Sets					
Symbol				Type	Set

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	16	
/RICHARD G KEEHN/ Primary Examiner, Art Unit 2444	19 August 2024	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification 	Application/Control No. 17/767,153	Applicant(s)/Patent Under Reexamination FAHER et al.
	Examiner RICHARD G KEEHN	Art Unit 2444

INTERNATIONAL CLASSIFICATION			
CLAIMED			
G06F21/62	/	21	/ 62
H04L9/40	/	9	/ 40
G06Q50/26	/	50	/ 26
NON-CLAIMED			
	/		/

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	16	
/RICHARD G KEEHN/ Primary Examiner, Art Unit 2444	19 August 2024	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification 	Application/Control No. 17/767,153	Applicant(s)/Patent Under Reexamination FAHER et al.
	Examiner RICHARD G KEEHN	Art Unit 2444

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1,47															
CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	4	10												
2	2	11	11												
5	3	12	12												
6	4	13	13												
7	5	14	14												
8	6	15	15												
9	7	16	16												
3	8														
10	9														

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 16	
/RICHARD G KEEHN/ Primary Examiner, Art Unit 2444 (Primary Examiner) _____ (Date) 19 August 2024		O.G. Print Claim(s) 1	O.G. Print Figure 3

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	1	"20220374533"	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/03 12:39 PM
L2	136	((("THALES") near3 ("DIS") near3 ("FRANCE") near3 ("SAS"))).AS,AANM,	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:06 PM
L4	14	((("FAHER") near3 ("Mourad")) OR ((("BAYLE") near3 ("Carole"))).INV	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:07 PM
L5	147	2 4	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:07 PM
L6	2	5 AND wallet.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:08 PM
L7	1	6 AND eid.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:08 PM
L8	0	6 AND eid.clm.	(USPAT)	OR	ON	ON	2024/05/06 05:08 PM
L9	208115	(G06F21/62 OR H04L63/101 OR H04L63/20 OR G06Q50/265 OR G06Q20/3227,326,363, 367,3825,3827,4014).c pc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/06 05:10 PM
L10	168211	9 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/06 05:11 PM
L11	476	(namespace "name space") WITH security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:42 PM
L12	2	(namespace "name space") WITH security WITH (rule policy procedure) WITH reader	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:42 PM
L13	19	(namespace "name space") WITH security WITH (rule policy procedure) WITH (select\$4 choos\$4)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:43 PM
L14	0	13 AND 10	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:43 PM
L15	3	13 AND (@ad	(US-PGPUB; USPAT;	OR	ON	ON	2024/05/07

		@prad)<20191018	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)				01:43 PM
L16	141	(EID "electronic identification") WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:46 PM
L17	11	11 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:47 PM
L18	0	17 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:47 PM
L19	4815	(namespace "name space") WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:47 PM
L20	11	19 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:48 PM
L21	0	20 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:48 PM
L22	262497	security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:48 PM
L23	11	16 WITH 22	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:49 PM
L24	0	23 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:49 PM
L25	476	(namespace "name space") WITH security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:49 PM
L26	476	22 AND 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:50 PM
L27	476	22 SAME 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:50 PM
L28	476	22 WITH 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	ON	2024/05/07 01:50 PM

L29	11	28 AND 16	JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:52 PM
L30	0	29 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:52 PM
L31	49	28 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:53 PM
L32	32	31 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:53 PM
L33	433	(select\$4 choos\$4) WITH namespace WITH access\$4	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:56 PM
L34	5841	namespace WITH (rule policy procedure check\$4 algorithm)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:57 PM
L35	159	33 AND 34	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:57 PM
L36	95	35 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:58 PM
L37	23024057	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:59 PM
L38	77	36 AND 37	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:59 PM
L39	77	38 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:00 PM
L40	19	38 AND (@ad @prad)<20191018 AND 9	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:00 PM
L41	1159	(mobile wireless portable cell cellular phone tablet ipad ipod	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2024/05/07 02:20 PM

L42	65	notebook radio) WITH namespace 41 AND wallet	IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:21 PM
L43	50	42 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:21 PM
L44	40942	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:51 PM
L45	1159	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH namespaces	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:52 PM
L46	51	44 AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:52 PM
L47	36	46 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:52 PM
L48	65	wallet AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:13 PM
L49	50	48 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:13 PM
L50	881	45 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:32 PM
L51	50	45 AND (@ad @prad)<20191018 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:32 PM
L52	66	45 AND (@ad @prad)<20191018 AND (eid wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:33 PM
L53	16	52 NOT 51	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:33 PM
L54	43457	(mobile wireless	(US-PGPUB; USPAT;	OR	ON	ON	2024/05/07

L55	40942	portable cell cellular phone tablet ipad ipod notebook radio) WITH (eid wallet)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	03:35 PM
L56	28	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH (wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:35 PM
L57	9	55 AND ((rule policy procedure safeguard) WITH namespace)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:36 PM
L58	8	56 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:36 PM
L59	3	((US-10922386-B1 OR US-11973758-B2).did. AND USPT.dbnm.) OR ((US-20090006642-A1 OR US-20160055248- A1 OR US- 20150040180-A1 OR US-20060265508-A1 OR US-20120159195- A1 OR US- 20220374533-A1).did. AND PGPB.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:40 PM
L60	289	58 AND 10	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:40 PM
L61	14	45 AND reader	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:54 PM
L61	14	45 AND (reader WITH wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	ON	2024/05/07 03:55 PM

L62	12	61 AND (@ad @prad)<20191018	JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:56 PM
L63	16	(list\$4 roster) WITH namespaces WITH (reader cardreader)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 05:46 PM
L64	10	(bytestring "byte string") WITH template WITH (rules policies)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 05:47 PM
L65	1	63 AND 64	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 05:47 PM
L66	0	65 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 05:47 PM
L67	1	"20220374533"	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L68	159	((("THALES") near3 ("DIS") near3 ("FRANCE") near3 ("SAS"))).AS,AANM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L69	16	((("FAHER") near3 ("Mourad")) OR (("BAYLE") near3 ("Carole"))).INV.	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L70	170	2 4	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L71	2	5 AND wallet.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L72	1	6 AND eid.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L73	0	6 AND eid.clm.	(USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L74	212175	(G06F21/62 OR H04L63/101 OR H04L63/20 OR G06Q50/265 OR G06Q20/3227,326,363, 367,3825,3827,4014).c pc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L75	168724	9 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L76	489	(namespace "name space") WITH security	(US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	ON	2024/08/19 08:10 AM

L77	2	WITH (rule policy procedure) (namespace "name space") WITH security WITH (rule policy procedure) WITH reader	JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L78	19	(namespace "name space") WITH security WITH (rule policy procedure) WITH (select\$4 choos\$4)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L79	0	13 AND 10	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L80	3	13 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L81	143	(EID "electronic identification") WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L82	11	11 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L83	0	17 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L84	4935	(namespace "name space") WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L85	11	19 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L86	0	20 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L87	268396	security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L88	11	16 WITH 22	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L89	0	23 AND (@ad	(US-PGPUB; USPAT;	OR	ON	ON	2024/08/19

		@prad)<20191018	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)				08:10 AM
L90	489	(namespace "name space") WITH security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L91	489	22 AND 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L92	489	22 SAME 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L93	489	22 WITH 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L94	11	28 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L95	0	29 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L96	49	28 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L97	32	31 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L98	442	(select\$4 choos\$4) WITH namespace WITH access\$4	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L99	5989	namespace WITH (rule policy procedure check\$4 algorithm)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L100	163	33 AND 34	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L101	95	35 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L102	23295819	(mobile wireless portable cell cellular	(US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	ON	2024/08/19 08:10 AM

L103	77	phone tablet ipad ipod notebook radio) 36 AND 37	JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L104	77	38 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L105	19	38 AND (@ad @prad)<20191018 AND 9	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L106	1186	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH namespace	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L107	65	41 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L108	50	42 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L109	42090	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L110	1186	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH namespaces	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L111	51	44 AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L112	36	46 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L113	65	wallet AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L114	50	48 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM

L115	882	45 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L116	50	45 AND (@ad @prad)<20191018 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L117	66	45 AND (@ad @prad)<20191018 AND (eid wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L118	16	52 NOT 51	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L119	44641	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH (eid wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L120	42090	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH (wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L121	28	55 AND ((rule policy procedure safeguard) WITH namespace)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L122	9	56 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L123	8	((US-10922386-B1 OR US-11973758-B2).did. AND USPT.dbnm.) OR ((US-20090006642-A1 OR US-20160055248-A1 OR US-20150040180-A1 OR US-20060265508-A1 OR US-20120159195-A1 OR US-20220374533-A1).did. AND PGPB.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L124	3	58 AND 10	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA,	OR	ON	ON	2024/08/19 08:10 AM

L125	274	45 AND reader	EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L126	14	45 AND (reader WITH wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L127	12	61 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L128	16	{list\$4 roster) WITH namespaces WITH (reader cardreader)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L129	10	(bytestring "byte string") WITH template WITH (rules policies)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L130	1	63 AND 64	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L131	0	65 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N1	75477	(G06F21/62 OR H04L63/101 OR H04L63/20 OR G06Q50/265 OR G06Q20/3227,326,363,367,3825,3827,4014).c pc.	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:08 AM
N2	3337	N1 AND wallet.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:09 AM
N3	5	N2 AND ("electronic	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19

N4	1	identification" eid).clm. N3 AND namespace.clm.	(US-PGPUB; USPAT)	OR	ON	ON	08:09 AM 2024/08/19 08:10 AM
N5	0	N3 AND namespace.clm.	(USPAT)	OR	ON	ON	2024/08/19 08:10 AM



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

180929 7590 08/28/2024
THALES DIS CPL USA, INC.
Intellectual Property
900 South Pine Island Road
Suite 710
PLANTATION, FL 33324

EXAMINER

KEEHN, RICHARD G

ART UNIT

PAPER NUMBER

2444

DATE MAILED: 08/28/2024

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/767,153	04/07/2022	Mourad FAHER	GMT4110US/WO MQ/MB	2044

TITLE OF INVENTION: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1200	\$0.00	\$0.00	\$1200	11/29/2024

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

180929 7590 08/28/2024
THALES DIS CPL USA, INC.
Intellectual Property
900 South Pine Island Road
Suite 710
PLANTATION, FL 33324

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17767.153	04/07/2022	Mourad FAHER	GMT4110US/WO MQ/MB	2044

TITLE OF INVENTION: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1200	\$0.00	\$0.00	\$1200	11/29/2024

EXAMINER	ART UNIT	CLASS-SUBCLASS
KEEHN, RICHARD G	2444	726-004000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____
- (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
- 3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required)

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

- ☐ Electronic Payment (via the USPTO patent electronic filing system) ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/767,153	04/07/2022	Mourad FAHER	GMT4110US/WO MQ/MB	2044
180929	7590	08/28/2024	EXAMINER	
THALES DIS CPL USA, INC.			KEEHN, RICHARD G	
Intellectual Property			ART UNIT	
900 South Pine Island Road			2444	
Suite 710			DATE MAILED: 08/28/2024	
PLANTATION, FL 33324				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.** Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is **COMMERCE/PAT-TM-7 Patent Application Files**, available in the Federal Register at 78 FR 19243 (March 29, 2013).

<https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf>

Routine uses of the information in this record may include disclosure to:

- 1) law enforcement, in the event that the system of records indicates a violation or potential violation of law;
- 2) a federal, state, local, or international agency, in response to its request;
- 3) a contractor of the USPTO having need for the information in order to perform a contract;
- 4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record;
- 5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record;
- 6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations;
- 7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals;
- 8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c));
- 9) the Office of Personnel Management (OPM) for personnel research purposes; and
- 10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Notice of Allowability	Application No. 17/767,153	Applicant(s) FAHER et al.	
	Examiner RICHARD G KEEHN	Art Unit 2444	AIA (FITF) Status Yes

– The MAILING DATE of this communication appears on the cover sheet with the correspondence address–

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 8/12/2024.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are 1-16. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
Certified copies:
a) ☒ All b) ☐ Some* c) ☐ None of the:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892) 2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____ 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____ 4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____	5. ☐ Examiner's Amendment/Comment 6. ☒ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____
--	---

/RICHARD G KEEHN/ Primary Examiner, Art Unit 2444	
--	--

DETAILED ACTION

1. Claims 1-16 are pending and have been examined.
2. There are no new, nor canceled claims.

Notice of Pre-AIA or AIA Status

3. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Response to Arguments

4. Applicant's amendments with arguments, see pages 6 and 7, filed 8/12/2024, with respect to the rejection of Claims 2, 3, 6-8, 10 and 12-16 under 35 U.S.C. 112(b) have been fully considered and are persuasive. **The rejection of Claims 2, 3, 6-8, 10 and 12-16 under 35 U.S.C. 112(b) has been withdrawn.**

Allowable Subject Matter

5. Claims 1-16 are allowed.
6. **The following is an examiner's statement of reasons for allowance:** It must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). Here, the limitations presented in the independent claims,

taken together as a whole and as presented, cannot be rejected by the prior art of record without using a level of hindsight reasoning that is impermissible. Specifically, the closest prior-art references US 2015/0040180 A1, US 2012/0159195 A1 and US 2009/0006642 A1, either alone or in combination, do not disclose all of the limitations required in the independent claims.

7. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RICHARD G KEEHN whose telephone number is (571)270-5007. The examiner can normally be reached M-F 9:00am - 5:00pm Eastern.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is

available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/RICHARD G KEEHN/
Primary Examiner, Art Unit 2444



UNITED STATES
PATENT AND TRADEMARK OFFICE

Page 1 of 2
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/767,153	10/25/2024 09:32:27 AM Z ET	GMT4110US/WO MQ/MB

Title of Invention

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Application Information

APPLICATION TYPE	Utility - U.S. National Stage under 35 USC 371	PATENT #	-
CONFIRMATION #	2044	FILED BY	GHEZALI Djouher
PATENT CENTER #	67717483	FILING DATE	04/07/2022
CUSTOMER #	180929	FIRST NAMED INVENTOR	Mourad FAHER
INTL. APPLICATION #	-	INTL. FILING DATE	-
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Adam Lewental

Documents

TOTAL DOCUMENTS: 4

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
GMT4110US_Request_RCE.pdf	3	Request for Continued Examination (RCE)	1628 KB
GMT4110US_IDS.pdf	4	Information Disclosure Statement (IDS) Form (SB08)	1010 KB
KR1020190115361.pdf	36	Foreign Reference	791 KB
US2020391695A1_Counterpart_KR1020190115361.pdf	28	Other reference-Patent/Application/Search Documents	2220 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
GMT4110US_Request_RCE.pdf	7428F5C02DBE93E3C563F2C875D4A8BD935AA4B286FB0CA4 BE2381310C614F1CF92505218797F7DEAABF347A25E7E2C8A 2BE5D9A2006C8DE7A0237ABCEA6CF4F
GMT4110US_IDS.pdf	CF6795023CD10B7FBB2E7FA675557C155F300602202903BB44 B2337DBBF7F6C9FFC7E330E79B9E345829D25865D658DE071 FE0C688703D28DCE7B5A2691942C0
KR1020190115361.pdf	54E04C99363B6B420A4DF37D034447FF373A6FC9C4C6883A2 553E14B0DC42D9BF65AC8D39FEE1D32255C983336C764CED 05EE26956C0777991FADBAF9444C320
US2020391695A1_Counterpart _KR1020190115361.pdf	048A5662BF78E4ECA5AFAB3282C108CC03795FB5CC6411F51 F951F24858044728E9983E02008F172B2166C197E4AED5EFBA B93CAA5DFBF04DAC9881277D2F51E

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION # 17/767,153	RECEIPT DATE / TIME 10/25/2024 09:32:27 AM Z ET	ATTORNEY DOCKET # GMT4110US/WO MQ/MB
------------------------------------	---	--

Title of Invention

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Application Information

APPLICATION TYPE	Utility - U.S. National Stage under 35 USC 371	PATENT #	-
CONFIRMATION #	2044	FILED BY	GHEZALI Djouher
PATENT CENTER #	67717483	AUTHORIZED BY	Adam Lewental
CUSTOMER #	180929	FILING DATE	04/07/2022
INTL. APPLICATION #	-	INTL. FILING DATE	-
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Mourad FAHER

Payment Information

PAYMENT METHOD DA / 604092	PAYMENT TRANSACTION ID E202400033058777	PAYMENT AUTHORIZED BY Adam Lewental
-------------------------------	--	--

FEE CODE	DESCRIPTION	ITEM PRICE(\$)	QUANTITY	ITEM TOTAL(\$)
1806	SUBMISSION OF AN INFORMATION DISCLOSURE STATEMENT	260.00	1	260.00
1801	REQUEST FOR CONTINUED EXAMINATION (RCE) - 1ST REQUEST (SEE 37 CFR 1.114)	1360.00	1	1360.00
TOTAL AMOUNT:				\$1,620.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0115361
(43) 공개일자 2019년10월11일

(51) 국제특허분류(Int. Cl.)

B60R 25/10 (2006.01) B60R 25/24 (2013.01)
G06F 21/35 (2013.01)

(52) CPC특허분류

B60R 25/10 (2013.01)
B60R 25/24 (2013.01)

(21) 출원번호 10-2018-0038324

(22) 출원일자 2018년04월02일

심사청구일자 없음

(71) 출원인

삼성전자주식회사

경기도 수원시 영통구 삼성로 129 (매탄동)

(72) 발명자

양이

경기도 수원시 영통구 효원로 363, 103동 801호

김중환

경기도 용인시 수지구 상현로 101, 113동 1702호
(상현동, 상현마을수지셀트힐아파트)

(뒷면에 계속)

(74) 대리인

윤앤리특허법인(유한)

전체 청구항 수 : 총 20 항

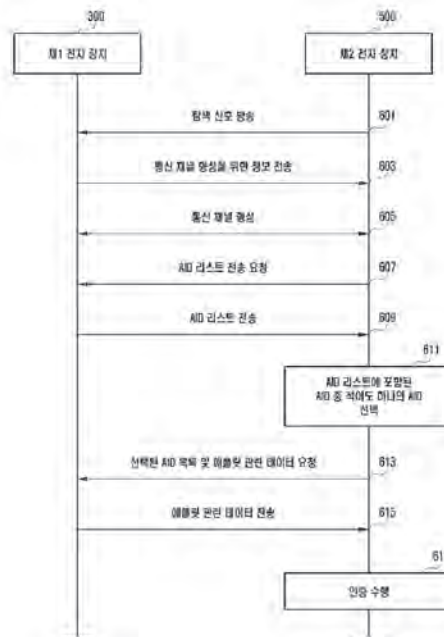
(54) 발명의 명칭 외부 전자 장치의 키와 관련된 어플리케이션을 관리하는 전자 장치 및 전자 장치의 동작 방법

(57) 요약

다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 전자 장치는 외부 전자 장치와 통신을 수행하는 통신 모듈; 및 외부 전자 장치의 인증에 이용되는 키를 관리하는 어플릿과 관련된 데이터의 변경을 모니터링하고, 어플릿과 관련된 정보를 관리하고, 적어도 하나 이상의 어플릿 식별자(applet identification,

(뒷면에 계속)

도 6



AID)를 포함하는 AID 리스트 및 상기 애플릿을 저장하는 보안 모듈을 포함하고, 상기 보안 모듈은 상기 외부 전자 장치로부터 상기 AID(Application identifier) 리스트를 전송할 것을 요청하는 신호를 수신하고, 상기 요청 신호의 수신에 대응하여, 상기 통신 모듈을 통하여 상기 AID 리스트를 상기 외부 전자 장치로 전송하고, 상기 외부 전자 장치로부터 상기 AID 리스트에 포함된 상기 AID들 중 상기 외부 전자 장치에 의해 선택된 적어도 하나 이상의 AID와 연관된 애플릿과 관련된 정보를 요청하는 신호를 수신하고, 상기 선택된 AID에 대응하는 애플릿과 관련된 정보를 상기 외부 전자 장치로 전송하도록 설정될 수 있다.

이 밖에 다양한 실시예들이 가능하다.

(52) CPC특허분류

G06F 21/35 (2013.01)

(72) 발명자

진병학

경기도 수원시 팔달구 권광로 243, 202동 804호(인계동, 래미안 노블클래스)

최보근

서울특별시 양천구 목동서로 400 신시가치10단지아파트 1021동 1006호

별첨서

청구범위

청구항 1

전자 장치에 있어서,

외부 전자 장치와 통신을 수행하는 통신 모듈; 및

외부 전자 장치의 인증에 이용되는 키를 관리하는 애플릿과 관련된 데이터의 변경을 모니터링하고, 애플릿과 관련된 정보를 관리하고, 적어도 하나 이상의 애플릿 식별자(applet identification, AID)를 포함하는 AID 리스트 및 상기 애플릿을 저장하는 보안 모듈을 포함하고,

상기 보안 모듈은

상기 외부 전자 장치로부터 상기 AID(Application identifier) 리스트를 전송할 것을 요청하는 신호를 수신하고,

상기 요청 신호의 수신에 대응하여, 상기 통신 모듈을 통하여 상기 AID 리스트를 상기 외부 전자 장치로 전송하고,

상기 외부 전자 장치로부터 상기 AID 리스트에 포함된 상기 AID들 중 상기 외부 전자 장치에 의해 선택된 적어도 하나 이상의 AID와 연관된 애플릿과 관련된 정보를 요청하는 신호를 수신하고,

상기 선택된 AID에 대응하는 애플릿과 관련된 정보를 상기 외부 전자 장치로 전송하도록 설정된 전자 장치.

청구항 2

제 1항에 있어서,

상기 애플릿과 관련된 정보는

상기 애플릿이 저장된 주소, 상기 AID, 상기 외부 전자 장치의 모델 식별자, 상기 애플릿의 활성화 여부를 지시하는 데이터, 상기 애플릿 각각에 지정된 우선 순위, 또는 상기 애플릿의 구체적인 데이터(application-specific data) 중 적어도 하나 이상을 포함하는 전자 장치.

청구항 3

제 2항에 있어서,

상기 애플릿의 구체적인 데이터는

상기 외부 전자 장치의 이용 허용 시간, 상기 외부 전자 장치의 이용 가능한 지역 범위 정보(geofencing limitation data), 또는 상기 외부 전자 장치가 수행 가능한 적어도 하나 이상의 기능에 대한 허용 여부를 지시하는 정보를 포함하는 전자 장치.

청구항 4

제 1항에 있어서,

상기 AID 리스트는

상기 애플릿 각각에 지정된 우선 순위에 기반하여 배열된 전자 장치.

청구항 5

제 1항에 있어서,

상기 보안 모듈은

상기 보안 모듈에 저장된 데이터를 관리하는 CRS; 및

상기 애플릿과 관련된 데이터의 변경을 모니터링하고, 상기 애플릿과 관련된 정보를 관리하는 PVKSE(proximity vehicle key system environment)를 더 포함하고,

상기 CRS는

상기 애플릿의 설정을 변경할 것을 요청하는 신호에 대응하여, 적어도 하나의 애플릿의 설정을 변경하고, 상기 데이터의 변경을 알리는 신호를 상기 PVKSE로 전송하고,

상기 PVKSE는

상기 데이터의 변경을 알리는 신호를 수신함에 대응하여, 상기 애플릿과 관련된 데이터를 변경하도록 설정된 전자 장치.

청구항 6

제 5항에 있어서,

상기 PVKSE 및 상기 CRS는 상기 보안 모듈의 발급된 보안 도메인(issued security domain)에 저장되며, 상기 애플릿은 추가 보안 도메인(supplementary security domain)에 저장되도록 설정된 전자 장치.

청구항 7

제 1항에 있어서,

상기 애플릿과 관련된 정보는

상기 애플릿마다 구분된 추가 보안 도메인에 저장되도록 설정된 전자 장치.

청구항 8

제 5항에 있어서,

상기 PVKSE는

상기 애플릿의 변경을 감지한 경우, 상기 애플릿과 관련된 정보를 변경하도록 설정된 전자 장치.

청구항 9

전자 장치에 있어서,

메모리;

외부 전자 장치와의 인증에 이용되는 데이터를 저장하는 보안 모듈;

통신 모듈; 및

프로세서를 포함하고,

상기 보안 모듈은

외부 전자 장치와의 연결을 위한 연결 요청 신호를 방송(broadcasting)하고, 상기 방송된 신호에 응답한 외부

전자 장치와 통신 채널을 수립하고,

상기 외부 전자 장치에 저장된 적어도 하나 이상의 AID(Application identifier)를 포함하는 AID 리스트를 전송할 것을 요청하는 신호를 전송하고,

상기 외부 전자 장치가 전송한 상기 AID 리스트에 포함된 AID 중 적어도 하나 이상의 AID를 선택하고,

상기 선택된 AID에 대응하는 애플릿을 지시하는 정보 및 상기 애플릿과 관련된 정보를 요청하는 신호를 상기 외부 전자 장치에 전송하고,

상기 외부 전자 장치로부터 수신한 상기 애플릿과 관련된 정보를 이용하여 상기 외부 전자 장치와 인증을 수행하도록 설정된 전자 장치.

청구항 10

제 9항에 있어서,

상기 보안 모듈은

상기 애플릿에 지정된 우선 순위에 기반하여 인증을 수행하도록 설정된 전자 장치.

청구항 11

제 10항에 있어서,

상기 보안 모듈은

상기 애플릿과 관련된 정보를 이용하여 상기 외부 전자 장치에 대한 인증을 수행하고,

상기 인증이 실패함을 확인함에 대응하여, 상기 인증이 수행된 AID보다 우선 순위가 낮은 AID를 선택하고,

상기 선택된 AID에 대응하는 애플릿과 관련된 관련 정보를 요청하도록 설정된 전자 장치.

청구항 12

제 9항에 있어서,

상기 보안 모듈은

상기 AID 리스트에 포함된 AID들 중 상기 전자 장치의 제조사에 대응하는 AID를 선택하도록 설정된 전자 장치.

청구항 13

제 9항에 있어서,

상기 보안 모듈은

상기 AID 리스트에 포함된 AID들 중 상기 전자 장치의 제조사에 대응하는 AID 중, 우선 순위가 가장 높은 AID를 선택하도록 설정된 전자 장치.

청구항 14

제 9항에 있어서,

상기 AID 리스트는

상기 외부 전자 장치에 대응하는 적어도 하나 이상의 AID 및 다른 사용자가 이용 가능한 공유된 외부 전자 장치

에 대응하는 적어도 하나 이상의 AID를 포함하는 전자 장치.

청구항 15

제 9항에 있어서,

상기 애플릿과 관련된 정보는

상기 애플릿이 저장된 주소, 상기 AID, 상기 전자 장치의 모델 식별자, 상기 애플릿의 활성화 여부를 지시하는 데이터, 상기 애플릿 각각에 지정된 우선 순위, 또는 상기 애플릿의 구체적인 데이터(application-specific data) 중 적어도 하나 이상을 포함하는 전자 장치.

청구항 16

제 15항에 있어서,

상기 애플릿의 구체적인 데이터는

상기 전자 장치의 이용 허용 시간, 상기 전자 장치의 이용 가능한 지역 범위 정보(geofencing limitation data), 또는 상기 전자 장치가 수행 가능한 적어도 하나 이상의 기능에 대한 허용 여부를 지시하는 정보를 포함하는 전자 장치.

청구항 17

제 16항에 있어서,

상기 보안 모듈은

상기 애플릿의 구체적인 데이터에 기반하여 상기 전자 장치가 제공 가능한 기능들 중 활성화될 기능을 결정하도록 설정된 전자 장치.

청구항 18

제 9항에 있어서,

상기 전자 장치는

운송 수단(vehicle)이거나, 운송 수단(vehicle)과 전기적으로 연결되는 전자 장치.

청구항 19

전자 장치의 동작 방법에 있어서,

외부 전자 장치와의 연결을 위한 연결 요청 신호를 방송(broadcasting)하고, 상기 방송된 신호에 응답한 외부 전자 장치와 통신 채널을 수립하는 동작;

상기 외부 전자 장치에 저장된 적어도 하나 이상의 AID(Application identifier)를 포함하는 AID 리스트를 전송할 것을 요청하는 신호를 전송하는 동작;

상기 외부 전자 장치가 전송한 상기 AID 리스트에 포함된 AID 중 적어도 하나 이상의 AID를 선택하는 동작;

상기 선택된 AID에 대응하는 애플릿을 지시하는 정보 및 상기 선택된 AID에 대응하는 애플릿과 관련된 정보를 요청하는 동작; 및

상기 외부 전자 장치로부터 수신한 상기 애플릿과 관련된 정보를 이용하여 상기 외부 전자 장치와 인증을 수행

하는 동작을 포함하는 전자 장치의 동작 방법.

청구항 20

제 19항에 있어서,

상기 적어도 하나 이상의 AID를 선택하는 동작은

상기 AID 리스트에 포함된 AID들 중 상기 전자 장치의 제조사와 다른 제조사에 대응하는 AID를 제외한 나머지 AID를 선택하는 동작을 포함하고,

상기 외부 전자 장치와 인증을 수행하는 동작은

상기 AID에 지정된 우선 순위에 기반하여 인증을 수행하는 동작을 포함하는 전자 장치의 동작 방법.

발명의 설명

기술 분야

[0001] 본 발명의 다양한 실시예는, 외부 전자 장치의 키와 관련된 어플리케이션을 관리하는 전자 장치 및 전자 장치의 동작 방법에 관한 것이다.

배경 기술

[0003] 무선 통신을 지원하는 스마트 키를 통해 외부 전자 장치와 인증을 수행할 수 있는 기술이 개발되고 있다. 예를 들어, 외부 전자 장치가 운송 수단인 경우, 운송 수단의 문의 잠금을 해제하거나, 운송 수단의 엔진의 시동을 켜는 등의 운송 수단이 제공할 수 있는 기능을 수행할 수 있는 스마트 키와 관련된 기술이 개발되고 있다. 스마트 키는 운송 수단과 근거리 통신을 이용해 인증 절차를 수행하고, 인증 완료 후 잠금 해제나 시동 등 운송 수단의 기능을 활성화할 수 있다.

[0004] 최근에는 운송 수단의 기능을 활성화하기 위한 별도의 스마트 키를 이용하지 않고, 사용자가 휴대 가능한 스마트폰, 웨어러블 기기 등 휴대 단말을 이용하여 운송 수단이 제공할 수 있는 기능을 수행하는 기술이 등장하고 있다.

[0005] 최근의 운송 수단 제조 업체는 휴대 단말에 운송 수단의 키를 제공하고, 운송 수단의 소유주 또는 운송 수단 공유자들은 휴대 단말을 이용하여 일반적인 스마트 키와 같이 운송 수단의 문을 열거나, 운송 수단의 엔진을 점화하는 등의 다양한 기능을 수행할 수 있다.

발명의 내용

해결하려는 과제

[0007] 운송 수단의 키 또는 운송 수단의 키의 관리를 위한 어플리케이션은, 보안성을 제공하기 위해서, 휴대 단말에 별도로 구비된 보안 모듈(security module)에 기반한 운송 수단 키 솔루션을 이용할 수 있다.

[0008] 한 명의 사용자가 복수의 운송 수단을 이용하거나, 복수의 사용자가 차량을 공동으로 이용하는 등의 상황이 있을 수 있다. 이러한 상황에서 사용자가 하나의 휴대 단말을 복수의 운송 수단 각각의 키로 사용함에 있어서 보안성을 확보하면서 동시에 사용의 편리성을 제공하는데 어려움이 있을 수 있다.

[0009] 특히, 운송 수단은, 운송 수단과 통신 연결이 수립된 휴대 단말이 얼마나 많은 운송 수단의 인증에 이용되는 어플리케이션을 가지고 있는지 알 수 없다. 운송 수단의 인증에 이용되는 복수의 어플리케이션들 모두 인증을 시도하는 경우, 인증에 소요되는 시간이 늘어날 수 있다.

파제의 해결 수단

- [0011] 본 발명의 다양한 실시예에 따른 전자 장치는 외부 전자 장치와 통신을 수행하는 통신 모듈; 및 외부 전자 장치의 인증에 이용되는 키를 관리하는 애플릿과 관련된 데이터의 변경을 모니터링하고, 애플릿과 관련된 정보를 관리하고, 적어도 하나 이상의 애플릿 식별자(applet identification, AID)를 포함하는 AID 리스트 및 상기 애플릿을 저장하는 보안 모듈을 포함하고, 상기 보안 모듈은 상기 외부 전자 장치로부터 상기 AID(Application identifier) 리스트를 전송할 것을 요청하는 신호를 수신하고, 상기 요청 신호의 수신에 대응하여, 상기 통신 모듈을 통하여 상기 AID 리스트를 상기 외부 전자 장치로 전송하고, 상기 외부 전자 장치로부터 상기 AID 리스트에 포함된 상기 AID들 중 상기 외부 전자 장치에 의해 선택된 적어도 하나 이상의 AID와 연관된 애플릿과 관련된 정보를 요청하는 신호를 수신하고, 상기 선택된 AID에 대응하는 애플릿과 관련된 정보를 상기 외부 전자 장치로 전송하도록 설정될 수 있다.
- [0012] 본 발명의 다양한 실시예에 따른 전자 장치는 메모리; 외부 전자 장치와의 인증에 이용되는 데이터를 저장하는 보안 모듈; 통신 모듈; 및 프로세서를 포함하고, 상기 보안 모듈은 외부 전자 장치와의 연결을 위한 연결 요청 신호를 방송(broadcasting)하고, 상기 방송된 신호에 응답한 외부 전자 장치와 통신 채널을 수립하고, 상기 외부 전자 장치에 저장된 적어도 하나 이상의 AID(Application identifier)를 포함하는 AID 리스트를 전송할 것을 요청하는 신호를 전송하고, 상기 외부 전자 장치가 전송한 상기 AID 리스트에 포함된 AID 중 적어도 하나 이상의 AID를 선택하고, 상기 선택된 AID에 대응하는 애플릿을 지시하는 정보 및 상기 애플릿과 관련된 정보를 요청하는 신호를 상기 외부 전자 장치로 전송하고, 상기 외부 전자 장치로부터 수신한 상기 애플릿과 관련된 정보를 이용하여 상기 외부 전자 장치와 인증을 수행하도록 설정될 수 있다.
- [0013] 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법은 외부 전자 장치와의 연결을 위한 연결 요청 신호를 방송(broadcasting)하고, 상기 방송된 신호에 응답한 외부 전자 장치와 통신 채널을 수립하는 동작; 상기 외부 전자 장치에 저장된 적어도 하나 이상의 AID(Application identifier)를 포함하는 AID 리스트를 전송할 것을 요청하는 신호를 전송하는 동작; 상기 외부 전자 장치가 전송한 상기 AID 리스트에 포함된 AID 중 적어도 하나 이상의 AID를 선택하는 동작; 상기 선택된 AID에 대응하는 애플릿을 지시하는 정보 및 상기 선택된 AID에 대응하는 애플릿과 관련된 정보를 요청하는 동작; 및 상기 외부 전자 장치로부터 수신한 상기 애플릿과 관련된 정보를 이용하여 상기 외부 전자 장치와 인증을 수행하는 동작을 포함할 수 있다.

발명의 효과

- [0015] 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법은, 전자 장치에 저장된 애플릿들 모두에 대한 인증을 수행하지 않고, 외부 전자 장치가 선택된 애플릿 식별자에 대한 인증을 수행함으로써, 인증에 소요되는 시간을 줄일 수 있다.

도면의 간단한 설명

- [0017] 도 1은 본 발명의 다양한 실시예에 따른, 전자 장치의 블록도이다.
- 도 2는 본 발명의 다양한 실시예에 따른 전자 장치 상에서 동작하는 프로그램의 블록도이다.
- 도 3은 본 발명의 다양한 실시예에 따른 전자 장치의 블록도이다.
- 도 4는 본 발명의 다양한 실시예에 따른 전자 장치에서, 보안 모듈을 도시한 블록도이다.
- 도 5는 본 발명의 다양한 실시예에 따른 전자 장치의 블록도이다.
- 도 6은 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법의 동작 흐름도이다.
- 도 7은 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법에서, 전자 장치의 인증에 이용되는 애플릿을 보안 모듈에 설치하는 동작을 도시한 작 흐름도이다.
- 도 8a는 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법에서, 전자 장치의 인증에 이용되는 애플릿의 활성화하는 동작을 도시한 동작 흐름도이다.

도 8b는 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법에서, 전자 장치의 인증에 이용되는 애플릿의 우선 순위를 설정하는 동작을 도시한 동작 흐름도이다.

도 9는 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법에서, 도 3의 외부 전자 장치 상에서 전자 장치의 인증을 수행하는 동작을 도시한 동작 흐름도이다.

도 10은 본 발명의 다양한 실시예에 따른 전자 장치가 전송하는 애플릿과 관련된 데이터의 구체적인 예시를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0018] 도 1은, 다양한 실시예들에 따른, 네트워크 환경(100) 내의 전자 장치(101)의 블록도이다. 도 1을 참조하면, 네트워크 환경(100)에서 전자 장치(101)는 제 1 네트워크(198)(예: 근거리 무선 통신 네트워크)를 통하여 전자 장치(102)와 통신하거나, 또는 제 2 네트워크(199)(예: 원거리 무선 통신 네트워크)를 통하여 전자 장치(104) 또는 서버(108)와 통신할 수 있다. 일 실시예에 따르면, 전자 장치(101)는 서버(108)를 통하여 전자 장치(104)와 통신할 수 있다. 일 실시예에 따르면, 전자 장치(101)는 프로세서(120), 메모리(130), 입력 장치(150), 음향 출력 장치(155), 표시 장치(160), 오디오 모듈(170), 센서 모듈(176), 인터페이스(177), 햅틱 모듈(179), 카메라 모듈(180), 전력 관리 모듈(188), 배터리(189), 통신 모듈(190), 가입자 식별 모듈(196), 또는 안테나 모듈(197)을 포함할 수 있다. 어떤 실시예에서는, 전자 장치(101)에는, 이 구성요소들 중 적어도 하나(예: 표시 장치(160) 또는 카메라 모듈(180))가 생략되거나, 하나 이상의 다른 구성 요소가 추가될 수 있다. 어떤 실시예에서는, 이 구성요소들 중 일부들은 하나의 통합된 회로로 구현될 수 있다. 예를 들면, 센서 모듈(176)(예: 지문 센서, 홍채 센서, 또는 조도 센서)은 표시 장치(160)(예: 디스플레이)에 임베디드된 채 구현될 수 있다.
- [0019] 프로세서(120)는, 예를 들면, 소프트웨어(예: 프로그램(140))를 실행하여 프로세서(120)에 연결된 전자 장치(101)의 적어도 하나의 다른 구성요소(예: 하드웨어 또는 소프트웨어 구성요소)를 제어할 수 있고, 다양한 데이터 처리 또는 연산을 수행할 수 있다. 일 실시예에 따르면, 데이터 처리 또는 연산의 적어도 일부로서, 프로세서(120)는 다른 구성요소(예: 센서 모듈(176) 또는 통신 모듈(190))로부터 수신된 명령 또는 데이터를 휘발성 메모리(132)에 로드하고, 휘발성 메모리(132)에 저장된 명령 또는 데이터를 처리하고, 결과 데이터를 비휘발성 메모리(134)에 저장할 수 있다. 일 실시예에 따르면, 프로세서(120)는 메인 프로세서(121)(예: 중앙 처리 장치 또는 어플리케이션 프로세서), 및 이와는 독립적으로 또는 함께 운영 가능한 보조 프로세서(123)(예: 그래픽 처리 장치, 이미지 시그널 프로세서, 센서 허브 프로세서, 또는 커뮤니케이션 프로세서)를 포함할 수 있다. 추가적으로 또는 대체적으로, 보조 프로세서(123)는 메인 프로세서(121)보다 지전력을 사용하거나, 또는 지정된 기능에 특화되도록 설정될 수 있다. 보조 프로세서(123)는 메인 프로세서(121)와 별개로, 또는 그 일부로서 구현될 수 있다.
- [0020] 보조 프로세서(123)는, 예를 들면, 메인 프로세서(121)가 인액티브(예: 슬립) 상태에 있는 동안 메인 프로세서(121)를 대신하여, 또는 메인 프로세서(121)가 액티브(예: 어플리케이션 실행) 상태에 있는 동안 메인 프로세서(121)와 함께, 전자 장치(101)의 구성요소들 중 적어도 하나의 구성요소(예: 표시 장치(160), 센서 모듈(176), 또는 통신 모듈(190))와 관련된 기능 또는 상태들의 적어도 일부를 제어할 수 있다. 일 실시예에 따르면, 보조 프로세서(123)(예: 이미지 시그널 프로세서 또는 커뮤니케이션 프로세서)는 기능적으로 관련 있는 다른 구성요소(예: 카메라 모듈(180) 또는 통신 모듈(190))의 일부로서 구현될 수 있다.
- [0021] 메모리(130)는, 전자 장치(101)의 적어도 하나의 구성요소(예: 프로세서(120) 또는 센서모듈(176))에 의해 사용되는 다양한 데이터를 저장할 수 있다. 데이터는, 예를 들어, 소프트웨어(예: 프로그램(140)) 및, 이와 관련된 명령에 대한 입력 데이터 또는 출력 데이터를 포함할 수 있다. 메모리(130)는, 휘발성 메모리(132) 또는 비휘발성 메모리(134)를 포함할 수 있다.
- [0022] 프로그램(140)은 메모리(130)에 소프트웨어로서 저장될 수 있으며, 예를 들면, 운영 체제(142), 미들 웨어(144) 또는 어플리케이션(146)을 포함할 수 있다.
- [0023] 입력 장치(150)는, 전자 장치(101)의 구성요소(예: 프로세서(120))에 사용될 명령 또는 데이터를 전자 장치(101)의 외부(예: 사용자)로부터 수신할 수 있다. 입력 장치(150)은, 예를 들면, 마이크, 마우스, 또는 키보드를 포함할 수 있다.
- [0024] 음향 출력 장치(155)는 음향 신호를 전자 장치(101)의 외부로 출력할 수 있다. 음향 출력 장치(155)는, 예를 들면, 스피커 또는 리시버를 포함할 수 있다. 스피커는 멀티미디어 재생 또는 녹음 재생과 같이 일반적인 용도로

사용될 수 있고, 리시버는 착신 전화를 수신하기 위해 사용될 수 있다. 일실시예에 따르면, 리시버는 스피커와 별개로, 또는 그 일부로서 구현될 수 있다.

- [0025] 표시 장치(160)는 전자 장치(101)의 외부(예: 사용자)로 정보를 시각적으로 제공할 수 있다. 표시 장치(160)은, 예를 들면, 디스플레이, 홀로그램 장치, 또는 프로젝터 및 해당 장치를 제어하기 위한 제어 회로를 포함할 수 있다. 일실시예에 따르면, 표시 장치(160)는 터치를 감지하도록 설정된 터치 회로(touch circuitry), 또는 상기 터치에 의해 발생하는 힘의 세기를 측정하도록 설정된 센서 회로(예: 압력 센서)를 포함할 수 있다.
- [0026] 오디오 모듈(170)은 소리를 전기 신호로 변환시키거나, 반대로 전기 신호를 소리로 변환시킬 수 있다. 일실시예에 따르면, 오디오 모듈(170)은, 입력 장치(150)를 통해 소리를 획득하거나, 음향 출력 장치(155), 또는 전자 장치(101)와 직접 또는 무선으로 연결된 외부 전자 장치(예: 전자 장치(102)) (예: 스피커 또는 헤드폰))를 통해 소리를 출력할 수 있다.
- [0027] 센서 모듈(176)은 전자 장치(101)의 작동 상태(예: 전력 또는 온도), 또는 외부의 환경 상태(예: 사용자 상태)를 감지하고, 감지된 상태에 대응하는 전기 신호 또는 데이터 값을 생성할 수 있다. 일실시예에 따르면, 센서 모듈(176)은, 예를 들면, 제스처 센서, 자이로 센서, 기압 센서, 마그네틱 센서, 가속도 센서, 그림 센서, 근접 센서, 컬러 센서, IR(infrared) 센서, 생체 센서, 온도 센서, 습도 센서, 또는 조도 센서를 포함할 수 있다.
- [0028] 인터페이스(177)는 전자 장치(101)의 외부 전자 장치(예: 전자 장치(102))와 직접 또는 무선으로 연결되기 위해 사용될 수 있는 하나 이상의 지정된 프로토콜들을 지원할 수 있다. 일실시예에 따르면, 인터페이스(177)는, 예를 들면, HDMI(high definition multimedia interface), USB(universal serial bus) 인터페이스, SD카드 인터페이스, 또는 오디오 인터페이스를 포함할 수 있다.
- [0029] 연결 단자(178)는, 그를 통해서 전자 장치(101)가 외부 전자 장치(예: 전자 장치(102))와 물리적으로 연결될 수 있는 커넥터를 포함할 수 있다. 일실시예에 따르면, 연결 단자(178)는, 예를 들면, HDMI 커넥터, USB 커넥터, SD 카드 커넥터, 또는 오디오 커넥터(예: 헤드폰 커넥터)를 포함할 수 있다.
- [0030] 햅틱 모듈(179)은 전기적 신호를 사용자가 촉각 또는 운동 감각을 통해서 인지할 수 있는 기계적인 자극(예: 진동 또는 움직임) 또는 전기적인 자극으로 변환할 수 있다. 일실시예에 따르면, 햅틱 모듈(179)은, 예를 들면, 모터, 압전 소자, 또는 전기 자극 장치를 포함할 수 있다.
- [0031] 카메라 모듈(180)은 정지 영상 및 동영상을 촬영할 수 있다. 일실시예에 따르면, 카메라 모듈(180)은 하나 이상의 렌즈들, 이미지 센서들, 이미지 시그널 프로세서들, 또는 플래시들을 포함할 수 있다.
- [0032] 전력 관리 모듈(188)은 전자 장치(101)에 공급되는 전력을 관리할 수 있다. 일실시예에 따르면, 전력 관리 모듈(388)은, 예를 들면, PMIC(power management integrated circuit)의 적어도 일부로서 구현될 수 있다.
- [0033] 배터리(189)는 전자 장치(101)의 적어도 하나의 구성 요소에 전력을 공급할 수 있다. 일실시예에 따르면, 배터리(189)는, 예를 들면, 재충전 불가능한 1차 전지, 재충전 가능한 2차 전지 또는 연료 전지를 포함할 수 있다.
- [0034] 통신 모듈(190)은 전자 장치(101)와 외부 전자 장치(예: 전자 장치(102), 전자 장치(104), 또는 서버(108))간의 직접(예: 유선) 통신 채널 또는 무선 통신 채널의 수립, 및 수립된 통신 채널을 통한 통신 수행을 지원할 수 있다. 통신 모듈(190)은 프로세서(120)(예: 어플리케이션 프로세서)와 독립적으로 운영되고, 직접(예: 유선) 통신 또는 무선 통신을 지원하는 하나 이상의 커뮤니케이션 프로세서를 포함할 수 있다. 일실시예에 따르면, 통신 모듈(190)은 무선 통신 모듈(192)(예: 셀룰러 통신 모듈, 근거리 무선 통신 모듈, 또는 GNSS(global navigation satellite system) 통신 모듈) 또는 유선 통신 모듈(194)(예: LAN(local area network) 통신 모듈, 또는 전력선 통신 모듈)을 포함할 수 있다. 이들 통신 모듈 중 해당하는 통신 모듈은 제 1 네트워크(198)(예: 블루투스, WiFi direct 또는 IrDA(infrared data association) 같은 근거리 통신 네트워크) 또는 제 2 네트워크(199)(예: 셀룰러 네트워크, 인터넷, 또는 컴퓨터 네트워크(예: LAN 또는 WAN)와 같은 원거리 통신 네트워크)를 통하여 외부 전자 장치와 통신할 수 있다. 이런 여러 종류의 통신 모듈들은 하나의 구성 요소(예: 단일 칩)으로 통합되거나, 또는 서로 별도의 복수의 구성 요소들(예: 복수 칩들)로 구현될 수 있다. 무선 통신 모듈(192)은 가입자 식별 모듈(196)에 저장된 가입자 정보(예: 국제 모바일 가입자 식별자(IMS))를 이용하여 제 1 네트워크(198) 또는 제 2 네트워크(199)와 같은 통신 네트워크 내에서 전자 장치(101)를 확인 및 인증할 수 있다.
- [0035] 안테나 모듈(197)은 신호 또는 전력을 외부(예: 외부 전자 장치)로 송신하거나 외부로부터 수신할 수 있다. 일실시예에 따르면, 안테나 모듈(197)은 하나 이상의 안테나들을 포함할 수 있고, 이로부터, 제 1 네트워크 198 또는 제 2 네트워크 199와 같은 통신 네트워크에서 사용되는 통신 방식에 적합한 적어도 하나의 안테나가, 예를

들면, 통신 모듈(190)에 의하여 선택될 수 있다. 신호 또는 전력은 상기 선택된 적어도 하나의 안테나를 통하여 통신 모듈(190)과 외부 전자 장치 간에 송신되거나 수신될 수 있다.

[0036] 상기 구성요소들 중 적어도 일부는 주변 기기들간 통신 방식(예: 버스, GPIO(general purpose input and output), SPI(serial peripheral interface), 또는 MIPI(mobile industry processor interface))를 통해 서로 연결되고 신호(예: 명령 또는 데이터)를 상호간에 교환할 수 있다.

[0037] 일실시예에 따르면, 명령 또는 데이터는 제 2 네트워크(199)에 연결된 서버(108)를 통해서 전자 장치(101)와 외부의 전자 장치(104)간에 송신 또는 수신될 수 있다. 전자 장치(102, 104) 각각은 전자 장치(101)와 동일한 또는 다른 종류의 장치일 수 있다. 일실시예에 따르면, 전자 장치(101)에서 실행되는 동작들의 전부 또는 일부는 외부 전자 장치들(102, 104, or 108) 중 하나 이상의 외부 장치들에서 실행될 수 있다. 예를 들면, 전자 장치(101)가 어떤 기능이나 서비스를 자동으로, 또는 사용자 또는 다른 장치로부터의 요청에 반응하여 수행해야 할 경우에, 전자 장치(101)는 기능 또는 서비스를 자체적으로 실행시키는 대신에 또는 추가적으로, 하나 이상의 외부 전자 장치들에게 그 기능 또는 그 서비스의 적어도 일부를 수행하라고 요청할 수 있다. 상기 요청을 수신한 하나 이상의 외부 전자 장치들은 요청된 기능 또는 서비스의 적어도 일부, 또는 상기 요청과 관련된 추가 기능 또는 서비스를 실행하고, 그 실행의 결과를 전자 장치(101)로 전달할 수 있다. 전자 장치(101)는 상기 결과를, 그대로 또는 추가적으로 처리하여, 상기 요청에 대한 응답의 적어도 일부로서 제공할 수 있다. 이를 위하여, 예를 들면, 클라우드 컴퓨팅, 분산 컴퓨팅, 또는 클라이언트-서버 컴퓨팅 기술이 이용될 수 있다.

[0039] 도 2은 다양한 실시예에 따른 프로그램(140)을 예시하는 블록도(200)이다. 일실시예에 따르면, 프로그램(140)은 전자 장치(101)의 하나 이상의 리소스들을 제어하기 위한 운영 체제(142), 미들웨어(144), 또는 상기 운영 체제(142)에서 실행 가능한 어플리케이션(146)을 포함할 수 있다. 운영 체제(142)는, 예를 들면, Android™, iOS™, Windows™, Symbian™, Tizen™, 또는 Bada™를 포함할 수 있다. 프로그램(140) 중 적어도 일부 프로그램은, 예를 들면, 제조 시에 전자 장치(101)에 프리로드되거나, 또는 사용자에게 의해 사용 시 외부 전자 장치(예: 전자 장치(102 또는 104), 또는 서버(108))로부터 다운로드되거나 갱신 될 수 있다.

[0040] 운영 체제(142)는 전자 장치(101)의 하나 이상의 시스템 리소스들(예: 프로세스, 메모리, 또는 전원)의 관리(예: 할당 또는 회수)를 제어할 수 있다. 운영 체제(142)는, 추가적으로 또는 대체적으로, 전자 장치(101)의 다른 하드웨어 디바이스, 예를 들면, 입력 장치(150), 음향 출력 장치(155), 표시 장치(160), 오디오 모듈(170), 센서 모듈(176), 인터페이스(177), 햅틱 모듈(179), 카메라 모듈(180), 전력 관리 모듈(188), 배터리(189), 통신 모듈(190), 가입자 식별 모듈(196), 또는 안테나 모듈(197)을 구동하기 위한 하나 이상의 드라이버 프로그램들을 포함할 수 있다.

[0041] 미들웨어(144)는 전자 장치(101)의 하나 이상의 리소스들로부터 제공되는 기능 또는 정보가 어플리케이션(146)에 의해 사용될 수 있도록 다양한 기능들을 어플리케이션(146)으로 제공할 수 있다. 미들웨어(144)는, 예를 들면, 어플리케이션 매니저(201), 윈도우 매니저(203), 멀티미디어 매니저(205), 리소스 매니저(207), 파워 매니저(209), 데이터베이스 매니저(211), 패키지 매니저(213), 커넥티비티 매니저(215), 노티피케이션 매니저(217), 로케이션 매니저(219), 그래픽 매니저(221), 시큐리티 매니저(223), 통화 매니저(225), 또는 음성 인식 매니저(227)를 포함할 수 있다.

[0042] 어플리케이션 매니저(201)는, 예를 들면, 어플리케이션(146)의 생명 주기를 관리할 수 있다. 윈도우 매니저(203)는, 예를 들면, 화면에서 사용되는 하나 이상의 GUI 자원들을 관리할 수 있다. 멀티미디어 매니저(205)는, 예를 들면, 미디어 파일들의 재생에 필요한 하나 이상의 포맷들을 파악하고, 그 중 선택된 해당하는 포맷에 맞는 코덱을 이용하여 상기 미디어 파일들 중 해당하는 미디어 파일의 인코딩 또는 디코딩을 수행할 수 있다. 리소스 매니저(207)는, 예를 들면, 어플리케이션(146)의 소스 코드 또는 메모리(130)의 메모리의 공간을 관리할 수 있다. 파워 매니저(209)는, 예를 들면, 배터리(189)의 용량, 온도 또는 전원을 관리하고, 이 중 해당 정보를 이용하여 전자 장치(101)의 동작에 필요한 관련 정보를 결정 또는 제공할 수 있다. 일실시예에 따르면, 파워 매니저(209)는 전자 장치(101)의 바이오스(BIOS: basic input/output system)(미도시)와 연동할 수 있다.

[0043] 데이터베이스 매니저(211)는, 예를 들면, 어플리케이션(146)에 의해 사용될 데이터베이스를 생성, 검색, 또는 변경할 수 있다. 패키지 매니저(213)는, 예를 들면, 패키지 파일의 형태로 배포되는 어플리케이션의 설치 또는 갱신을 관리할 수 있다. 커넥티비티 매니저(215)는, 예를 들면, 전자 장치(101)와 외부 전자 장치 간의 무선 연결 또는 직접 연결을 관리할 수 있다. 노티피케이션 매니저(217)는, 예를 들면, 지정된 이벤트(예: 착신 통화,

메시지, 또는 알람)의 발생을 사용자에게 알리기 위한 기능을 제공할 수 있다. 로케이션 매니저(219)는, 예를 들면, 전자 장치(101)의 위치 정보를 관리할 수 있다. 그래픽 매니저(221)는, 예를 들면, 사용자에게 제공될 하나 이상의 그래픽 효과들 또는 이와 관련된 사용자 인터페이스를 관리할 수 있다.

[0044] 시큐리티 매니저(223)는, 예를 들면, 시스템 보안 또는 사용자 인증을 제공할 수 있다. 통화(telephony) 매니저(225)는, 예를 들면, 전자 장치(101)에 의해 제공되는 음성 통화 기능 또는 영상 통화 기능을 관리할 수 있다. 음성 인식 매니저(227)는, 예를 들면, 사용자의 음성 데이터를 서버(108)로 전송하고, 그 음성 데이터에 적어도 일부 기반하여 전자 장치(101)에서 수행될 기능에 대응하는 명령어(command), 또는 그 음성 데이터에 적어도 일부 기반하여 변환된 문자 데이터를 서버(108)로부터 수신할 수 있다. 일 실시예에 따르면, 미들웨어(244)는 동적으로 기존의 구성요소를 일부 삭제하거나 새로운 구성요소들을 추가할 수 있다. 일 실시예에 따르면, 미들웨어(144)의 적어도 일부는 운영 체제(142)의 일부로 포함되거나, 또는 운영 체제(142)와는 다른 별도의 소프트웨어로 구현될 수 있다.

[0045] 어플리케이션(146)은, 예를 들면, 홈(251), 다이얼러(253), SMS/MMS(255), IM(instant message)(257), 브라우저(259), 카메라(261), 알람(263), 연락처(265), 음성 인식(267), 이메일(269), 달력(271), 미디어 플레이어(273), 앨범(275), 워치(277), 헬스(279)(예: 운동량 또는 혈당과 같은 생체 정보를 측정), 또는 환경 정보(281)(예: 기압, 습도, 또는 온도 정보 측정) 어플리케이션을 포함할 수 있다. 일 실시예에 따르면, 어플리케이션(146)은 전자 장치(101)와 외부 전자 장치 사이의 정보 교환을 지원할 수 있는 정보 교환 어플리케이션(미도시)을 더 포함할 수 있다. 정보 교환 어플리케이션은, 예를 들면, 외부 전자 장치로 지정된 정보(예: 통화, 메시지, 또는 알람)를 전달하도록 설정된 noti피케이션 릴레이 어플리케이션, 또는 외부 전자 장치를 관리하도록 설정된 장치 관리 어플리케이션을 포함할 수 있다. noti피케이션 릴레이 어플리케이션은, 예를 들면, 전자 장치(101)의 다른 어플리케이션(예: 이메일 어플리케이션(269))에서 발생된 지정된 이벤트(예: 메일 수신)에 대응하는 알람 정보를 외부 전자 장치로 전달할 수 있다. 추가적으로 또는 대체적으로, noti피케이션 릴레이 어플리케이션은 외부 전자 장치로부터 알람 정보를 수신하여 전자 장치(101)의 사용자에게 제공할 수 있다.

[0046] 장치 관리 어플리케이션은, 예를 들면, 전자 장치(101)와 통신하는 외부 전자 장치 또는 그 일부 구성 요소(예: 표시 장치(160) 또는 카메라 모듈(180))의 전원(예: 턴-온 또는 턴-오프) 또는 기능(예: 표시 장치(160) 또는 카메라 모듈(180)의 밝기, 해상도, 또는 포커스)을 제어할 수 있다. 장치 관리 어플리케이션은, 추가적으로 또는 대체적으로, 외부 전자 장치에서 동작하는 어플리케이션의 설치, 삭제, 또는 갱신을 지원할 수 있다.

[0048] 도 3은 본 발명의 다양한 실시예에 따른 전자 장치의 블록도이다.

[0049] 도 3을 참조하면, 본 발명의 다양한 실시예에 따른 전자 장치(300)(예: 도 1의 전자 장치(101)는 프로세서(310)(예: 도 1의 프로세서(120)), 통신 모듈(320)(예: 도 1의 통신 모듈(190)), 보안 모듈(330), 메모리(340)(예: 도 1의 메모리(130)), 및 디스플레이(350)(예: 도 1의 표시 장치(160))를 포함할 수 있다.

[0050] 본 발명의 다양한 실시예에 따르면, 프로세서(310)는 보안 모듈(330) 상에 설치된 애플릿의 설정의 변경을 수행하도록 보안 모듈(330)을 제어할 수 있다. 예를 들면, 프로세서(310)는 전자 장치(300)의 사용자가 애플릿의 설정의 변경을 수행하기 위한 화면을 디스플레이(350)에 디스플레이하고, 사용자의 입력에 기반하여 애플릿의 설정의 변경을 요청하는 신호를 보안 모듈(330)에 전송할 수 있다.

[0051] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330) 상에 설치된 애플릿은 외부 전자 장치(예: 도 5의 전자 장치(500))가 제공 가능한 다양한 기능을 이용하기 위해서, 전자 장치(300)의 인증을 수행하기 위한 애플릿을 의미할 수 있다. 예를 들어, 애플릿은 외부 전자 장치(500)의 사용을 위한 키(key)를 의미할 수 있다. 외부 전자 장치(500)가 운송 수단인 경우, 보안 모듈(330) 상에 설치된 애플릿은 운송 수단의 인증에 이용되는 키를 관리하는 애플릿일 수 있다. 보안 모듈(330) 상에 설치된 애플릿은 외부 전자 장치(500)의 제조사에 의해 제공될 수 있다.

[0052] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)의 인증은 전자 장치(300)가 외부 전자 장치(500)가 제공 가능한 다양한 기능을 수행하기 위한 유효한 권한을 가지고 있는지 여부를 확인하는 절차를 의미할 수 있다. 본 발명의 다양한 실시예에 따르면, 외부 전자 장치(500)는 운송 수단(vehicle) 또는 운송 수단(vehicle)을 제어하기 위해서 전기적으로 연결된 다양한 전자 장치를 의미할 수 있다. 외부 전자 장치(500)에 대해서는 도 5에서 구체적으로 후술한다.

[0053] 본 발명의 다양한 실시예에 따르면, 통신 모듈(320)은 외부 전자 장치(500)와 통신 채널을 설립하고, 외부 전자

장치(500)와 다양한 데이터를 송수신할 수 있다. 통신 모듈(320)은 근거리 통신(예를 들면, Bluetooth, NFC, UWB 등)을 이용하여 외부 전자 장치(500)와 다양한 데이터를 송수신할 수 있으나, 이에 제한되지 않고, 셀룰러 네트워크(예를 들면, LTE, 5G 네트워크 등)를 이용하여 외부 전자 장치(500)와 다양한 데이터를 송수신할 수 있다.

- [0054] 본 발명의 다양한 실시예에 따르면, 메모리(340)는 외부 전자 장치(500)의 키를 설정하는 어플리케이션을 저장할 수 있다.
- [0055] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330)은 프로세서(310) 또는 메모리(예: 도 1의 메모리(130))와 물리적으로 분리된 모듈로써, 보안 모듈(330) 상에 저장된 데이터를 암호화하여 저장할 수 있다. 본 발명의 다른 실시예에 따르면, 보안 모듈(330)은 메모리(340)의 일 영역에 포함될 수 있으며, 보안 모듈(330)은 메모리(340) 상에 저장된 데이터를 암호화하여 저장된 부분을 의미할 수 있다.
- [0056] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330)은 보안 모듈(330) 상의 데이터의 접근 요청을 수신함에 대응하여, 데이터의 접근 요청의 주체(예를 들면, 메모리(130) 상에 설치된 다양한 어플리케이션 등)의 접근 권한, 또는 무결성 검증을 수행하고, 수행한 결과에 따라 보안 모듈(330) 상에 저장된 데이터의 접근/편집을 허가 또는 저장된 데이터를 전송할 수 있다.
- [0057] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330)은 외부 전자 장치(500)가 인증을 수행하는데 이용되는 애플릿을 관리하는 CRS(contactless register service)를 포함할 수 있다. CRS(미도시)는 사용자의 요청에 기반하여 애플릿에 할당된 데이터의 수정, 추가, 또는 삭제를 수행할 수 있다.
- [0058] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330)은 PVKSE(proximity vehicle key system environment)를 포함할 수 있다. PVKSE(미도시)는 애플릿에 할당된 데이터의 수정, 추가, 또는 삭제와 같은 동작의 모니터링을 수행하고, 애플릿과 관련된 데이터의 변경을 감지하면, 애플릿과 관련된 정보를 생성 또는 생성된 애플릿과 관련된 정보를 변경할 수 있다. PVKSE는 보안 모듈(330)에 저장된 데이터를 관리하는 CRS(contactless registry service)와는 소프트웨어적으로 별도로 구현된 구성 요소를 의미할 수 있다.
- [0059] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330)은 보안 모듈(330)상에 저장된 애플릿들 각각의 애플릿 식별자(application identification, AID)를 포함하는 AID 리스트를 생성할 수 있다. AID 리스트는 PVKSE에서 생성 및 관리할 수 있다. 보안 모듈(330)은 외부 전자 장치(500)의 요청에 대응해서, AID 리스트를 외부 전자 장치(500)로 전송할 수 있다.
- [0060] 본 발명의 다양한 실시예에 따르면, 외부 전자 장치(500)는 AID 리스트에 포함된 AID들 중, 인증을 수행할 적어도 하나의 AID를 선택하고, 선택된 AID를 지시하는 정보 및 선택된 AID에 대응하는 애플릿과 관련된 정보를 요청하는 신호를 전자 장치(300)로 전송할 수 있다.
- [0061] 본 발명의 다양한 실시예에 따르면, 외부 전자 장치(500)가 전송하는 신호는 ISO 7816-4의 Table 60에 정의된 Command header 및 Command body로 이루어진 메시지 구조(표 1 참조)를 이용할 수 있다.

표 1

[0062]	Code	Value
Command head	CLA (ISO 7816.4의 5.4.1에 정의)	00
	INS	A4
	P1(ISO 7816.4의 Table 62에 정의 됨)	04
	P2	00
Command body	Lc (Command data field의 길이)	0d
	Data (2VK.SYS.DDF01)	32564B2E5359532E4444463031
	Le	00

- [0064] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330)은 외부 전자 장치(500)가 전송한 선택된 AID를 지시하는 정

보 및 선택된 AID 에 대응하는 애플릿과 관련된 정보를 수신함에 대응하여, 선택된 AID에 대응하는 애플릿과 관련된 정보를 외부 전자 장치(500)로 전송할 수 있다.

[0065] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330)이 외부 전자 장치(500)로 전송하는 애플릿과 관련된 정보는 ISO 7816-4에 정의된 파일 제어 정보(file control information, FCI)에 대한 템플릿을 이용할 수 있다.

표 2

태그	값	필수 요소
'6F'	FCI Template (파일 제어 정보에 대한 템플릿을 지시하는 부분)	Y
'84'	'2VK.SYS.DDF01'	Y
'A5'	FCI Proprietary Template	Y
	"BFOC" FCI Issue Discretionary Data (보안 모듈(330)의 발행된 임의의 데이터를 지시하는 부분)	Y
	'61' Directory Entry (애플릿의 저장된 주소를 지시하는 부분)	Y
	'4F' DF Name (AID) (애플릿 식별자를 지시하는 부분)	Y
	'50' Application label(애플릿 라벨링)	N
	'87' Priority indicator(highest)(우선 순위를 지시하는 부분)	N
	'9F30' Application-specific data (구체적인 데이터)	N
	...	
	'61' Directory Entry	N
	'4F' DF Name (AID)	N
	'50' Application label	N
	'87' Priority indicator(lowest)	N
	'9F30' Application-specific data	N

[0068] 표 2를 참조하면, 애플릿과 관련된 정보는 데이터 및 데이터를 지시하는 태그(tag) 형태로 구현될 수 있다. 추가적으로, 데이터의 길이를 지시하는 항목이 태그와 데이터 사이에 추가될 수 있다. 애플릿과 관련된 정보는 외부 전자 장치(500)가 선택한 AID가 복수인 경우, AID들 각각에 대응하는 애플릿과 관련된 정보를 모두 포함할 수 있다. AID가 복수인 경우, AID들 각각에 대응하는 애플릿과 관련된 정보는 우선 순위가 높은 순서대로 전송될 수 있다. 우선 순위는 전자 장치(300)의 사용자에게 의해 설정될 수 있다. 또한, 우선 순위는 외부 전자 장치(500)의 이용 빈도에 따라서 변경될 수 있다. 예를 들면, 외부 전자 장치(500)의 이용 빈도가 높을수록 우선 순위는 높게 설정될 수 있다.

[0069] 본 발명의 다양한 실시예에 따르면, 애플릿과 관련된 정보는 외부 전자 장치의 제조사의 식별자를 의미하는 애플릿 식별자(4F), 외부 전자 장치의 모델을 지시하는 애플릿 라벨(50), 애플릿의 우선 순위를 지시하는 우선 순위 정보(87), 또는 애플릿의 구체적인 데이터(9F30)를 포함할 수 있다.

[0070] 본 발명의 다양한 실시예에 따르면, 애플릿과 관련된 정보 중 파일 제어 정보에 대한 템플릿을 지시하는 정보(6F), 데이터 필드(84), 파일 제어 정보의 특정 템플릿(FCI Proprietary template, A5), 보안 모듈(330)의 발행된 임의의 데이터를 지시하는 부분(BFOC), 애플릿의 저장된 주소를 지시하는 부분(61), 또는 애플리케이션 식별자(50)는 애플릿과 관련된 정보의 필수 요소에 해당될 수 있다. 외부 전자 장치의 모델을 지시하는 애플릿 라벨(50), 애플릿의 우선 순위를 지시하는 우선 순위 정보(87) 또는 애플릿의 구체적인 데이터(9F30)는 애플릿과 관련된 정보의 부가 요소에 해당될 수 있다.

[0071] 본 발명의 다양한 실시예에 따르면, 애플릿과 관련된 정보는 애플릿의 구체적인 데이터(9F30) 끝에 애플릿의 상태를 지시하는 데이터를 포함할 수 있다.

- [0072] 본 발명의 다양한 실시예에 따르면, 애플릿의 식별자(4F)는 애플릿을 구분할 수 있는 식별자를 의미할 수 있다. 예를 들면, 외부 전자 장치(500)의 제조사의 식별자를 의미할 수 있다. 외부 전자 장치의 제조사의 식별자는 제조사마다 모두 다를 수 있다. 외부 전자 장치(500)는 애플릿의 식별자(4F)를 확인하고, 외부 전자 장치(500)의 제조사와 동일한 제조사에 대응하는 AID를 선택할 수 있다.
- [0073] 본 발명의 다양한 실시예에 따르면, 애플릿 라벨(50)은 외부 전자 장치의 모델의 식별자 또는 외부 전자 장치의 제조사의 식별자를 의미할 수 있다. 외부 전자 장치가 동일한 제조사에 의해 제조된 것이라도, 모델(중형차, 대형차)에 따라서 애플릿 라벨(50)이 다를 수 있다.
- [0074] 본 발명의 다양한 실시예에 따르면, 우선 순위 정보(87)는 외부 전자 장치(500)가 인증을 수행하는 순서와 관련된 우선 순위에 대한 정보를 의미할 수 있다. 우선 순위 정보(87)는 숫자로 구현될 수 있으며, 숫자의 크기가 작을수록 우선 순위가 높을 수 있다.
- [0075] 본 발명의 다양한 실시예에 따르면, 애플릿의 구체적인 데이터(9F30)는 애플릿의 다양한 데이터가 포함될 수 있는 영역으로, 외부 전자 장치(500)와 전자 장치(300) 사이의 인증에 필요한 다양한 데이터가 포함될 수 있다. 애플릿의 구체적인 데이터(9F30)는 외부 전자 장치(500)의 이용 허용 시간(예를 들면, 외부 전자 장치(500)의 운행이 가능한 시간), 외부 전자 장치(500)의 이용 가능한 지역 범위 정보(geofencing limitation data, 예를 들면, 외부 전자 장치(500)의 운행이 허용되는 지역적인 범위), 외부 전자 장치(500)의 최대 허용 속도, 외부 전자 장치(500)에 포함된 다양한 장치(예를 들면, 트렁크, 또는 콘솔 박스 등) 또는 외부 전자 장치(500)가 수행 가능한 다양한 기능(예를 들면, 차신 유지 보조, 차신 이탈 알림, 크루즈 컨트롤, 어댑티브 크루즈 컨트롤, 또는 엔진 사용 가능 여부)의 허용 여부를 지시하는 데이터를 포함할 수 있다.
- [0076] 본 발명의 다양한 실시예에 따르면, 표 3을 참조하면, 애플릿의 상태를 지시하는 데이터는 크게 3 가지의 상태(애플릿과 관련된 정보를 요청하는 메시지의 오류 발생, 애플릿이 존재하지 않는 상태, 및 애플릿과 관련된 정보의 전송이 성공함을 나타내는 상태) 중 한가지 상태를 지시할 수 있다.

표 3

Field	Length	Value		
Status Word	2	Status Word		
		Value	Type	Meaning
		'6A86'	Error	Incorrect P1/P2
		'6A82'	Error	Application not found
		'9000'	Normal	Successful Processing

- [0079] 표 1을 참조하여 생성된 외부 전자 장치(500)가 전자 장치(300)로 AID 리스트를 요청하는 신호는 예를 들어, “00A404000D32564B2E5359532E444446303100” 로 구현될 수 있다. 전자 장치(300)가 외부 전자 장치(500)에 전송하는 애플릿과 관련된 데이터는 상기의 설명에 의해 구현될 수 있으며, 구체적인 예시는 도 10에 기재되어 있다.
- [0080] 도 10을 참조하면, 애플릿과 관련된 데이터는 표 2에 정의된 포맷을 이용하여 표 4와 같이 구현될 수 있다. 표 4는 표 2에 정의된 포맷을 이용하여 구현된 애플릿과 관련된 데이터의 구체적인 예시로, 도 10에 도시된 애플릿과 관련된 데이터의 상세한 설명을 기재하고 있다.

표 4

[0081]

태그	설명		예시
'6F'	FCI Template (파일 제어 정보에 대한 템플릿을 지시하는 부분)		6F
	'84'	'2VK.SYS.DDF01'	32564B2E53 59532E4444 463031
	'A5'	FCI Proprietary Template	A5

		'BFOC'	FCI Issue Discretionary Data (보안 모듈(330)의 발행된 임의의 데이터를 지시하는 부분)		BFOC
			'61'	Directory Entry (에플릿의 저장된 주소를 지시하는 부분)	61
				'4F'	DF Name (AID) (에플릿 식별자를 지시하는 부분)
				'50'	Application label(에플릿 라벨링)
				'87'	Priority indicator(highest)(우선 순위를 지시하는 부분)
				'9F30'	Application-specific data (구체적인 데이터)

- [0083] 본 발명의 다양한 실시예에 따르면, 외부 전자 장치(500)는 전자 장치(300)가 전송한 에플릿과 관련된 데이터를 이용하여 전자 장치(300)에 대한 인증을 수행할 수 있다. 외부 전자 장치(500)는 전자 장치(300)의 인증이 완료됨에 대응하여, 인증된 범위 내에서의 외부 전자 장치(500)가 수행 가능한 기능을 제공할 수 있다. 예를 들면, 외부 전자 장치(500)는 전자 장치(300)의 인증이 완료됨에 대응하여, 외부 전자 장치(500)의 문의 잠금을 해제할 수 있으며, 외부 전자 장치(500)의 시동의 ON/OFF 제어 잠금을 해제할 수도 있다.
- [0084] 본 발명의 다양한 실시예에 따르면, 외부 전자 장치(500)의 인증에 이용되는 에플릿과 관련된 정보는 전자 장치(300)의 보안 모듈(330)에 저장될 수 있다. 보안 모듈(300)은 별도의 보안 솔루션을 제공할 수 있어, 보안에 민감한 에플릿과 관련된 정보는 안전하게 저장될 수 있으며, 안전하게 이용될 수 있다. 에플릿과 관련된 정보가 보안 모듈(330)에 저장되는 구체적인 예시에 대해서는 도 4에서 후술한다.
- [0086] 도 4는 본 발명의 다양한 실시예에 따른 전자 장치에서, 보안 모듈을 도시한 블록도이다.
- [0087] 도 4를 참조하면, 본 발명의 다양한 실시예에 따른 전자 장치(300)의 보안 모듈(330)은 발급된 보안 도메인(issued security domain, ISD, 481)과 추가 보안 도메인(supplementary security domain, SSD, 482)로 구분될 수 있다.
- [0088] 본 발명의 다양한 실시예에 따르면, ISD(481)에는 PVKSE(410) 및 CRS(420)가 설치될 수 있다. PVKSE(410)는 SSD(482)에 설치된 적어도 하나 이상의 에플릿(430, 440, 450, 460, 또는 470)을 관리할 수 있는 소프트웨어적 요소를 의미할 수 있다. 본 발명의 다양한 실시예에 따른 보안 모듈(330)은 적어도 하나 이상의 에플릿(430, 440, 450, 460, 또는 470)을 관리하는 CRS(420)를 포함하고, CRS(420)의 제어에 기반하여 적어도 하나 이상의 에플릿(430, 440, 450, 460, 또는 470)의 관리를 수행할 수 있다.
- [0089] 본 발명의 다양한 실시예에 따르면, CRS(420)는 보안 모듈(330) 상에 설치되는 파일을 관리하는 소프트웨어적인 요소를 의미할 수 있다. CRS(420)는 프로세서(예: 도 3의 프로세서(310))의 요청에 기반하여 보안 모듈(330)에 저장된 다양한 데이터의 관리(예를 들면, 데이터의 암호화, 또는 암호화된 데이터의 복호화)를 수행할 수 있으며, 보안 모듈(330)에 저장된 데이터를 메모리(예: 도 1의 메모리(130))에 이동시킬 수 있다.
- [0090] 외부 전자 장치(500)는 전자 장치(300)의 인증을 수행하기 위해서, 보안 모듈(330)에 저장된 AID 리스트의 전송을 전자 장치(300)에 요청할 수 있다. 예를 들어, 보안 모듈(330)에 저장된 AID 리스트의 전송은 SELECT PVKSE로 정의된 명령어를 이용할 수 있다. PVKSE(410)는 SELECT PVKSE로 정의된 명령어를 수신함에 대응하여 AID 리스트의 생성 및 전송을 수행할 수 있다.
- [0091] 본 발명의 다양한 실시예에 따르면, PVKSE(410)는 에플릿의 다양한 데이터의 변경을 모니터링하고, 데이터의 변경을 감지한 경우, 데이터 변경을 반영한 에플릿과 관련된 정보를 생성 또는 변경할 수 있다. PVKSE(410)는 외부 전자 장치(500)의 요청에 대응하여 외부 전자 장치(500)가 선택한 적어도 하나 이상의 AID에 대응하는 에플릿과 관련된 정보를 전송할 수 있다.
- [0092] 본 발명의 다양한 실시예에 따르면, 외부 전자 장치(500)는 선택된 AID를 지시하는 정보를 SELECT AID로 정의된 명령어를 이용하여 보안 모듈(330)에 전송할 수 있다. 예를 들어, 보안 모듈(330)의 PVKSE(410)는 SELECT

AID로 정의된 명령어를 수신함에 대응하여, 외부 전자 장치(500)가 선택한 적어도 하나 이상의 AID에 대응하는 애플릿과 관련된 정보를 전송할 수 있다.

[0093] 본 발명의 다양한 실시예에 따르면, 적어도 하나 이상의 애플릿(430, 440, 450, 460, 또는 470)들 각각은 SSD(482)에 저장될 수 있다. SSD(482)는 외부 전자 장치(500)의 제조사별로 구별된 상태로, 제조사 각각에 대응하는 애플릿을 대응하는 제조사별로 구별된 SSD(482)에 저장할 수 있다. 예를 들면, 제조사 1에 대응하는 애플릿들(450, 460)은 제조사 1에 대응하는 SSD 공간(484)에 저장될 수 있고, 제조사 2에 대응하는 애플릿(470)은 제조사 2에 대응하는 SSD 공간(485)에 저장될 수 있다. SSD(482)는 다양한 사용자가 이용 가능한 외부 전자 장치(예를 들면, 카 셰어링의 공유 대상이 되는 운송 수단)를 이용 가능한 공유 키를 위한 애플릿들(430, 440)을 별도로 저장할 수 있는 SSD 공간(483)을 더 포함할 수 있다.

[0094] 본 발명의 다양한 실시예에 따르면, 적어도 하나 이상의 애플릿(430, 440, 450, 460, 470)들 각각은 애플릿의 활성화 여부를 지시하는 데이터(430-a, 440-a, 450-a, 460-a, 470-a)를 포함할 수 있다. 활성화된 애플릿(예: 430, 440, 460, 470)은 외부 전자 장치(500)와 전자 장치(300)의 인증을 수행 가능한 애플릿을 의미하며, 비활성화된 애플릿(예: 450)은 외부 전자 장치(500)와 전자 장치(300)의 인증이 수행될 수 없는 애플릿을 의미할 수 있다. 애플릿의 활성화 여부는 전자 장치(300)의 사용자의 입력에 따라 정해질 수 있으며, 애플릿의 활성화를 수행하는 구체적인 내용은 도 8a에서 후술한다.

[0095] 본 발명의 다양한 실시예에 따르면, 적어도 하나 이상의 애플릿(430, 440, 450, 460, 470)들 각각은 애플릿의 우선 순위를 지시하는 데이터(430-b, 440-b, 450-b, 460-b, 470-b)를 포함할 수 있다. 우선 순위는 전자 장치(300)의 사용자에게 의해 설정될 수 있다. 또한, 우선 순위는 외부 전자 장치(500)의 이용 빈도에 따라서 변경될 수 있다. 예를 들면, 외부 전자 장치(500)의 이용 빈도가 높을수록 우선 순위는 높게 설정될 수 있다. 애플릿의 우선 순위를 설정하는 구체적인 내용은 도 8b에서 후술한다.

[0096] 본 발명의 다양한 실시예에 따르면, 적어도 하나 이상의 애플릿(430, 440, 450, 460, 또는 470)들 각각은 애플릿과 관련된 정보를 포함할 수 있으며, 애플릿과 관련된 정보는 외부 전자 장치의 제조사의 식별자를 의미하는 애플릿 식별자(4F), 외부 전자 장치의 모델을 지시하는 애플릿 라벨(50), 애플릿의 우선 순위를 지시하는 우선 순위 정보(87), 애플릿의 구체적인 데이터(9F30)를 포함할 수 있다. 애플릿과 관련된 정보는 애플릿의 구체적인 데이터(9F30) 끝에 애플릿의 상태를 지시하는 데이터를 포함할 수 있다.

[0098] 도 5는 본 발명의 다양한 실시예에 따른 전자 장치의 블록도이다.

[0099] 도 5를 참조하면, 본 발명의 다양한 실시예에 따른 전자 장치(500)(예: 도 1의 전자 장치(102) 또는 전자 장치(104))는 프로세서(510), 통신 모듈(520) 및 보안 모듈(530)을 포함할 수 있다. 도 5에 도시된 전자 장치(500)는 도 3에서 서술된 외부 전자 장치를 의미할 수 있다. 전자 장치(500)는 운송 수단(vehicle) 또는 운송 수단(vehicle)을 제어하기 위해서 전기적으로 연결된 다양한 전자 장치를 의미할 수 있다. 외부 전자 장치(예: 도 3에 도시된 전자 장치(300))와 도 5에 도시된 전자 장치(500)의 인증을 통해, 전자 장치(500)가 수행 가능한 다양한 기능들 중 적어도 일부의 기능(예를 들면, 전자 장치(500)의 문 잠금 해제, 전자 장치(500)의 엔진의 시동을 키는 기능)을 수행할 수 있다.

[0100] 본 발명의 다양한 실시예에 따르면, 통신 모듈(520)은 외부 전자 장치(300)와 통신 채널을 설립하고, 외부 전자 장치(300)와 다양한 데이터를 송수신할 수 있다. 통신 모듈(520)은 근거리 통신(예를 들면, Bluetooth, NFC, UWB 등)을 이용하여 외부 전자 장치(300)와 다양한 데이터를 송수신할 수 있으나, 이에 제한되지 않고, 셀룰러 네트워크(예를 들면, LTE, 5G 네트워크 등)를 이용하여 외부 전자 장치(300)와 다양한 데이터를 송수신할 수 있다.

[0101] 본 발명의 다양한 실시예에 따르면, 보안 모듈(530)은 프로세서(510) 또는 메모리(예: 도 1의 메모리(130))와 물리적으로 분리된 모듈로써, 보안 모듈(530) 상에 저장된 데이터를 암호화하여 저장할 수 있다. 본 발명의 다른 실시예에 따르면, 보안 모듈(530)은 메모리(130)의 일 영역에 포함될 수 있으며, 보안 모듈(530)은 메모리(130) 상에 저장된 데이터를 암호화하여 저장된 부분을 의미할 수 있다.

[0102] 본 발명의 다양한 실시예에 따르면, 보안 모듈(530)은 보안 모듈(530) 상의 데이터의 접근 요청을 수신함에 대응하여, 데이터의 접근 요청의 주체(예를 들면, 메모리(130) 상에 설치된 다양한 애플릿)의 접근 권한, 무결성 검증을 수행하고, 수행한 결과에 따라 보안 모듈(330) 상에 저장된 데이터의 접근/편집을 허가 또는 저장된 데이터를 전송할 수 있다. 보안 모듈(530) 상에는 외부 전자 장치(300)가 전송한 다양한 데이터(예를 들면, 애플

릿과 관련된 정보, 애플릿 리스트, 외부 전자 장치(300)가 전송한 인증에 필요한 데이터(공개 키) 또는 외부 전자 장치(300)와의 인증에 요구되는 데이터(비밀 키)가 저장될 수 있다.

- [0103] 본 발명의 다양한 실시예에 따르면, 프로세서(510)는 외부 전자 장치(300)와의 연결을 위한 연결 요청 신호를 방송(broadcast)하도록 통신 모듈(520)을 제어할 수 있다. 프로세서(510)는 방송된 연결 요청 신호에 응답한 외부 전자 장치(300)와 통신 채널을 설립할 수 있다.
- [0104] 본 발명의 다양한 실시예에 따르면, 프로세서(510)는 전자 장치(500)가 수행할 수 있는 다양한 기능들 중 적어도 일부의 기능을 활성화하는 요청 신호를 외부 전자 장치(300)로부터 수신할 수 있다. 예를 들면, 외부 전자 장치(300)는 외부 전자 장치(300)의 사용자 입력에 기반하여 전자 장치(500)의 일부 기능을 수행할 것(예를 들면, 전자 장치(500)의 문의 잠금을 해제, 전자 장치(500)의 라이트를 켜는 기능, 또는 전자 장치(500)의 자동 출차 기능)을 요청하는 신호를 생성하고, 생성된 신호를 전자 장치(500)로 전송할 수 있다. 프로세서(510)는 전자 장치(500)의 일부 기능을 수행할 것을 요청하는 신호의 수신에 대응하여 외부 전자 장치(300)와의 인증을 시작할 수 있다. 외부 전자 장치(300) 상에 설치된 애플릿(전자 장치(500)와의 인증을 위한 애플릿을 의미할 수 있다)이 복수인 경우, 복수의 애플릿들 각각에 대한 인증을 수행하는 경우, 인증에 걸리는 시간이 길어질 수 있다. 본 발명의 다양한 실시예에 따르면, 프로세서(510)는 복수의 애플릿들 모두에 대한 인증을 수행하지 않고, 인증을 수행하기 이전, AID 리스트를 보낼 것을 요청하는 신호를 외부 전자 장치(300)에 전송할 수 있다.
- [0105] 본 발명의 다양한 실시예에 따르면, AID 리스트의 요청 신호는 표 1에 기재된 메시지 구조를 이용하여 구현될 수 있다.
- [0106] 본 발명의 다양한 실시예에 따르면, 프로세서(510)는 외부 전자 장치(300)가 전송한 AID 리스트에 포함된 AID들 중, 적어도 하나 이상의 AID를 선택할 수 있다.
- [0107] 본 발명의 다양한 실시예에 따르면, 프로세서(510)는 AID 리스트에 포함된 AID들 중, 전자 장치(500)가 지원하지 않는 AID를 갖는 애플릿을 필터링(filter-out)하는 방식을 통해, 남겨진 적어도 하나 이상의 AID를 선택하는 방식으로, AID를 선택할 수 있다.
- [0108] 본 발명의 다른 실시예에 따르면, 프로세서(510)는 AID 리스트에 포함된 AID들 중, 전자 장치(500)의 제조사와 동일한 AID를 갖는 애플릿을 선택하는 방식으로, AID를 선택할 수 있다.
- [0109] 본 발명의 또 다른 실시예에 따르면, 프로세서(510)는 AID 리스트에 포함된 AID들 중, 전자 장치(500)의 제조사와 동일한 AID를 갖는 애플릿과, 공유 키(sharing key)에 대응하는 AID들 중, 전자 장치(500)가 지원하지 않는 AID를 갖는 애플릿을 필터링(filter-out)하는 방식을 통해, 남겨진 적어도 하나 이상의 AID를 선택하는 방식으로, AID를 선택할 수 있다.
- [0110] 본 발명의 다양한 실시예에 따르면, 프로세서(510)는 선택된 AID들을 지시하는 정보를 외부 전자 장치(300)로 전송할 수 있다. 예를 들면, 프로세서(510)는 선택된 AID 들의 리스트를 생성하고, 생성된 AID 리스트를 외부 전자 장치(300)로 전송할 수 있다.
- [0111] 본 발명의 다양한 실시예에 따르면, 프로세서(510)는 적어도 하나 이상의 선택된 AID에 대응하는 애플릿과 관련된 정보를 요청하는 신호를 외부 전자 장치(300)에 전송할 수 있다. 애플릿과 관련된 정보는 ISO 7816-4에 정의된 파일 제어 정보(file control information)에 대한 템플릿을 이용하여 구현될 수 있으며, 표 2에 기재되어 있다. 애플릿과 관련된 정보는 외부 전자 장치의 제조사의 식별자를 의미하는 애플릿 식별자(4F), 외부 전자 장치의 모델을 지시하는 애플릿 라벨(50), 애플릿의 우선 순위를 지시하는 우선 순위 정보(87), 애플릿의 구체적인 데이터(9F30)를 포함할 수 있다. 애플릿과 관련된 정보는 애플릿의 구체적인 데이터(9F30) 끝에 애플릿의 상태를 지시하는 데이터를 포함할 수 있다. 애플릿과 관련된 정보의 구체적인 내용은 도 3에서 서술한 바 있다.
- [0112] 본 발명의 다양한 실시예에 따르면, 프로세서(510)는 애플릿과 관련된 정보를 외부 전자 장치(300)로부터 수신할 수 있다. 프로세서(510)는 애플릿과 관련된 정보를 이용하여 외부 전자 장치(300)와의 인증을 수행할 수 있다.
- [0113] 본 발명의 다양한 실시예에 따르면, 프로세서(510)는 애플릿과 관련된 정보에 포함된 우선 순위 정보에 기반하여 먼저 인증을 수행한 애플릿을 결정할 수 있다. 예를 들면, 프로세서(510)가 복수의 AID를 선택한 경우, 복수의 AID 각각에 대응하는 우선 순위 정보를 확인할 수 있다. 프로세서(510)는 우선 순위가 가장 높은 애플릿을 이용하여 외부 전자 장치(300)와 인증을 수행할 수 있다. 프로세서(510)가 우선 순위가 가장 높은 애플릿을 이용하여 외부 전자 장치(300)와 인증을 수행하다가, 인증이 실패한 경우, 그 다음으로 우선 순위가 높은 애플릿

을 이용하여 외부 전자 장치(300)와 인증을 수행할 수 있다.

- [0114] 본 발명의 다양한 실시예에 따른 전자 장치(500)는 외부 전자 장치(300)에 저장된 모든 애플릿에 대한 인증을 수행하는 것이 아니라, 먼저 AID 리스트를 수신하고, AID 리스트에서 인증을 수행할 애플릿을 먼저 선택하고, 선택된 애플릿을 이용하여 인증을 수행할 수 있다. 상기의 기재된 방법을 이용하여 복수의 애플릿을 구비하는 외부 전자 장치(300)와의 인증을 수행하는 경우, 인증에 요구되는 시간이 줄어들 수 있다.
- [0115] 본 발명의 다양한 실시예에 따르면, 프로세서(510)가 수행하는 기능들의 적어도 일부는 보안 모듈(530)에 의해서도 수행될 수도 있다.
- [0116] 본 발명의 다양한 실시예에 따르면, 전자 장치(500)는 외부 전자 장치(300)의 인증이 완료됨에 대응하여, 인증된 범위 내에서의 전자 장치(500)가 수행 가능한 기능을 제공할 수 있다. 예를 들면, 전자 장치(500)는 외부 전자 장치(300)의 인증이 완료됨에 대응하여, 전자 장치(500)의 문의 잠금을 해제할 수 있으며, 전자 장치(500)의 시동의 ON/OFF 제어 잠금을 해제할 수도 있다.
- [0118] 본 발명의 다양한 실시예에 따른 전자 장치는 외부 전자 장치와 통신을 수행하는 통신 모듈(예: 도 3의 통신 모듈(320)); 및 외부 전자 장치의 인증에 이용되는 키를 관리하는 애플릿과 관련된 데이터의 변경을 모니터링하고, 애플릿과 관련된 정보를 관리하고, 적어도 하나 이상의 애플릿 식별자(applet identification, AID)를 포함하는 AID 리스트 및 상기 애플릿을 저장하는 보안 모듈(예: 도 3의 보안 모듈(330))을 포함하고, 상기 보안 모듈은 상기 외부 전자 장치(예: 도 4의 전자 장치(400))로부터 상기 AID(Application identifier) 리스트를 전송할 것을 요청하는 신호를 수신하고, 상기 요청 신호의 수신에 대응하여, 상기 통신 모듈(320)을 통하여 상기 AID 리스트를 상기 외부 전자 장치(400)로 전송하고, 상기 외부 전자 장치(400)로부터 상기 AID 리스트에 포함된 상기 AID들 중 상기 외부 전자 장치(400)에 의해 선택된 적어도 하나 이상의 AID와 연관된 애플릿과 관련된 정보를 요청하는 신호를 수신하고, 상기 선택된 AID에 대응하는 애플릿과 관련된 정보를 상기 외부 전자 장치(400)로 전송하도록 설정될 수 있다.
- [0119] 본 발명의 다양한 실시예에 따르면, 상기 애플릿과 관련된 정보는 상기 애플릿이 저장된 주소, 상기 AID, 상기 외부 전자 장치의 모델 식별자, 상기 애플릿의 활성화 여부를 지시하는 데이터, 상기 애플릿 각각에 지정된 우선 순위, 또는 상기 애플릿의 구체적인 데이터(application-specific data) 중 적어도 하나 이상을 포함할 수 있다.
- [0120] 본 발명의 다양한 실시예에 따르면, 상기 애플릿의 구체적인 데이터는 상기 외부 전자 장치의 이용 허용 시간, 상기 외부 전자 장치의 이용 가능한 지역 범위 정보(geofencing limitation data), 또는 상기 외부 전자 장치가 수행 가능한 적어도 하나 이상의 기능에 대한 이용 여부를 지시하는 정보를 포함할 수 있다.
- [0121] 본 발명의 다양한 실시예에 따르면, 상기 AID 리스트는 상기 애플릿 각각에 지정된 우선 순위에 기반하여 배열될 수 있다.
- [0122] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(330)은 상기 보안 모듈에 저장된 데이터를 관리하는 CRS(예: 도 4의 CRS(420)); 및 상기 애플릿과 관련된 데이터의 변경을 모니터링하고, 상기 애플릿과 관련된 정보를 관리하는 PVKSE(proximity vehicle key system environment)(예: 도 4의 PVKSE(410))를 더 포함하고, 상기 CRS(420)는 상기 애플릿의 설정을 변경할 것을 요청하는 신호에 대응하여, 적어도 하나의 애플릿의 설정을 변경하고, 상기 데이터의 변경을 알리는 신호를 상기 PVKSE(410)로 전송하고, 상기 PVKSE(410)는 상기 데이터의 변경을 알리는 신호를 수신함에 대응하여, 상기 애플릿과 관련된 데이터를 변경하도록 설정될 수 있다.
- [0123] 본 발명의 다양한 실시예에 따르면, 상기 PVKSE(410) 및 상기 CRS(420)는 상기 보안 모듈의 발급된 보안 도메인(issued security domain)(예: 도 4의 ISD(481))에 저장되며, 상기 애플릿은 추가 보안 도메인(supplementary security domain)(예: 도 4의 SSD(482))에 저장되도록 설정될 수 있다.
- [0124] 본 발명의 다양한 실시예에 따르면, 상기 애플릿과 관련된 정보는 상기 애플릿마다 구분된 추가 보안 도메인에 저장되도록 설정될 수 있다.
- [0125] 본 발명의 다양한 실시예에 따르면, 상기 PVKSE(410)는 상기 애플릿의 변경을 감지한 경우, 상기 애플릿과 관련된 정보를 변경하도록 설정될 수 있다.

- [0127] 본 발명의 다양한 실시예에 따른 전자 장치는 메모리; 외부 전자 장치와의 인증에 이용되는 데이터를 저장하는 보안 모듈(예: 도 5의 보안 모듈(530)); 통신 모듈(예: 도 5의 통신 모듈(520)); 및 프로세서(예: 도 5의 프로세서(510))를 포함하고, 상기 보안 모듈(530)은 외부 전자 장치(예: 도 3의 전자 장치(300))와의 연결을 위한 연결 요청 신호를 방송(broadcasting)하고, 상기 방송된 신호에 응답한 외부 전자 장치(300)와 통신 채널을 수립하고, 상기 외부 전자 장치(300)에 저장된 적어도 하나 이상의 AID(Application identifier)를 포함하는 AID 리스트를 전송할 것을 요청하는 신호를 전송하고, 상기 외부 전자 장치(300)가 전송한 상기 AID 리스트에 포함된 AID 중 적어도 하나 이상의 AID를 선택하고, 상기 선택된 AID에 대응하는 애플릿을 지시하는 정보 및 상기 애플릿과 관련된 정보를 요청하는 신호를 상기 외부 전자 장치(300)에 전송하고, 상기 외부 전자 장치(300)로부터 수신한 상기 애플릿과 관련된 정보를 이용하여 상기 외부 전자 장치와 인증을 수행하도록 설정될 수 있다.
- [0128] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(530)은 상기 애플릿에 지정된 우선 순위에 기반하여 인증을 수행하도록 설정될 수 있다.
- [0129] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(530)은 상기 애플릿과 관련된 정보를 이용하여 상기 외부 전자 장치(300)에 대한 인증을 수행하고, 상기 인증이 실패함을 확인함에 대응하여, 상기 인증이 수행된 AID보다 우선 순위가 낮은 AID를 선택하고, 상기 선택된 AID에 대응하는 애플릿과 관련된 관련 정보를 요청하도록 설정될 수 있다.
- [0130] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(530)은 상기 AID 리스트에 포함된 AID들 중 상기 전자 장치(400)의 제조사에 대응하는 AID를 선택하도록 설정될 수 있다.
- [0131] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(530)은 상기 AID 리스트에 포함된 AID들 중 상기 전자 장치(400)의 제조사에 대응하는 AID 중, 우선 순위가 가장 높은 AID를 선택하도록 설정될 수 있다.
- [0132] 본 발명의 다양한 실시예에 따르면, 상기 AID 리스트는 상기 외부 전자 장치(300)에 대응하는 적어도 하나 이상의 AID 및 다른 사용자가 이용 가능한 공유된 외부 전자 장치(300)에 대응하는 적어도 하나 이상의 AID를 포함할 수 있다.
- [0133] 본 발명의 다양한 실시예에 따르면, 상기 애플릿과 관련된 정보는 상기 애플릿이 저장된 주소, 상기 AID, 상기 전자 장치(400)의 모델 식별자, 상기 애플릿의 활성화 여부를 지시하는 데이터, 상기 애플릿 각각에 지정된 우선 순위, 또는 상기 애플릿의 구체적인 데이터(application-specific data) 중 적어도 하나 이상을 포함할 수 있다.
- [0134] 본 발명의 다양한 실시예에 따르면, 상기 애플릿의 구체적인 데이터는 상기 전자 장치(400)의 이용 허용 시간, 상기 전자 장치(400)의 이용 가능한 지역 범위 정보(geofencing limitation data), 또는 상기 전자 장치(400)가 수행 가능한 적어도 하나 이상의 기능에 대한 허용 여부를 지시하는 정보를 포함할 수 있다.
- [0135] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(530)은 상기 애플릿의 구체적인 데이터에 기반하여 상기 전자 장치(400)가 제공 가능한 기능들 중 활성화될 기능을 결정하도록 설정될 수 있다.
- [0136] 본 발명의 다양한 실시예에 따르면, 상기 전자 장치(400)는 운송 수단(vehicle)이거나, 운송 수단(vehicle)과 전기적으로 연결될 수 있다.
- [0138] 도 6은 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법의 동작 흐름도이다.
- [0139] 도 6을 참조하면, 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법은 제 1 전자 장치(예: 도 3의 전자 장치(300)) 및 제 2 전자 장치(예: 도 5의 전자 장치(500)) 사이에서 구현될 수 있다.
- [0140] 동작 601에서, 제 2 전자 장치(500)는 탐색 신호(discovery signal)를 방송(broadcasting)할 수 있다. 동작 603에서, 제 1 전자 장치(300)는 탐색 신호를 수신하고, 통신 채널 생성을 위한 정보를 제 2 전자 장치(500)에 전송할 수 있다. 동작 605에서, 제 2 전자 장치(500)는 탐색 신호에 응답한 제 1 전자 장치(300)와 통신 채널을 설립할 수 있다. 본 발명의 다양한 실시예에 따르면, 통신 채널은 제 1 전자 장치(300)와 제 2 전자 장치(500)의 근거리 통신 방식에 의해 구현된 채널을 의미할 수 있으나, 셀룰러 네트워크 통신 방식에 의해 통신 채널이 구현될 수도 있다.
- [0141] 동작 607에서, 제 2 전자 장치(500)는 제 1 전자 장치(300)와의 인증을 위해서, AID 리스트를 전송할 것을 요청

하는 신호를 제 1 전자 장치(300)로 전송할 수 있다.

- [0142] 본 발명의 다양한 실시예에 따르면, 제 2 전자 장치(500)는 제 2 전자 장치(500)가 수행할 수 있는 다양한 기능들 중 적어도 일부의 기능을 활성화하는 요청 신호를 제 1 전자 장치(300)로부터 수신할 수 있다. 제 2 전자 장치(500)는 적어도 일부의 기능을 활성화하는 요청 신호를 수신함에 대응하여, 제 1 전자 장치(300)에 AID 리스트를 전송할 것을 요청하는 신호를 전송할 수 있다.
- [0143] 동작 609에서, 제 1 전자 장치(300)는 AID 리스트 전송 요청에 대응하여 AID 리스트를 제 2 전자 장치(500)로 전송할 수 있다. AID 리스트는 제 1 전자 장치(300)의 보안 모듈(예: 도 3의 보안 모듈(330))에 저장된 애플릿들 각각의 식별자의 리스트를 포함할 수 있다. 애플릿은 제 1 전자 장치(300)와 제 2 전자 장치(500) 사이의 인증을 수행하기 위한 다양한 정보를 포함할 수 있다.
- [0144] 동작 611에서, 제 2 전자 장치(500)는 AID 리스트에 포함된 AID들 중 적어도 하나 이상의 AID를 선택할 수 있다.
- [0145] 본 발명의 다양한 실시예에 따르면, 제 2 전자 장치(500)는 AID 리스트에 포함된 AID들 중, 제 2 전자 장치(500)가 지원하지 않는 AID를 갖는 애플릿을 필터링(filter-out)하는 방식을 통해, 남겨진 적어도 하나 이상의 AID를 선택하는 방식으로, AID를 선택할 수 있다.
- [0146] 본 발명의 일 실시예에 따르면, 제 2 전자 장치(500)는 AID 리스트에 포함된 AID들 중, 제 2 전자 장치(500)의 제조사와 동일한 AID를 갖는 애플릿을 선택하는 방식으로, AID를 선택할 수 있다.
- [0147] 본 발명의 일 실시예에 따르면, 제 2 전자 장치(500)는 AID 리스트에 포함된 AID들 중, 제 2 전자 장치(500)의 제조사와 동일한 AID를 갖는 애플릿과, 공유 키(sharing key)에 대응하는 AID들 중, 제 2 전자 장치(500)가 지원하지 않는 AID를 갖는 애플릿을 필터링(filter-out)하는 방식을 통해, 남겨진 적어도 하나 이상의 AID를 선택하는 방식으로, AID를 선택할 수 있다.
- [0148] 동작 613에서, 제 2 전자 장치(500)는 선택된 AID 목록 및 선택된 AID들 각각에 대응하는 애플릿과 관련된 데이터를 전송할 것을 요청하는 신호를 제 1 전자 장치(300)에 전송할 수 있다. 동작 615에서, 제 1 전자 장치(300)는 애플릿과 관련된 데이터를 제 2 전자 장치(500)에 전송할 수 있다.
- [0149] 본 발명의 다양한 실시예에 따르면, 애플릿과 관련된 정보는 ISO 7816-4에 정의된 파일 제어 정보(file control information)에 대한 템플릿을 이용하여 구현될 수 있으며, 표 2에 기재되어 있다. 애플릿과 관련된 정보는 외부 전자 장치의 제조사의 식별자를 의미하는 애플릿 식별자(4F), 외부 전자 장치의 모델을 지시하는 애플릿 라벨(50), 애플릿의 우선 순위를 지시하는 우선 순위 정보(87), 애플릿의 구체적인 데이터(9F30)를 포함할 수 있다. 애플릿과 관련된 정보는 애플릿의 구체적인 데이터(9F30) 끝에 애플릿의 상태를 지시하는 데이터를 포함할 수 있다. 애플릿과 관련된 정보의 구체적인 내용은 도 3에서 서술한 바 있다.
- [0150] 동작 617에서, 제 2 전자 장치(500)는 애플릿과 관련된 정보를 이용하여 제 1 전자 장치(300)와의 인증 절차를 수행할 수 있다.
- [0151] 본 발명의 다양한 실시예에 따른 제 2 전자 장치(500)는 제 1 전자 장치(300)에 저장된 모든 애플릿에 대한 인증을 수행하는 것이 아니라, 먼저 AID 리스트를 수신하고, AID 리스트에서 인증을 수행할 애플릿을 먼저 선택하고, 선택된 애플릿을 이용하여 인증을 수행할 수 있다. 상기의 기재된 방법을 이용하여 복수의 애플릿을 구비하는 제 1 전자 장치(300)와의 인증을 수행하는 경우, 인증에 요구되는 시간이 줄어들 수 있다.
- [0152] 본 발명의 다양한 실시예에 따르면, 제 2 전자 장치(500)는 제 1 전자 장치(300)의 인증이 완료됨에 대응하여, 인증된 범위 내에서의 제 2 전자 장치(500)가 수행 가능한 기능을 제공할 수 있다. 예를 들면, 제 2 전자 장치(500)는 제 1 전자 장치(300)의 인증이 완료됨에 대응하여, 제 2 전자 장치(500)의 문의 잠금을 해제할 수 있으며, 제 2 전자 장치(500)의 시동의 ON/OFF 제어 잠금을 해제할 수도 있다.
- [0154] 도 7은 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법에서, 전자 장치의 인증에 이용되는 애플릿을 보안 모듈에 설치하는 동작을 도시한 동작 흐름도이다.
- [0155] 도 7에 도시된 동작은 전자 장치(예: 도 3의 전자 장치(300))의 보안 모듈(예: 도 3의 보안 모듈(330)) 상에 외부 전자 장치(예: 도 5의 전자 장치(500))와의 인증을 수행하기 위한 애플릿 및 애플릿을 관리하기 위한 PVKSE(예: 도 4의 PVKSE(410))를 설치하는 동작을 도시하고 있다.

- [0156] 동작 710에서, 프로세서(예: 도 3의 프로세서(310))는 보안 모듈(330)에 PVKSE(410)를 설치할 수 있다. 본 발명의 다양한 실시예에 따르면, PVKSE(410)는 보안 모듈(330)의 ISD(481)에 설치될 수 있다. 외부 전자 장치(500)의 키를 설정하기 위한 애플릿이 메모리(예: 도 1의 메모리(130)) 상에 설치되면서, 외부 전자 장치(500)의 키가 보안 모듈(330)의 SSD(482) 상에 설치될 때, PVKSE(410)가 ISD(481) 상에 설치될 수 있다.
- [0157] 본 발명의 다양한 실시예에 따르면, PVKSE(410)는 전자 장치(300)의 제조시 미리 설치될 수 있으며, 이 경우, 동작 710은 생략될 수 있다.
- [0158] 동작 720에서, CRS(420)는 보안 모듈(330) 상에 외부 전자 장치(500)의 인증에 이용되는 키와 관련된 애플릿을 설치할 수 있다.
- [0159] 본 발명의 다양한 실시예에 따르면, PVKSE(410)는 아래의 표 5의 형태로 정의된 메시지를 수신하고, CRS(420)는 수신한 메시지를 이용하여 보안 모듈(330)의 SSD(482)에 애플릿을 설치할 수 있다.

표 5

Tag	Length	Value Description
'4F'	AID Length of PVKSE	AID of PVKSE

- [0161] 표 5를 참조하면, PVKSE(410)가 수신한 메시지는 애플릿을 추가하는 것을 표시하는 태그(4F), AID의 길이, 및 AID를 포함할 수 있다. 본 발명의 다양한 실시예에 따르면, PVKSE(410)는 AID 뿐만 아니라, 애플릿 라벨, 애플릿의 우선 순위, 애플릿의 구체적인 테이터를 수신하고, CRS(420)는 수신한 테이터를 SSD(482)에 추가할 수 있다. 아래의 표 6은 PVKSE(410)가 애플릿을 설치하기 위해 수신한 메시지의 구체적인 예시를 기재하고 있다.

표 6

.....
A3 0F /
4F 0D 32564B2E5359532E4444463031 //Add the PVKSE to the CREL list
A6 19 /
BFOC 16 /
61 14 /
4F 09 D28600015901140001 // AID= D28600015901140001
50 06 424D57205835// Application Label = 'BMW X5'
87 01 01 / Priority indicator = 01
.....

- [0163] 동작 730에서, CRS(420)는 외부 전자 장치(500)의 애플릿의 활성화 여부 또는 애플릿의 우선 순위를 정의할 수 있다. 동작 730에 기재된 내용은 도 8a 내지 도 8b에서 후술한다.
- [0165] 도 8a는 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법에서, 전자 장치의 인증에 이용되는 애플릿의 활성화하는 동작을 도시한 동작 흐름도이다.
- [0166] 도 8a를 참조하면, 전자 장치(예: 전자 장치(300))의 인증에 이용되는 애플릿을 활성화 또는 비활성화하는 동작은 AMUI(application management user interface, 801), CRS(contactless register service, 803), 애플릿(805), PVKSE(807)의 동작을 통하여 이루어질 수 있다.
- [0167] 본 발명의 다양한 실시예에 따르면, AMUI(801)는 사용자와 애플릿(805) 사이에 구현된 인터페이스를 의미할 수 있다. 사용자와 애플릿(805) 사이에 구현된 인터페이스는 시각적 요소를 포함할 수 있으며, 사용자는 AMUI(801) 상에서의 입력을 통해 애플릿(805)의 활성화 요청을 입력할 수 있다. CRS(803)(예: 도 4의 CRS(420))은 보안 모듈(예: 도 3의 보안 모듈(330)) 상에 설치되는 파일 및 애플릿을 관리하는 구성 요소를 의미할 수 있다. 애플릿(805)(예: 도 4의 애플릿(430, 440, 450, 460, 470))은 외부 전자 장치(예: 도 5의 전자 장치(500))와의 인증에 이용되는 테이터를 의미할 수 있다. PVKSE(807)(예: 도 4의 PVKSE(410))은 적어도 하나 이상의 애플릿(805)

의 변경을 모니터링하고, 애플릿(805)와 관련된 정보를 생성 및 관리할 수 있는 소프트웨어적 요소를 의미할 수 있다.

- [0168] 동작 809에서, AMUI(801)는 외부 전자 장치(500)와의 인증에 이용될 수 있는 키를 관리하는 어플리케이션을 실행할 수 있다. 외부 전자 장치(500)와의 인증에 이용될 수 있는 키를 관리하는 어플리케이션은 전자 장치(예: 도 3의 전자 장치(300))의 메모리(예: 도 3의 메모리(340)) 상에 설치될 수 있다. 어플리케이션의 실행은 전자 장치(300)의 사용자 입력에 의해 트리거될 수 있다.
- [0169] 동작 811에서, AMUI(801)는 외부 전자 장치(500)의 인증에 이용되는 애플릿의 정보(811)를 CRS(803)로 요청할 수 있다. 동작 813에서, CRS(803)는 애플릿의 정보를 보안 모듈(330)의 SSD(예: 도 5의 SSD(482))에서 검색하고, 검색 결과에 기반한 애플릿 정보를 AMUI(801)로 전송할 수 있다.
- [0170] 동작 815에서, AMUI(801)는 CRS(803)로부터 수신한 애플릿 정보를 표시 장치(예: 도 1의 표시 장치(160))에 디스플레이할 수 있다. 동작 817에서, AMUI(801)는 디스플레이된 애플릿 정보에 대한 사용자 선택에 기반하여 선택된 애플릿을 활성화할 수 있다. 동작 819에서, AMUI(801)는 선택된 애플릿의 활성화 요청을 CRS(803)로 전송할 수 있다.
- [0171] 동작 821에서, CRS(803)는 선택된 애플릿을 활성화될 수 있도록 애플릿(805)을 제어할 수 있다. 본 발명의 다양한 실시예에 따르면, CRS(803)는 선택된 애플릿에 포함된 활성화 여부를 지시하는 데이터를 변경함으로써, 선택된 애플릿을 활성화하도록 애플릿(805)을 제어할 수 있다. 활성화된 애플릿은 외부 전자 장치(500)와 전자 장치(300)의 인증을 수행 가능한 애플릿을 의미하며, 비활성화된 애플릿은 외부 전자 장치(500)와 전자 장치(300)의 인증이 수행될 수 없는 애플릿을 의미할 수 있다.
- [0172] 동작 823에서, 애플릿(805)은 애플릿(805)의 활성화 상태의 변경을 지시하는 데이터를 PVKSE(807)에 전송할 수 있다. 동작 825에서, PVKSE(807)는 애플릿(805)의 활성화 상태의 변경 여부에 기반하여 애플릿 관련 정보를 생성 또는 변경할 수 있다. 예를 들어, PVKSE(807)은 애플릿(805)이 활성화 상태로 변경된 경우, 표 2에 도시된 템플릿에, 활성화된 애플릿(805)의 정보(AID, 애플릿 라벨, 우선 순위 정보, 애플릿의 구체적인 데이터 등)를 추가하는 방식으로 애플릿 관련 정보를 변경할 수 있다.
- [0173] 동작 827에서, 애플릿(805)은 애플릿(805)의 활성화 상태 변경의 성공을 알리는 메시지를 CRS(803)에 전송하고, 동작 829에서, CRS(803)는 애플릿(805)의 활성화 상태의 변경의 성공을 알리는 메시지를 AMUI(801)로 전송할 수 있다.
- [0175] 도 8b는 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법에서, 전자 장치의 인증에 이용되는 애플릿의 우선 순위를 설정하는 동작을 도시한 동작 흐름도이다.
- [0176] 도 8b를 참조하면, 전자 장치(예: 전자 장치(300))의 인증에 이용되는 애플릿에 할당된 우선 순위를 설정하는 동작은 AMUI(application management user interface, 801), CRS(contactless register service, 803), 애플릿(805), PVKSE(807)의 동작을 통하여 이루어질 수 있다.
- [0177] 본 발명의 다양한 실시예에 따르면, AMUI(801)는 사용자와 애플릿(805) 사이에 구현된 인터페이스를 의미할 수 있다. CRS(803)(예: 도 4의 CRS(420))은 보안 모듈(예: 도 3의 보안 모듈(330)) 상에 설치되는 파일 및 애플릿을 관리하는 구성 요소를 의미할 수 있다. 애플릿(805)(예: 도 4의 애플릿(430, 440, 450, 460, 470))은 외부 전자 장치(예: 도 5의 전자 장치(500))와의 인증에 이용되는 데이터를 의미할 수 있다. PVKSE(807)(예: 도 4의 PVKSE(410))은 적어도 하나 이상의 애플릿(805)의 변경을 모니터링하고, 애플릿(805)과 관련된 정보를 생성 및 관리할 수 있는 소프트웨어적 요소를 의미할 수 있다.
- [0178] 동작 831에서, AMUI(801)는 외부 전자 장치(500)와의 인증에 이용될 수 있는 키를 관리하는 어플리케이션을 실행할 수 있다. 외부 전자 장치(500)와의 인증에 이용될 수 있는 키를 관리하는 어플리케이션은 전자 장치(예: 도 3의 전자 장치(300))의 메모리(예: 도 3의 메모리(340)) 상에 설치될 수 있다. 어플리케이션의 실행은 전자 장치(300)의 사용자 입력에 의해 트리거될 수 있다.
- [0179] 동작 833에서, AMUI(801)는 외부 전자 장치(500)의 인증에 이용되는 애플릿 정보를 CRS(803)로 요청할 수 있다. 동작 835에서, CRS(803)는 애플릿 정보를 보안 모듈(330)의 SSD(482)에서 검색하고, 검색 결과에 기반한 애플릿 정보를 AMUI(801)로 전송할 수 있다.

- [0180] 동작 837에서, AMUI(801)는 CRS(803)로부터 수신한 애플릿 정보를 표시 장치(예: 도 1의 표시 장치(160))에 디스플레이하고, 디스플레이된 애플릿 정보에 대한 사용자 입력에 기반하여 우선 순위 변경의 대상이 되는 애플릿을 선택할 수 있다. AMUI(801)는 선택된 애플릿의 우선 순위 설정을 요청하는 사용자 입력을 수신할 수 있다. 애플릿의 우선 순위 설정은 우선 순위가 설정되어 있지 않은 애플릿에 대한 우선 순위를 지정하는 동작 또는 우선 순위가 설정된 애플릿의 우선 순위를 변경하는 동작을 의미할 수 있다.
- [0181] 동작 839에서, AMUI(801)는 선택된 애플릿의 우선 순위 설정을 요청하는 신호를 CRS(803)으로 전송할 수 있다.
- [0182] 동작 841에서, CRS(803)는 선택된 애플릿의 우선 순위의 설정 동작을 수행하도록 애플릿(805)을 제어할 수 있다. 본 발명의 다양한 실시예에 따르면, 애플릿(805)은 CRS(803)의 제어에 기반하여 선택된 애플릿에 포함된 우선 순위를 지시하는 우선 순위 정보를 변경 또는 생성함으로써, 선택된 애플릿의 우선 순위를 설정할 수 있다. 우선 순위는 외부 전자 장치(500) 상에서 인증이 우선적으로 수행되는 순위를 의미할 수 있다.
- [0183] 동작 843에서, 애플릿(805)은 우선 순위 설정이 되었음을 지시하는 메시지를 PVKSE(807)로 전송할 수 있다. 동작 845에서, PVKSE(807)는 우선 순위 설정을 지시하는 메시지를 수신함에 대응하여, 애플릿 관련 정보를 생성 또는 변경할 수 있다. PVKSE(807)은 애플릿(805)의 우선 순위가 변경된 경우, 표 2에 도시된 템플릿에, 활성화된 애플릿(805)의 정보에 포함된 우선 순위 정보를 변경하는 방식으로 애플릿 관련 정보를 변경할 수 있다.
- [0184] 동작 847에서, 애플릿(805)은 우선 순위 설정이 성공했음을 알리는(notify) 메시지를 CRS(803)로 전송할 수 있다. 동작 849에서, CRS(803)는 우선 순위 설정이 성공했음을 알리는 메시지를 AMUI(801)로 전송할 수 있다. 동작 851에서, AMUI(801)는 애플릿 리스트를 업데이트할 수 있다. 애플릿 리스트는 변경된 우선 순위에 기반하여 업데이트될 수 있으며, 애플릿 리스트는 애플릿들 각각에 설정된 우선 순위의 순서(예를 들면, 우선 순위가 가장 높은 애플릿 순으로)에 따라서 배열될 수 있다.
- [0186] 도 9는 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법에서, 도 5의 전자 장치 상에서 전자 장치의 인증을 수행하는 동작을 도시한 동작 흐름도이다.
- [0187] 동작 901에서, 전자 장치(예: 도 5의 전자 장치(500))의 프로세서(예: 도 5의 프로세서(510))는 제 1 AID 리스트를 수신할 수 있다.
- [0188] 예를 들면, 도 4에 도시된 보안 모듈(330) 상에 저장된 애플릿들 중 활성화된 애플릿의 식별자를 포함하는 제 1 AID 리스트는 Vendor1 Vehicle Key2(Vendor 1 VK2)/ Vendor2 Vehicle Key1(Vendor 2 VK1)/ Sharing Key1(SK1)/ Sharing Key2(SK2)가 포함될 수 있다.
- [0189] 본 발명의 다양한 실시예에 따르면, 전자 장치(500)의 프로세서(510)는 전자 장치(500)가 수행할 수 있는 다양한 기능들 중 적어도 일부의 기능을 활성화하는 요청 신호를 외부 전자 장치(예: 도 3의 전자 장치(300))로부터 수신할 수 있다. 예를 들면, 외부 전자 장치(300)는 외부 전자 장치(300)의 사용자 입력에 기반하여 전자 장치(500)의 일부 기능을 수행할 것(예를 들면, 전자 장치(500)의 문의 잠금을 해제, 전자 장치(500)의 라이트를 켜는 기능, 또는 전자 장치(500)의 자동 출차 기능)을 요청하는 신호를 생성하고, 생성된 신호를 전자 장치(500)로 전송할 수 있다. 프로세서(510)는 외부 전자 장치(300)가 전송한 전자 장치(500)의 일부 기능을 수행할 것을 요청하는 신호의 수신에 대응하여 외부 전자 장치(300)와의 인증을 시작할 수 있다.
- [0190] 본 발명의 다양한 실시예에 따르면, 제 1 AID 리스트는 외부 전자 장치(300)의 보안 모듈(330) 상에 구현된 PVKSE(예: 도 4의 PVKSE(410))에 의해 생성될 수 있다.
- [0191] 동작 903에서, 프로세서(510)는 제 1 AID 리스트에 포함된 AID들 중, 전자 장치(500)가 지원 가능한 적어도 하나 이상의 AID를 선택하고, 선택된 적어도 하나 이상의 AID가 포함된 제 2 AID 리스트를 생성하고, 외부 전자 장치(300)로 제 2 AID 리스트를 전송할 수 있다.
- [0192] 본 발명의 다양한 실시예에 따르면, 프로세서(510)는 제 1 AID 리스트에 포함된 AID들 중, 전자 장치(500)가 지원하지 않는 AID를 갖는 애플릿을 필터링(filter-out)하는 방식을 통해, 남겨진 적어도 하나 이상의 AID를 선택하는 방식으로, AID를 선택할 수 있다.
- [0193] 본 발명의 다른 실시예에 따르면, 프로세서(510)는 제 1 AID 리스트에 포함된 AID들 중, 전자 장치(500)의 제조사와 동일한 AID를 갖는 애플릿을 선택하는 방식으로, AID를 선택할 수 있다.
- [0194] 본 발명의 또 다른 실시예에 따르면, 프로세서(510)는 제 1 AID 리스트에 포함된 AID들 중, 전자 장치(500)의

제조사와 동일한 AID를 갖는 애플릿과, 공유 키(sharing key)에 대응하는 AID들 중, 전자 장치(500)가 지원하지 않는 AID를 갖는 애플릿을 필터링(filter-out)하는 방식을 통해, 남겨진 적어도 하나 이상의 AID를 선택하는 방식으로, AID를 선택할 수 있다.

[0195] 예를 들면, 전자 장치(500)가 제조사 1에 의해 제조된 경우, 제 1 AID 리스트에 포함된 AID들인 Vendor1 Vehicle Key2(Vendor 1 VK2)/ Vendor2 Vehicle Key1(Vendor 2 VK1)/ Sharing Key1(SK1)/ Sharing Key2(SK2) 중, 제조사 2에 대응하는 Vendor2 Vehicle Key1(Vendor 2 VK1)와 제조사 3에 대응하는 Sharing Key2(SK2)을 제외한 나머지 AID들인 Vendor1 Vehicle Key2(Vendor 1 VK2)/ Sharing Key1(SK1)가 선택될 수 있다.

[0196] 본 발명의 다양한 실시예에 따르면, 외부 전자 장치(300)의 PVKSE(410)는 제 2 AID 리스트를 수신하고, 제 2 AID 리스트에 포함된 AID 각각에 대응하는 애플릿과 관련된 정보를 전자 장치(500)로 전송할 수 있다. 전자 장치(500)는 PVKSE(410)가 전송한 애플릿과 관련된 정보를 수신할 수 있다.

[0197] 예를 들면, 제 2 AID 리스트는 전자 장치(500)가 선택한 AID들이 포함될 수 있으며, 제 2 AID 리스트에는 Vendor1 Vehicle Key2(Vendor 1 VK2)/ Sharing Key1(SK1)가 포함될 수 있다.

[0198] 동작 905에서, 프로세서(510)는 제 2 AID 리스트에 포함된 AID들 중, 우선 순위가 가장 높은 AID를 선택할 수 있다. 동작 907에서, 프로세서(510)는 우선 순위가 가장 높은 AID에 대응하는 애플릿 관련 정보를 이용하여 인증을 수행할 수 있다.

[0199] 동작 909에서, 프로세서(510)는 인증이 성공했는지 판단하고, 동작 911에서, 프로세서(510)는 인증이 실패한 경우, 제 2 AID 리스트에 포함되고, 인증에 이용되지 않은 AID들 중, 가장 우선 순위가 높은 AID를 선택하고, 동작 907에 기재된 인증을 다시 수행할 수 있다.

[0201] 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법은 통신 모듈(예: 도 5의 통신 모듈(520))이 외부 전자 장치(예: 도 3의 전자 장치(300))와의 연결을 위한 연결 요청 신호를 방송(broadcasting)하고, 상기 방송된 신호에 응답한 외부 전자 장치(300)와 통신 채널을 수립하는 동작; 보안 모듈(예: 도 5의 보안 모듈(530))이 상기 외부 전자 장치(300)에 저장된 적어도 하나 이상의 AID(Application identifier)를 포함하는 AID 리스트를 전송할 것을 요청하는 신호를 전송하는 동작; 보안 모듈(530)이 상기 외부 전자 장치(300)가 전송한 상기 AID 리스트에 포함된 AID 중 적어도 하나 이상의 AID를 선택하는 동작; 보안 모듈(530)이 상기 선택된 AID에 대응하는 애플릿을 지시하는 정보 및 상기 선택된 AID에 대응하는 애플릿과 관련된 정보를 외부 전자 장치(300)에 요청하는 동작; 및 보안 모듈(530)이 상기 외부 전자 장치(300)로부터 수신한 상기 애플릿과 관련된 정보를 이용하여 상기 외부 전자 장치(300)와 인증을 수행하는 동작을 포함할 수 있다.

[0202] 본 발명의 다양한 실시예에 따르면, 상기 적어도 하나 이상의 AID를 선택하는 동작은 보안 모듈(530)이 상기 AID 리스트에 포함된 AID들 중 상기 전자 장치(예: 도 5의 전자 장치(500))의 제조사와 다른 제조사에 대응하는 AID를 제외한 나머지 AID를 선택하는 동작을 포함하고, 상기 외부 전자 장치(400)와 인증을 수행하는 동작은 상기 AID에 지정된 우선 순위에 기반하여 인증을 수행하는 동작을 포함할 수 있다.

[0205] 본 문서에 개시된 다양한 실시예들에 따른 전자 장치는 다양한 형태의 장치가 될 수 있다. 전자 장치는, 예를 들면, 휴대용 통신 장치 (예: 스마트폰), 컴퓨터 장치, 휴대용 멀티미디어 장치, 휴대용 의료 기기, 카메라, 웨어러블 장치, 또는 가전 장치를 포함할 수 있다. 본 문서의 실시예에 따른 전자 장치는 전술한 기기들에 한정되지 않는다.

[0206] 본 문서의 다양한 실시예들 및 이에 사용된 용어들은 본 문서에 기재된 기술적 특징들을 특정한 실시예들로 한정하려는 것이 아니며, 해당 실시예의 다양한 변경, 균등물, 또는 대체물을 포함하는 것으로 이해되어야 한다. 도면의 설명과 관련하여, 유사한 또는 관련된 구성요소에 대해서는 유사한 참조 부호가 사용될 수 있다. 아이템에 대응하는 명사의 단수 형은 관련된 문맥상 명백하게 다르게 지시하지 않는 한, 상기 아이템 한 개 또는 복수개를 포함할 수 있다. 본 문서에서, "A 또는 B", "A 및 B 중 적어도 하나", "A 또는 B 중 적어도 하나," "A, B 또는 C," "A, B 및 C 중 적어도 하나," 및 "A, B, 또는 C 중 적어도 하나"와 같은 문구들 각각은 그 문구들 중 해당하는 문구에 함께 나열된 항목들의 모든 가능한 조합을 포함할 수 있다. "제 1", "제 2", 또는 "첫째" 또는 "둘째"와 같은 용어들은 단순히 해당 구성요소를 다른 해당 구성요소와 구분하기 위해 사용될

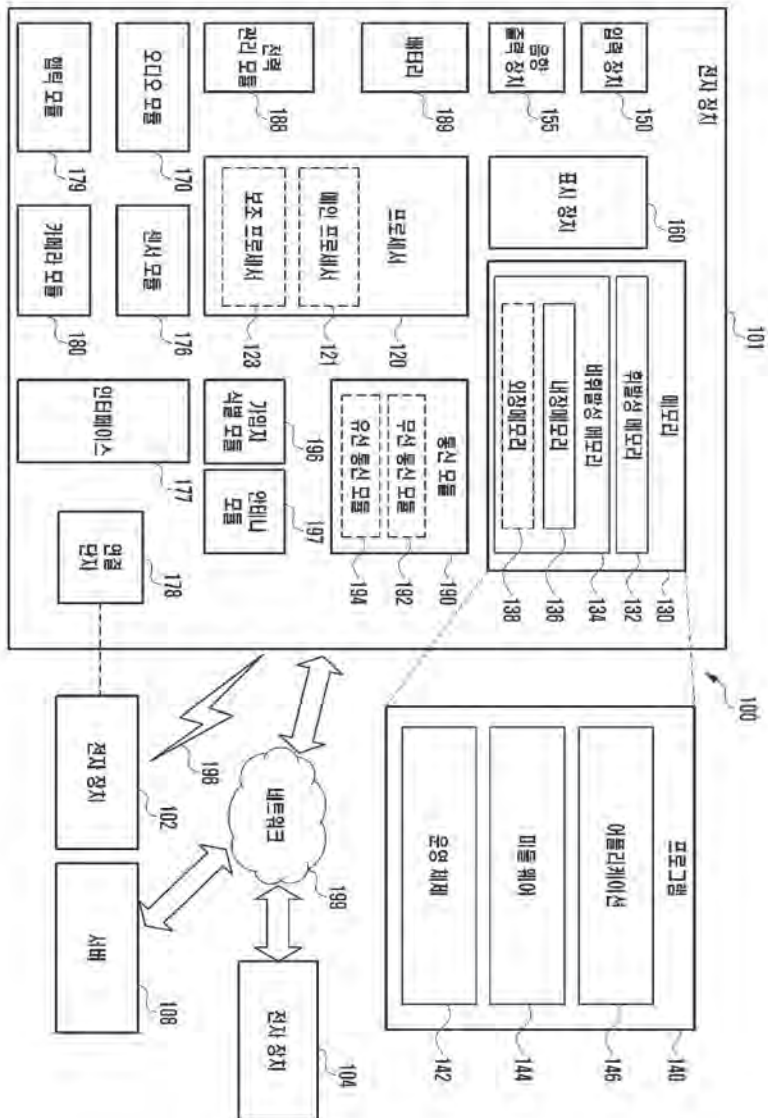
수 있으며, 해당 구성요소들을 다른 측면(예: 중요성 또는 순서)에서 한정하지 않는다. 어떤(예: 제 1) 구성요소가 다른(예: 제 2) 구성요소에, “기능적으로” 또는 “통신적으로” 라는 용어와 함께 또는 이런 용어 없이, “커플드” 또는 “커넥티드” 라고 언급된 경우, 그것은 상기 어떤 구성요소가 상기 다른 구성요소에 직접적으로(예: 유선으로), 무선으로, 또는 제 3 구성요소를 통하여 연결될 수 있다는 것을 의미한다.

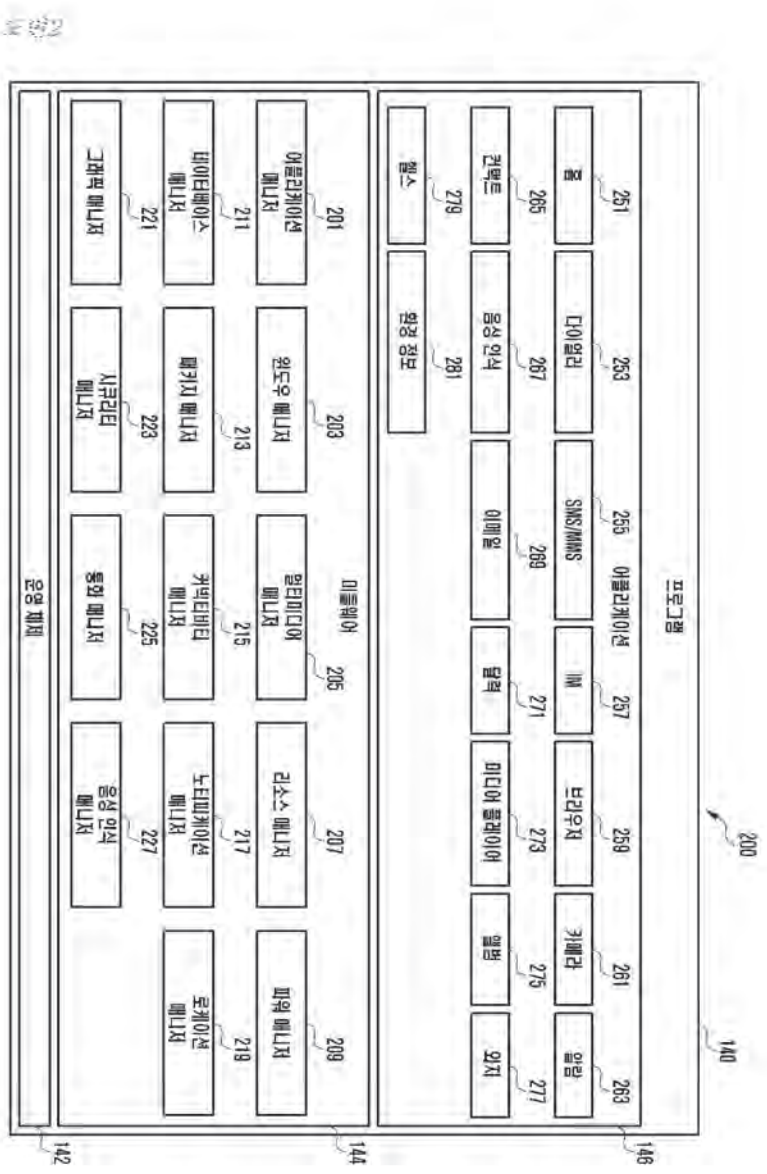
[0207] 본 문서에서 사용된 용어 “모듈”은 하드웨어, 소프트웨어 또는 펌웨어로 구현된 유닛을 포함할 수 있으며, 예를 들면, 로직, 논리 블록, 부품, 또는 회로 등의 용어와 상호 호환적으로 사용될 수 있다. 모듈은, 일체로 구성된 부품 또는 하나 또는 그 이상의 기능을 수행하는, 상기 부품의 최소 단위 또는 그 일부가 될 수 있다. 예를 들면, 일실시예에 따르면, 모듈은 ASIC(application-specific integrated circuit)의 형태로 구현될 수 있다.

[0208] 본 문서의 다양한 실시예들은 기기(machine)(예: 전자 장치(101)) 의해 읽을 수 있는 저장 매체(storage medium)(예: 내장 메모리(136) 또는 외장 메모리(138))에 저장된 하나 이상의 명령어들을 포함하는 소프트웨어(예: 프로그램(140))로서 구현될 수 있다. 예를 들면, 기기(예: 전자 장치(101))의 프로세서(예: 프로세서(120))는, 저장 매체로부터 저장된 하나 이상의 명령어들 중 적어도 하나의 명령을 호출하고, 그것을 실행할 수 있다. 이것은 기기가 상기 호출된 적어도 하나의 명령어에 따라 적어도 하나의 기능을 수행하도록 운영되는 것을 가능하게 한다. 상기 하나 이상의 명령어들은 컴퓨터로 읽을 수 있는 형태(예: 비일시적(non-transitory) 저장매체)로 제공될 수 있다. 여기서, ‘비일시적’은 저장매체가 실체(tangible)하는 장치이고, 신호(signal)(예: 전자 기파)를 포함하지 않는다는 것을 의미할 뿐이며, 이 용어는 데이터가 저장매체에 반영구적으로 저장되는 경우와 임시적으로 저장되는 경우를 구분하지 않는다.

[0209] 일실시예에 따르면, 본 문서에 개시된 다양한 실시예들에 따른 방법은 컴퓨터 프로그램 제품(computer program product)에 포함되어 제공될 수 있다. 컴퓨터 프로그램 제품은 상품으로서 판매자 및 구매자 간에 거래될 수 있다. 컴퓨터 프로그램 제품은 기기로 읽을 수 있는 저장 매체(예: compact disc read only memory (CD-ROM))의 형태로 배포되거나, 또는 어플리케이션 스토어(예: 플레이 스토어™)를 통해 또는 두개의 사용자 장치들(예: 스마트폰들) 간에 직접, 온라인으로 배포(예: 다운로드 또는 업로드)될 수 있다. 온라인 배포의 경우에, 컴퓨터 프로그램 제품의 적어도 일부는 제조사의 서버, 어플리케이션 스토어의 서버, 또는 중계 서버의 메모리와 같은 기기로 읽을 수 있는 저장 매체에 적어도 일시 저장되거나, 임시적으로 생성될 수 있다.

[0210] 다양한 실시예들에 따르면, 상기 기술한 구성요소들의 각각의 구성요소(예: 모듈 또는 프로그램)는 단수 또는 복수의 개체를 포함할 수 있다. 다양한 실시예들에 따르면, 전술한 해당 구성요소들 중 하나 이상의 구성요소들 또는 동작들이 생략되거나, 또는 하나 이상의 다른 구성요소들 또는 동작들이 추가될 수 있다. 대체적으로 또는 추가적으로, 복수의 구성요소들(예: 모듈 또는 프로그램)은 하나의 구성요소로 통합될 수 있다. 이런 경우, 통합된 구성요소는 상기 복수의 구성요소들 각각의 구성요소의 하나 이상의 기능들을 상기 통합 이전에 상기 복수의 구성요소들 중 해당 구성요소에 의해 수행되는 것과 동일 또는 유사하게 수행할 수 있다. 다양한 실시예들에 따르면, 모듈, 프로그램 또는 다른 구성요소에 의해 수행되는 동작들은 순차적으로, 병렬적으로, 반복적으로, 또는 휴리스틱하게 실행되거나, 상기 동작들 중 하나 이상이 다른 순서로 실행되거나, 생략되거나, 또는 하나 이상의 다른 동작들이 추가될 수 있다.







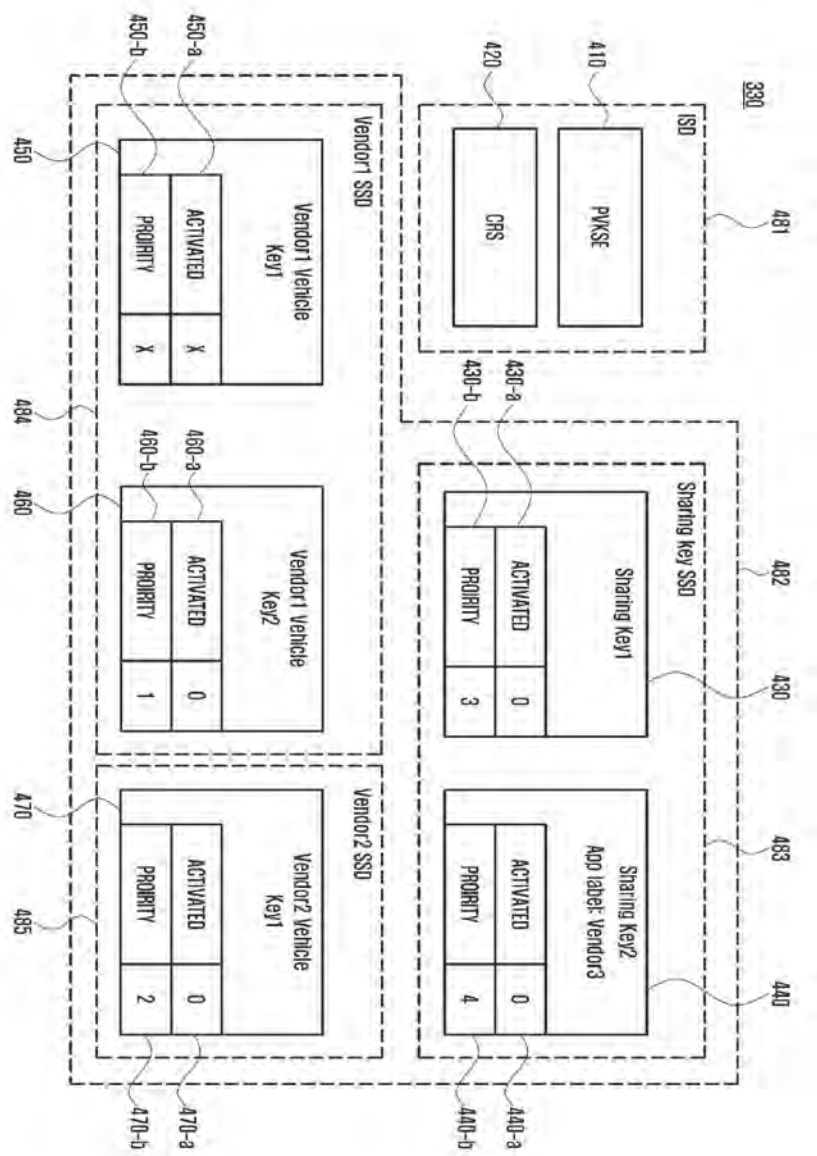
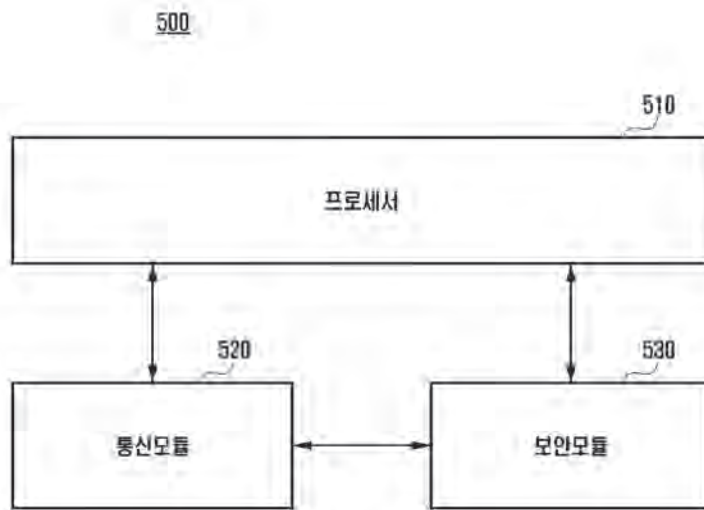
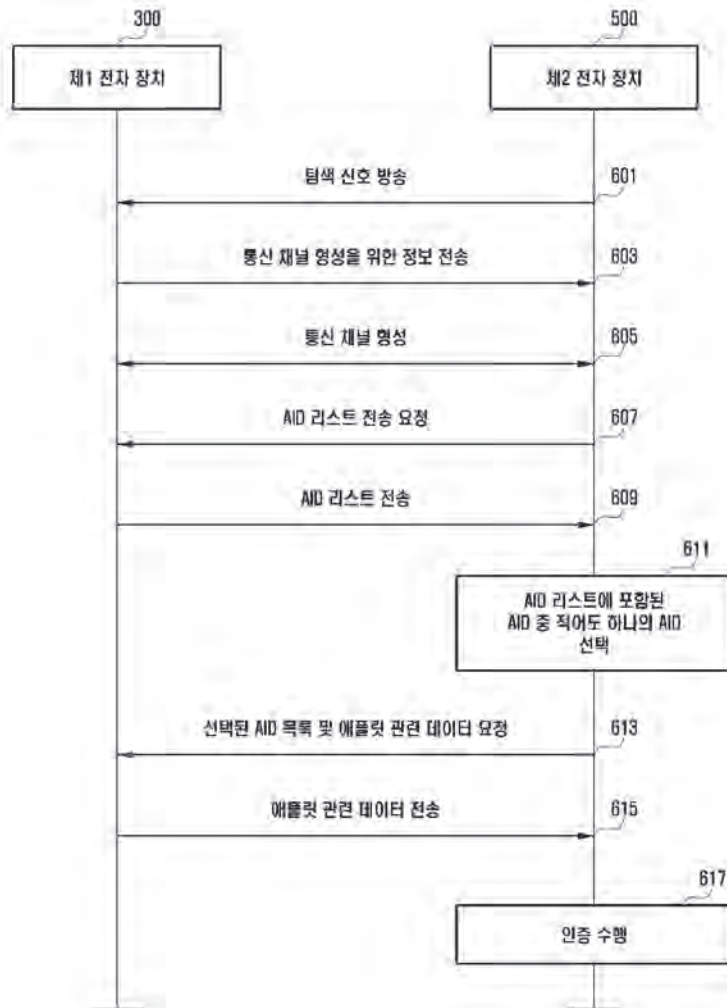


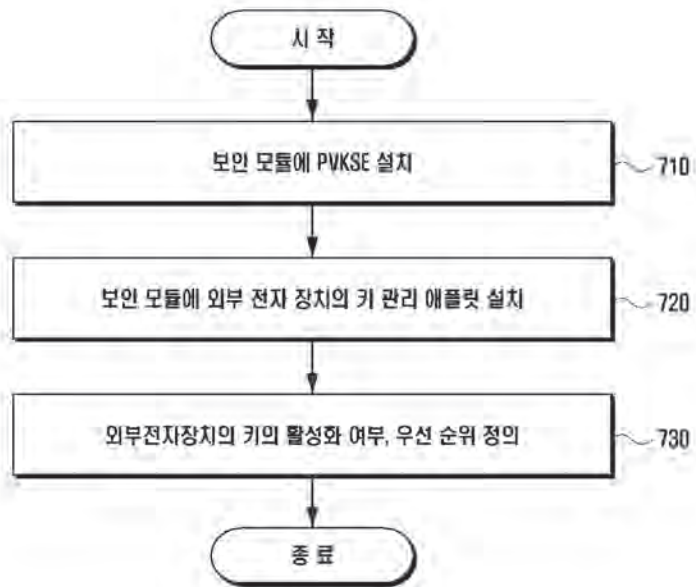
FIG 5



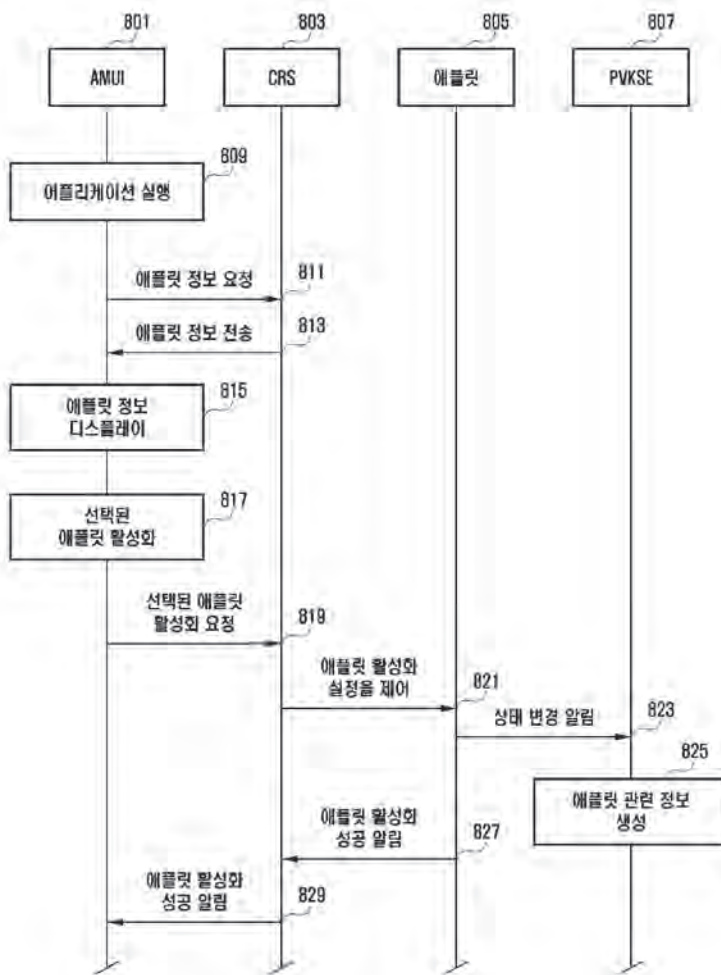
도 8b



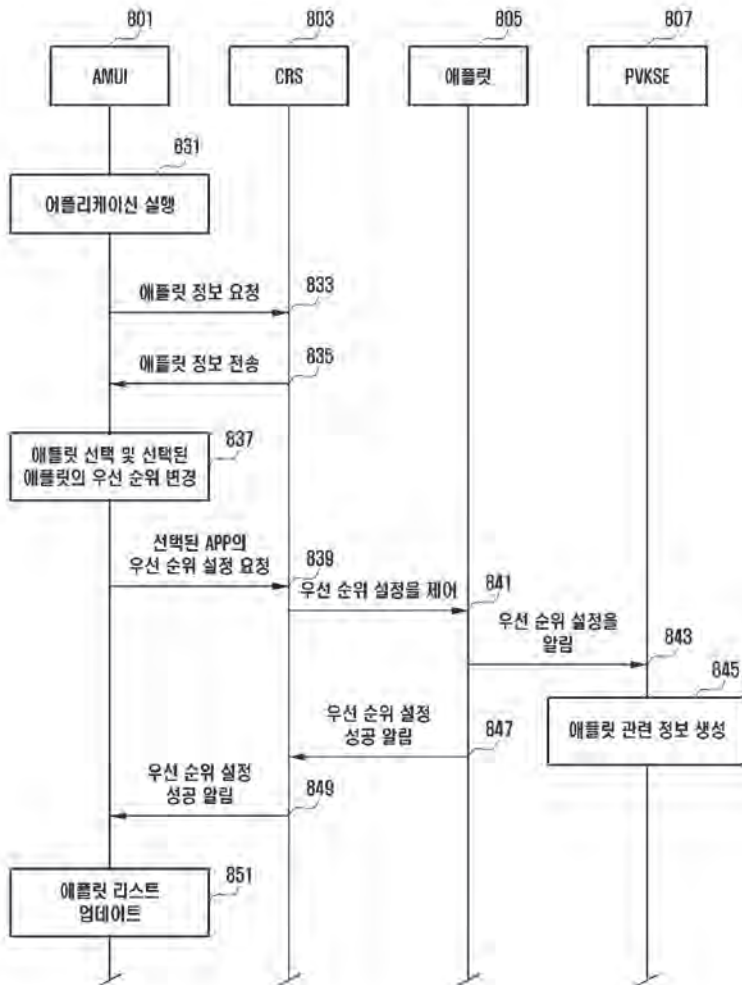
도 2



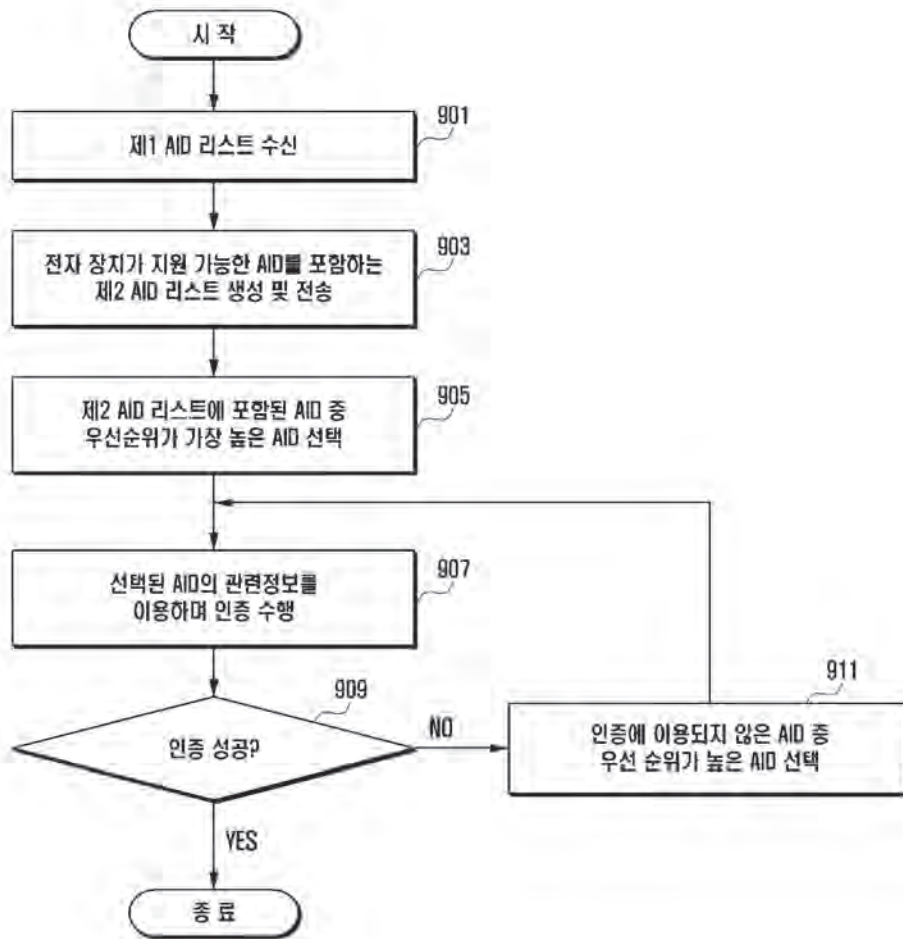
도 8a



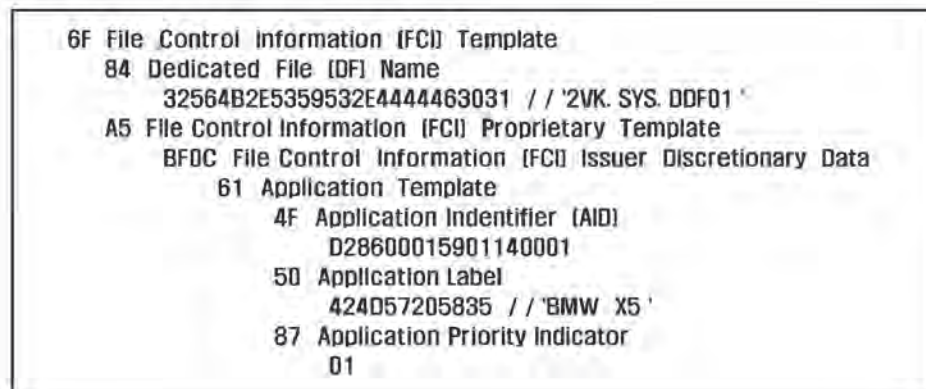
도면 11



도면 9



도면 10



Doc code: RCEX

Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (01-22)

Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	17/767,153	Filing Date	2022-04-07	Docket Number (if applicable)	GMT4110US/WO MQ/MB	Art Unit	2444
First Named Inventor	Mourad FAHER			Examiner Name	RICHARD G KEEHN		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV**SUBMISSION REQUIRED UNDER 37 CFR 1.114**

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____☐ Other _____☒ Enclosed☐ Amendment/Reply☒ Information Disclosure Statement (IDS)☐ Affidavit(s)/ Declaration(s)☐ Other _____**MISCELLANEOUS**☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____.
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)☐ Other _____**FEES****The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**☒ The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to
Deposit Account No 604092**SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED**☒ Patent Practitioner Signature☐ Applicant Signature

Doc code: RCEX

Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Adam F. LEWENTAL/	Date (YYYY-MM-DD)	2024-10-25
Name	Adam F. LEWENTAL	Registration Number	73527

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17767153
	Filing Date	2022-04-07
	First Named Inventor	Mourad FAHER
	Art Unit	2444
	Examiner Name	RICHARD G KEEHN
	Attorney Docket Number	GMT4110US/WO MQ/MB

U.S. PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S. PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1	20160029483	A1	2016-10-06	United Services Automobile Association (USAA) -US			
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1020190115361	KR	A	2019-10-11	Samsung Electronics co ltd		☒
If you wish to add additional Foreign Patent Document citation information please click the Add button.							Add	
NON-PATENT LITERATURE DOCUMENTS							Remove	
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.						T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17767153
Filing Date	2022-04-07
First Named Inventor	Mourad FAHER
Art Unit	2444
Examiner Name	RICHARD G KEEHN
Attorney Docket Number	GMT4110US/WO MQ/MB

1		☐
---	--	--------------------------

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17767153
Filing Date	2022-04-07
First Named Inventor	Mourad FAHER
Art Unit	2444
Examiner Name	RICHARD G KEEHN
Attorney Docket Number	GMT4110US/WO MQ/MB

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Adam F. Lewental/	Date (YYYY-MM-DD)	2024-10-25
Name/Print	Adam F. LEWENTAL	Registration Number	73527

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



US 20200391695A1

(19) **United States**(12) **Patent Application Publication****YANG et al.**(10) **Pub. No.: US 2020/0391695 A1**(43) **Pub. Date: Dec. 17, 2020**

(54) **ELECTRONIC DEVICE FOR MANAGING APPLICATION RELATING TO KEY OF EXTERNAL ELECTRONIC DEVICE, AND OPERATING METHOD OF ELECTRONIC DEVICE**

(52) **U.S. Cl.**

CPC *B60R 25/241* (2013.01); *G06F 21/35* (2013.01)

(71) Applicant: **Samsung Electronics Co., Ltd.**,
Gyeonggi-do (KR)

(57)

ABSTRACT

(72) Inventors: **Yi YANG**, Gyeonggi-do (KR);
Jonghwan KIM, Gyeonggi-do (KR);
Byounghak JIN, Gyeonggi-do (KR);
Bokun CHOI, Gyeonggi-do (KR)

In an electronic device and an operating method of an electronic device, according to various embodiments, the electronic device comprises: a communication module frequently performing communication with an external electronic device; and a security module which monitors a change in data relating to an applet for managing a key used for the authentication of the external electronic device, which manages information relating to the applet, and which stores the applet and an applet identification (AID) list including at least one AID, wherein the security module can be configured to receive, from the external electronic device, a signal for requesting the application identifier (AID) list to be transmitted, transmit the AID list to the external electronic device through the communication module in response to the reception of the requesting signal, receive, from the external electronic device, a signal for requesting information relating to an applet associated with at least one AID selected, from among AIDs included in the AID list, by the external electronic device, and transmit, to the external electronic device, information relating to an applet corresponding to the selected AID. Additional various embodiments are possible.

(21) Appl. No.: **16/977,731**

(22) PCT Filed: **Mar. 14, 2019**

(86) PCT No.: **PCT/KR2019/002945**

§ 371 (c)(1),

(2) Date: **Sep. 2, 2020**

(30) **Foreign Application Priority Data**

Apr. 2, 2018 (KR) 10-2018-0038324

Publication Classification

(51) **Int. Cl.**

B60R 25/24 (2006.01)

G06F 21/35 (2006.01)

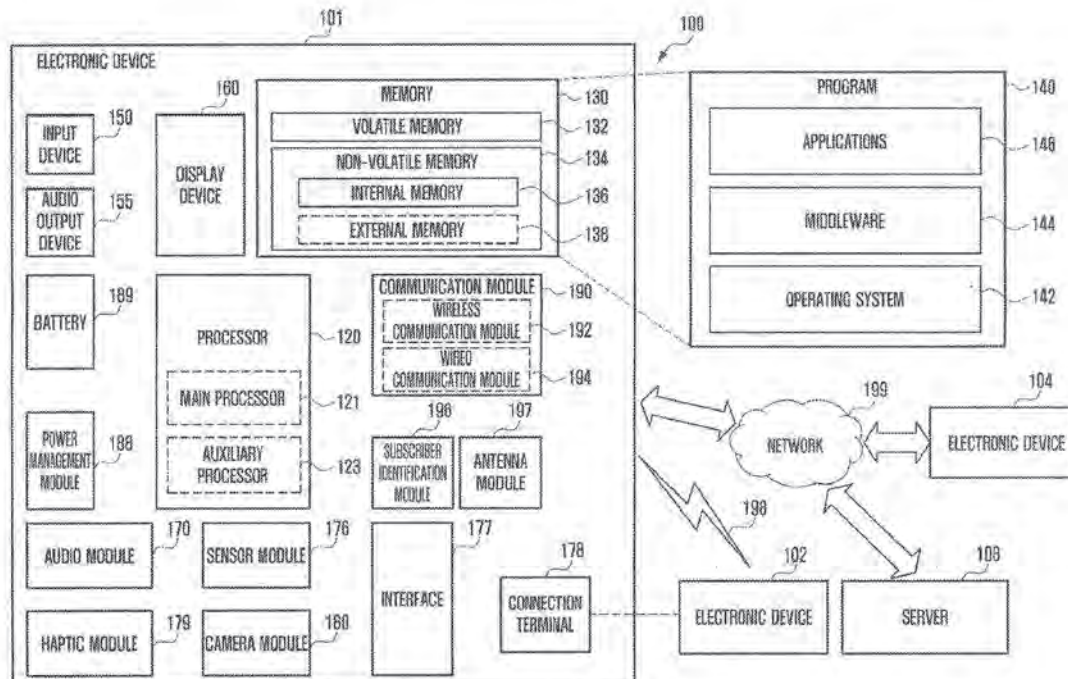


FIG. 1

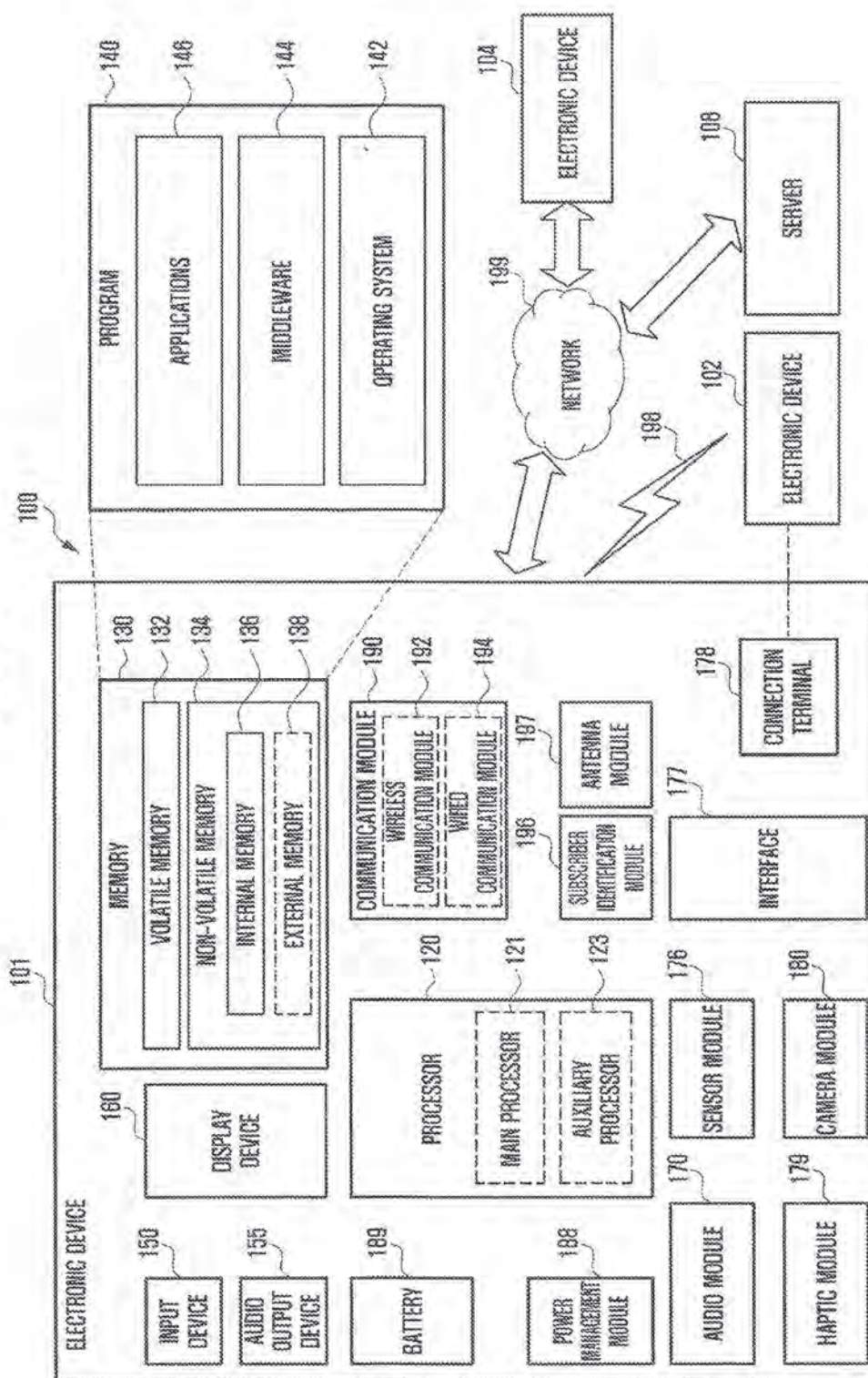


FIG. 2

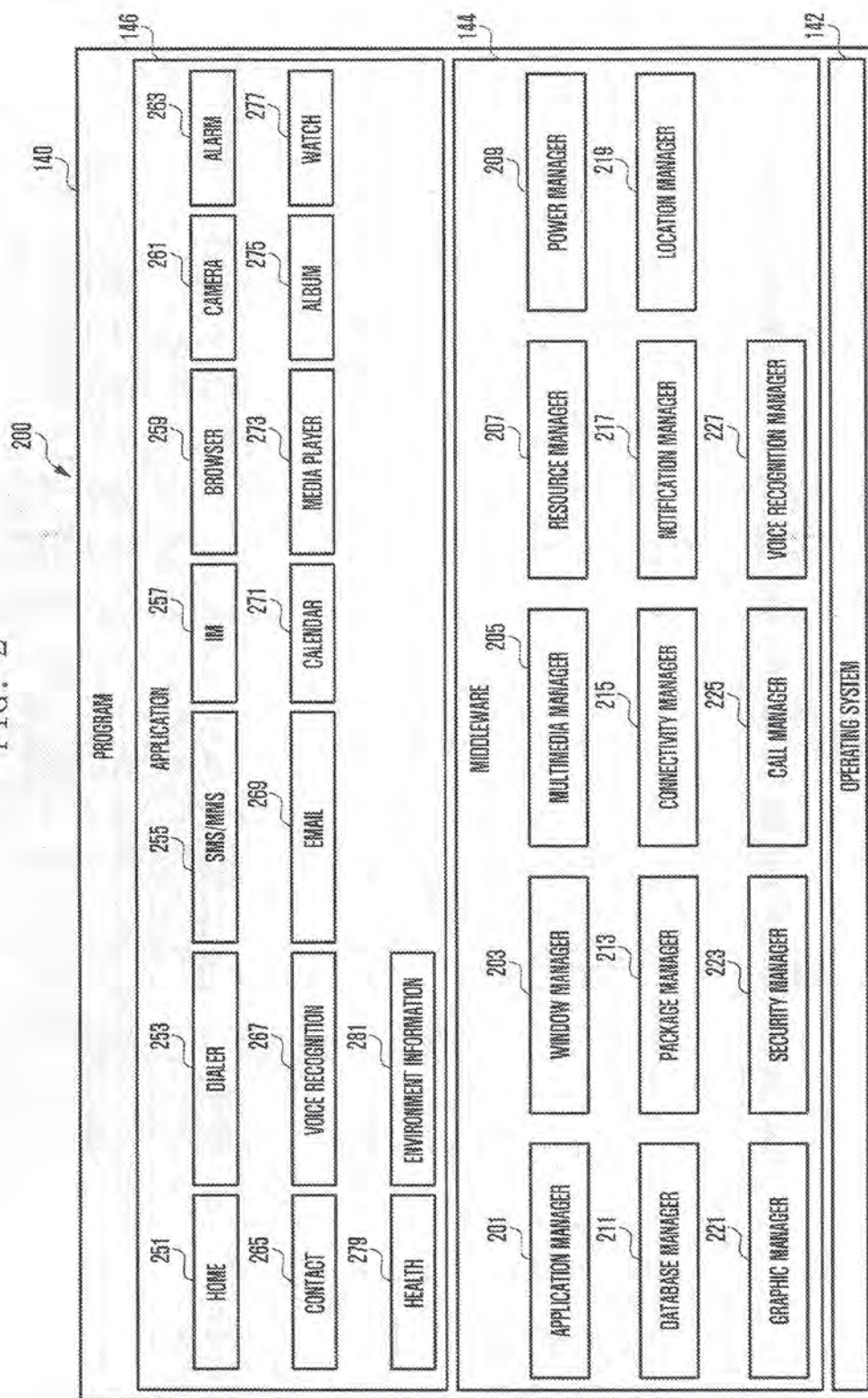
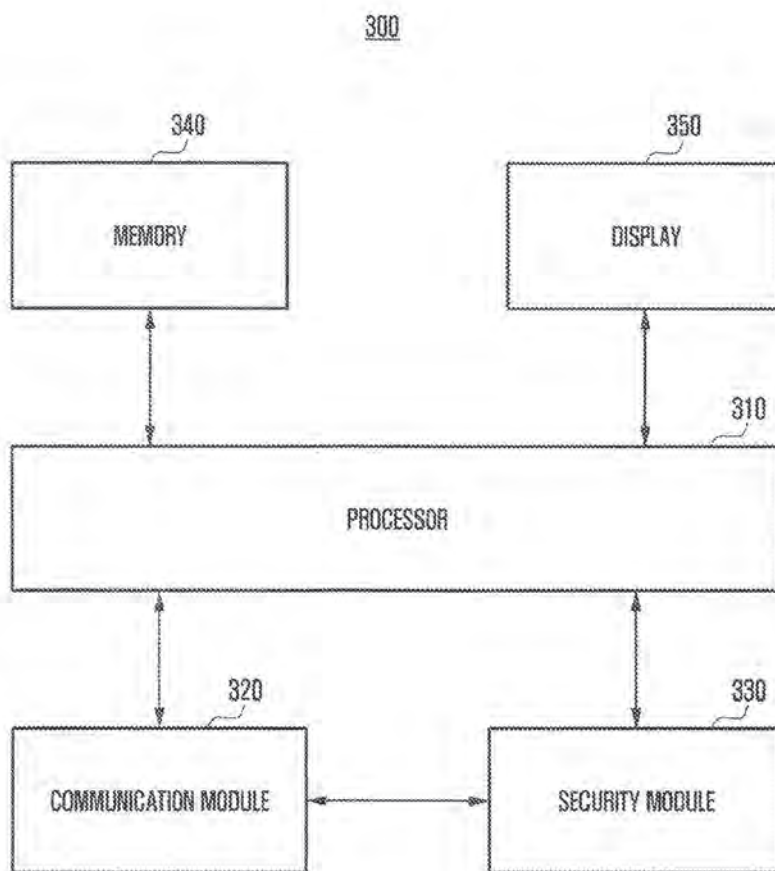


FIG. 3



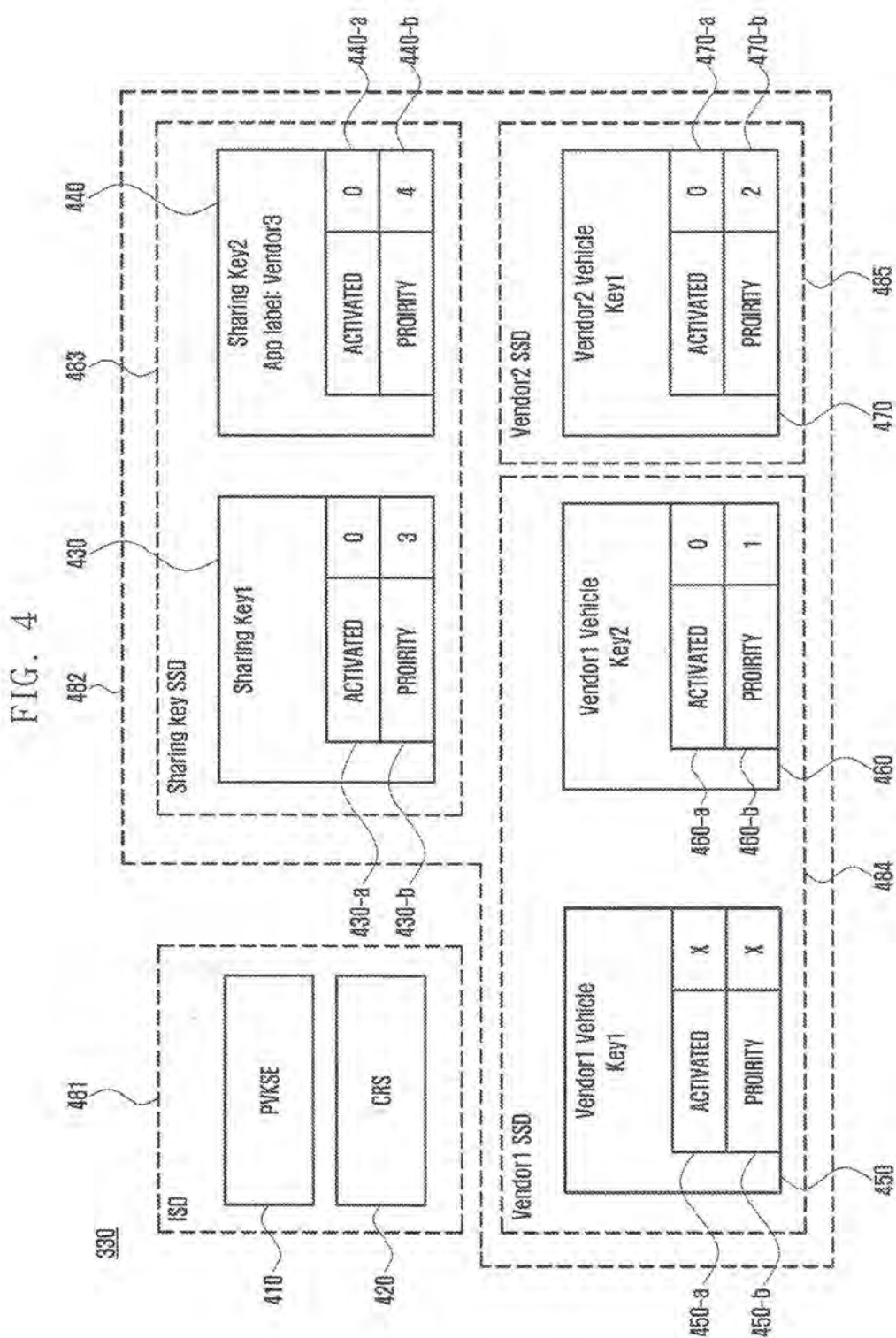


FIG. 5

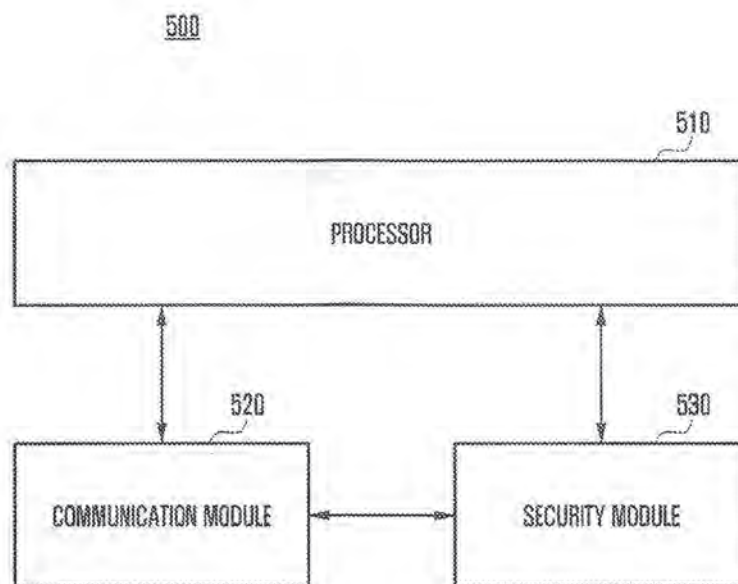


FIG. 6

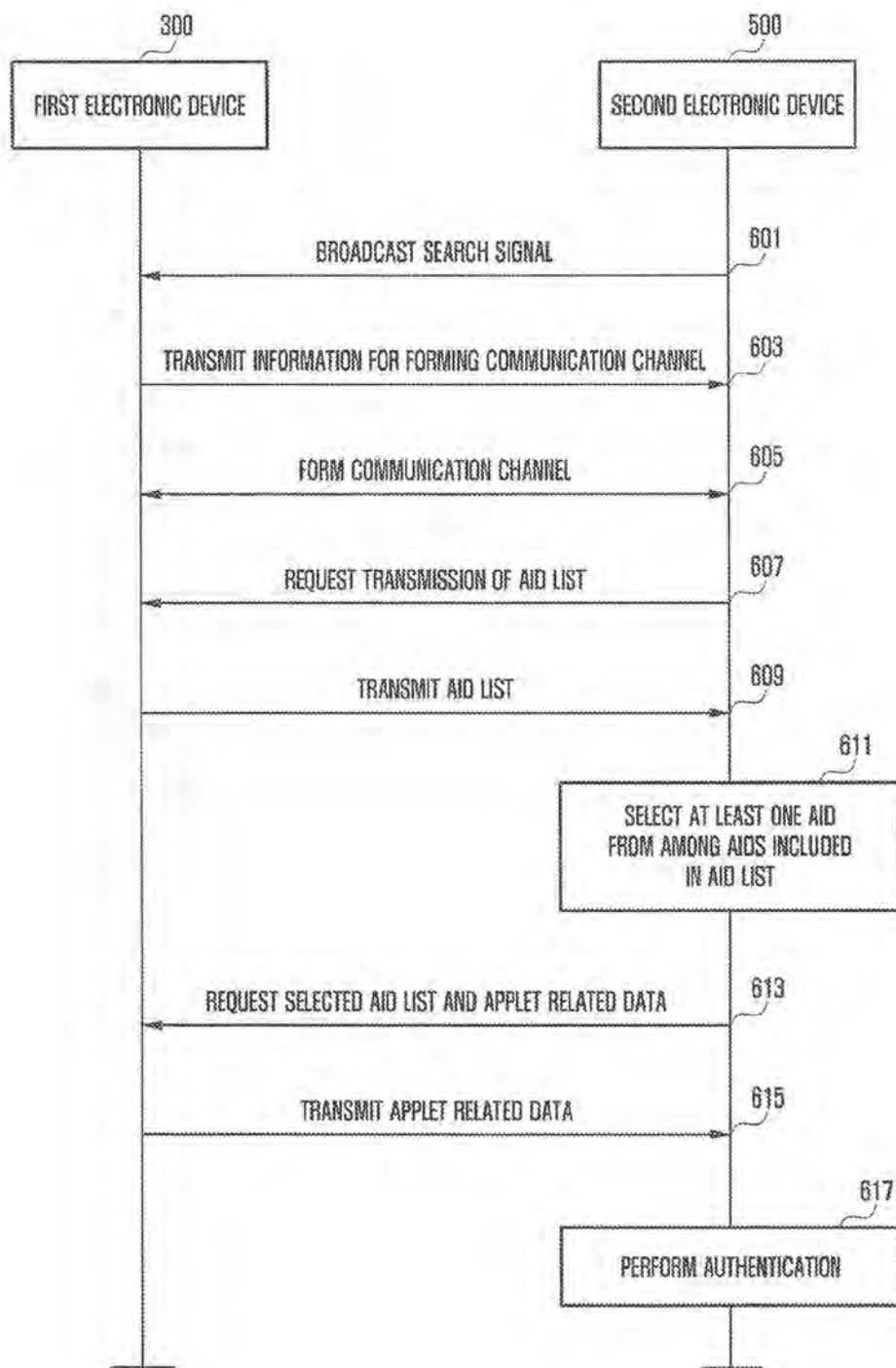


FIG. 7

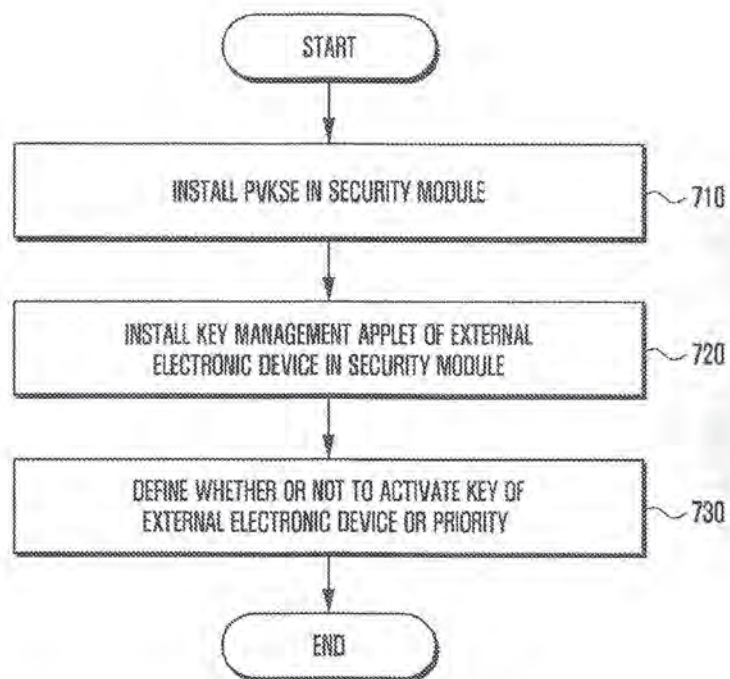


FIG. 8A

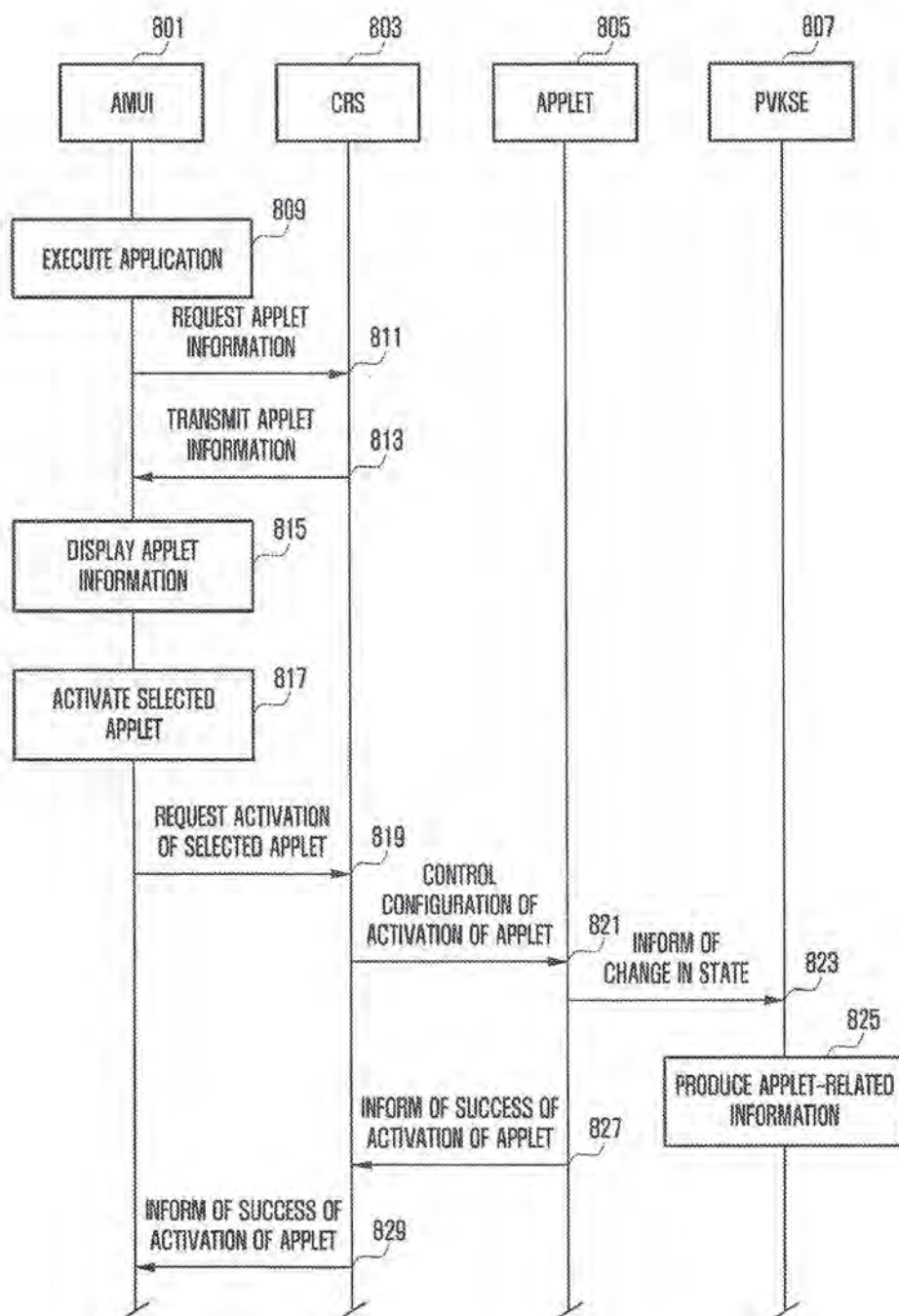


FIG. 8B

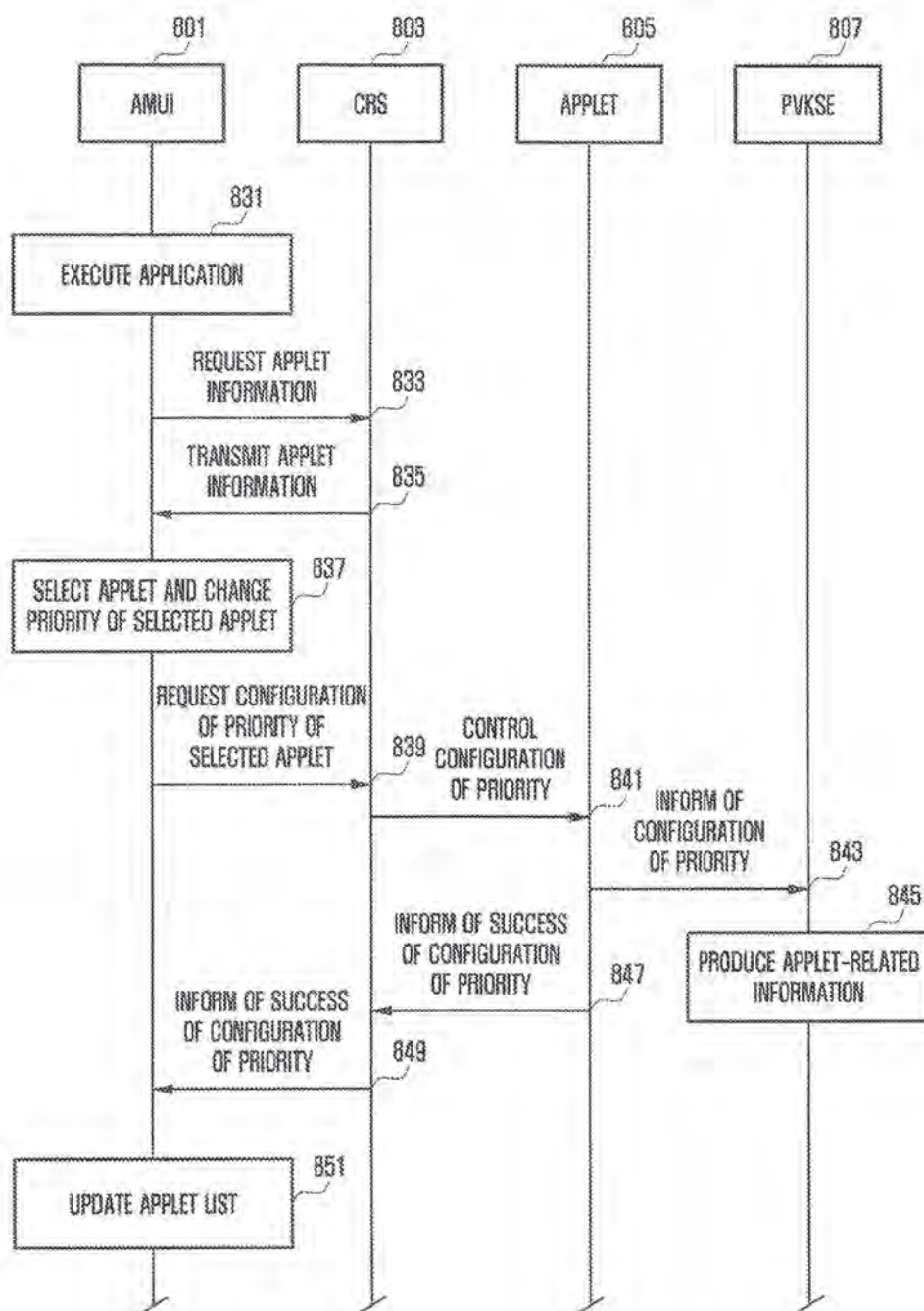


FIG. 9

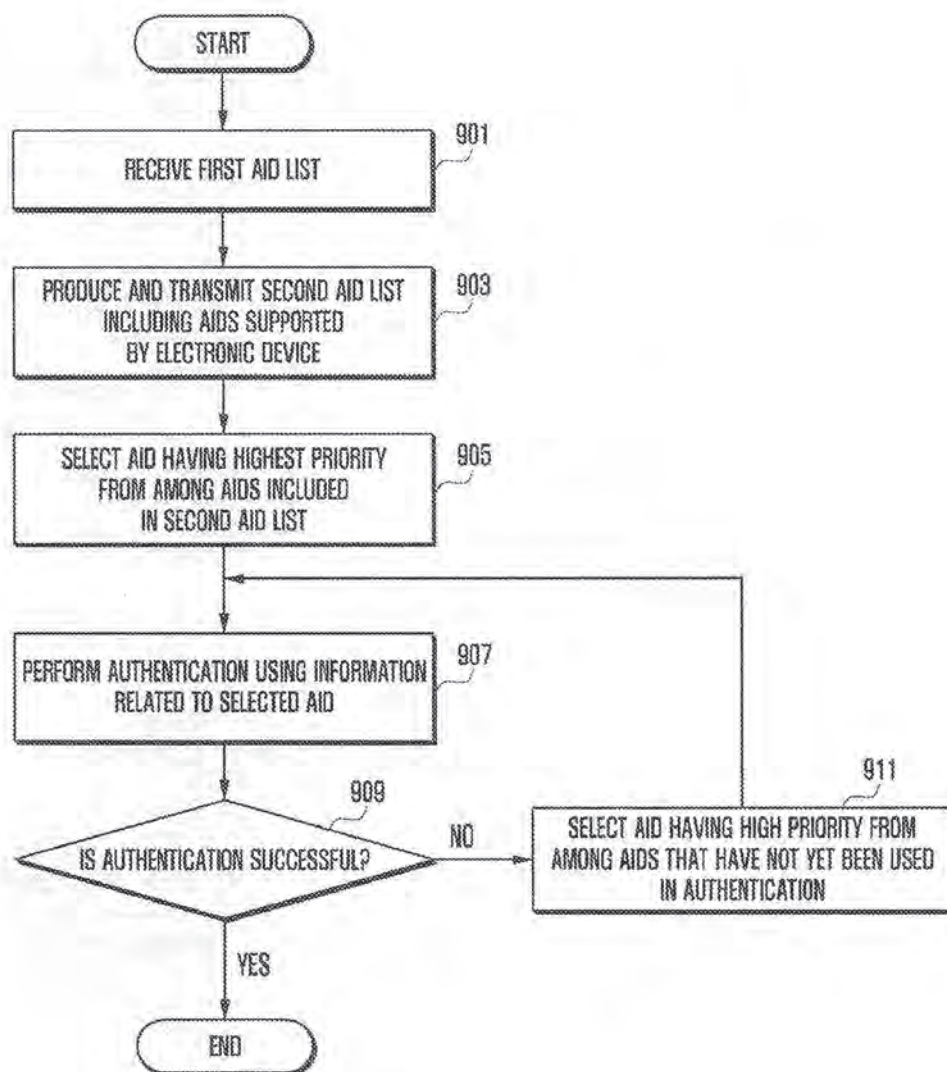


FIG. 10

```
6F File Control Information (FCI) Template
  84 Dedicated File (DF) Name
    32564B2E5359532E4444463031 // '2VK.SYS.DDF01'
  A5 File Control Information (FCI) Proprietary Template
    BFOC File Control Information (FCI) Issuer Discretionary Data
      61 Application Template
        4F Application Identifier (AID)
          028600015901140001
        50 Application Label
          424057205835 // 'BMW X5'
        87 Application Priority Indicator
          01
```


**ELECTRONIC DEVICE FOR MANAGING
APPLICATION RELATING TO KEY OF
EXTERNAL ELECTRONIC DEVICE, AND
OPERATING METHOD OF ELECTRONIC
DEVICE**

TECHNICAL FIELD

[0001] Various embodiments of the disclosure relate to an electronic device for managing an application related to a key of an external electronic device and an operating method of an electronic device.

BACKGROUND ART

[0002] Technology capable of performing authentication with an external electronic device through a smart key supporting wireless communication is being developed. For example, in the case where an external electronic device is a vehicle, development of technology related to a smart key capable of performing functions provided by a vehicle, such as unlocking a vehicle door, starting an engine of a vehicle, and the like is under way. The smart key is capable of performing an authentication procedure with a vehicle using short-range communication and activating functions of the vehicle, such as unlocking or starting thereof, after the authentication is completed.

[0003] Recently, technology has been introduced in order to perform functions provided by a vehicle using a portable terminal such as a smartphone, a wearable device, or the like, which can be held by a user, instead of using a separate smart key for activating the functions of the vehicle.

[0004] Recently, vehicle manufacturers have provided a vehicle key to a portable terminal so that the owner or sharers of a vehicle can perform various types of functions such as opening the vehicle door, igniting an engine of the vehicle, and the like using the portable terminal in the same manner as a normal smart key.

DISCLOSURE OF INVENTION

Technical Problem

[0005] A vehicle key or an application for managing the vehicle key may use a vehicle key solution based on a security module separately provided in a portable terminal in order to provide security.

[0006] There may be a situation in which a single user uses a plurality of vehicles or in which a plurality of users shares a vehicle. In this situation, it may not be easy for a user to use a single portable terminal as a key for each of a plurality of vehicles with security and convenience.

[0007] In particular, the vehicle has no information on the number of applications used in authentication for vehicles, which are provided in a portable terminal that establishes a communication connection with the vehicle. If all of a plurality of applications used for authentication of the vehicles attempt authentication, the time required for authentication may increase.

Solution to Problem

[0008] An electronic device according to various embodiments of the disclosure may include: a communication module configured to communicate with an external electronic device; and a security module configured to monitor a change in data related to applets for managing keys used

for authentication of the external electronic device, manage information related to the applet, and store an applet identification (AID) list including one or more AIDs and the applets, wherein the security module may be configured to: receive, from the external electronic device, a signal making a request for transmitting the AID (application identifier) list; in response to reception of the request signal, transmit the AID list to the external electronic device through the communication module; receive, from the external electronic device, a signal requesting information related to an applet associated with at least one AID selected from among the AIDs included in the AID list by the external electronic device; and transmit the information related to the applet corresponding to the selected AID to the external electronic device.

[0009] An electronic device according to various embodiments of the disclosure may include: a memory; a security module configured to store data fused for authentication with an external electronic device; a communication module; and a processor, wherein the security module may be configured to broadcast a connection request signal or a connection with the external electronic device, establish a communication channel with the external electronic device that responds to the broadcast signal, transmit a signal making a request for transmitting an application identifier (AID) list including one or more AIDs stored in the external electronic device, select at least one AID from among the AIDs included in the AID list transmitted by the external electronic device, request information indicating an applet corresponding to the selected AID and information related to the applet corresponding to the selected AID, and perform authentication with the external electronic device using the information related to the applet received from the external electronic device.

[0010] An operating method of an electronic device according to various embodiments of the disclosure may include: broadcasting a connection request signal for a connection with an external electronic device and establishing a communication channel with the external electronic device that responds to the broadcast signal; transmitting a signal making a request for transmitting an application identifier (AID) list including one or more AIDs stored in the external electronic device; selecting at least one AID from among the AIDs included in the AID list transmitted by the external electronic device; requesting information indicating an applet corresponding to the selected AID and information related to the applet corresponding to the selected AID; and performing authentication with the external electronic device using the information related to the applet received from the external electronic device.

Advantageous Effects of Invention

[0011] In the electronic device and the operating method of the electronic device according to various embodiments of the disclosure, an external electronic device performs authentication for a selected applet identification, instead of performing authentication for all of the applets stored in the electronic device, thereby reducing the time required for authentication.

BRIEF DESCRIPTION OF DRAWINGS

[0012] FIG. 1 is a block diagram of an electronic device according to various embodiments of the disclosure.

[0013] FIG. 2 is a block diagram of a program operating in an electronic device according to various embodiments of the disclosure.

[0014] FIG. 3 is a block diagram of an electronic device according to various embodiments of the disclosure.

[0015] FIG. 4 is a block diagram illustrating a security module in an electronic device according to various embodiments of the disclosure.

[0016] FIG. 5 is a block diagram of an electronic device according to various embodiments of the disclosure.

[0017] FIG. 6 is an operational flowchart of an operating method of an electronic device according to various embodiments of the disclosure.

[0018] FIG. 7 is an operational flowchart illustrating an operation of installing an applet used for authentication of an electronic device in a security module in an operating method of an electronic device according to various embodiments of the disclosure.

[0019] FIG. 8A is an operational flowchart illustrating an operation of activating an applet used for authentication of an electronic device in an operating method of an electronic device according to various embodiments of the disclosure.

[0020] FIG. 8B is an operational flowchart illustrating an operation of configuring priority of applet used for authentication of an electronic device in an operating method of an electronic device according to various embodiments of the disclosure.

[0021] FIG. 9 is an operational flowchart illustrating an operation of performing authentication of an electronic device in an external electronic device shown in FIG. 3 in an operating method of an electronic device according to various embodiments of the disclosure.

[0022] FIG. 10 is a diagram illustrating a specific example of data related to an applet transmitted by an electronic device according to various embodiments of the disclosure.

MODE FOR THE INVENTION

[0023] FIG. 1 is a block diagram illustrating an electronic device 101 in a network environment 100 according to various embodiments. Referring to FIG. 1, the electronic device 101 in the network environment 100 may communicate with an electronic device 102 via a first network 198 (e.g., a short-range wireless communication network), or an electronic device 104 or a server 108 via a second network 199 (e.g., a long-range wireless communication network). According to an embodiment, the electronic device 101 may communicate with the electronic device 104 via the server 108. According to an embodiment, the electronic device 101 may include a processor 120, memory 130, an input device 150, a sound output device 155, a display device 160, an audio module 170, a sensor module 176, an interface 177, a haptic module 179, a camera module 180, a power management module 188, a battery 189, a communication module 190, a subscriber identification module (SIM) 196, or an antenna module 197. In some embodiments, some of the components may be omitted from the electronic device 101, or one or more other components may be added in the electronic device 101. In some embodiments, some of the components may be implemented as single integrated circuitry. For example, the sensor module 176 (e.g., a fingerprint sensor, an iris sensor, or an illuminance sensor) may be implemented as embedded in the display device 160 (e.g., a display).

[0024] The processor 120 may execute, for example, software (e.g., a program 140) to control at least one other component (e.g., a hardware or software component) of the electronic device 101 coupled with the processor 120, and may perform various data processing or computation. According to one embodiment, as at least part of the data processing or computation, the processor 120 may load a command or data received from another component (e.g., the sensor module 176 or the communication module 190) in volatile memory 132, process the command or the data stored in the volatile memory 132, and store resulting data in non-volatile memory 134. According to an embodiment, the processor 120 may include a main processor 121 (e.g., a central processing unit (CPU) or an application processor (AP)), and an auxiliary processor 123 (e.g., a graphics processing unit (GPU), an image signal processor (ISP), a sensor hub processor, or a communication processor (CP)) that is operable independently from, or in conjunction with, the main processor 121. Additionally or alternatively, the auxiliary processor 123 may be adapted to consume less power than the main processor 121, or to be specific to a specified function. The auxiliary processor 123 may be implemented as separate from, or as part of the main processor 121.

[0025] The auxiliary processor 123 may control at least some of functions or states related to at least one component (e.g., the display device 160, the sensor module 176, or the communication module 190) among the components of the electronic device 101, instead of the main processor 121 while the main processor 121 is in an inactive (e.g., sleep) state, or together with the main processor 121 while the main processor 121 is in an active state (e.g., executing an application). According to an embodiment, the auxiliary processor 123 (e.g., an image signal processor or a communication processor) may be implemented as part of another component (e.g., the camera module 180 or the communication module 190) functionally related to the auxiliary processor 123.

[0026] The memory 130 may store various data used by at least one component (e.g., the processor 120 or the sensor module 176) of the electronic device 101. The various data may include, for example, software (e.g., the program 140) and input data or output data for a command related thereto. The memory 130 may include the volatile memory 132 or the non-volatile memory 134.

[0027] The program 140 may be stored in the memory 130 as software, and may include, for example, an operating system (OS) 142, middleware 144, or an application 146.

[0028] The input device 150 may receive a command or data to be used by other component (e.g., the processor 120) of the electronic device 101 from the outside (e.g., a user) of the electronic device 101. The input device 150 may include, for example, a microphone, a mouse, or a keyboard.

[0029] The sound output device 155 may output sound signals to the outside of the electronic device 101. The sound output device 155 may include, to example, a speaker or a receiver. The speaker may be used for general purposes, such as playing multimedia or playing record, and the receiver may be used for an incoming calls. According to an embodiment, the receiver may be implemented as separate from, or as part of the speaker.

[0030] The display device 160 may visually provide information to the outside (e.g., a user) of the electronic device 101. The display device 160 may include, for example, as

display, a hologram device, or a projector and control circuitry to control a corresponding one of the display, hologram device, and projector. According to an embodiment, the display device 160 may include touch circuitry adapted to detect a touch, or sensor circuitry (e.g., a pressure sensor) adapted to measure the intensity of force incurred by the touch.

[0031] The audio module 170 may convert a sound into an electrical signal and vice versa. According to an embodiment, the audio module 170 may obtain the sound via the input device 150, or output the sound via the sound output device 155 or a headphone of an external electronic device (e.g., an electronic device 102) directly (e.g., wiredly) or wirelessly coupled with the electronic device 101.

[0032] The sensor module 176 may detect an operational state (e.g., power or temperature) of the electronic device 101 or an environmental state (e.g., a state of user) external to the electronic device 101, and then generate an electrical signal or data value corresponding to the detected state. According to an embodiment, the sensor module 176 may include, for example, a gesture sensor, a gyro sensor, an atmospheric pressure sensor, a magnetic sensor, an acceleration sensor, a grip sensor, a proximity sensor, a color sensor, an infrared (IR) sensor, a biometric sensor, a temperature sensor, a humidity sensor, or an illuminance sensor.

[0033] The interface 177 may support one or more specified protocols to be used for the electronic device 101 to be coupled with the external electronic device (e.g., the electronic device 102) directly (e.g., wiredly) or wirelessly. According to an embodiment, the interface 177 may include, for example, a high definition multimedia interface (HDMI), a universal serial bus (USB) interface, a secure digital (SD) card interface, or an audio interface.

[0034] A connecting terminal 178 may include a connector via which the electronic device 101 may be physically connected with the external electronic device (e.g., the electronic device 102). According to an embodiment, the connecting terminal 178 may include, for example, a HDMI connector, a USB connector, a SD card connector, or an audio connector (e.g., a headphone connector).

[0035] The haptic module 179 may convert an electrical signal into a mechanical stimulus (e.g., a vibration or a movement) or electrical stimulus which may be recognized by a user via his tactile sensation or kinesthetic sensation. According to an embodiment, the haptic module 179 may include, for example, a motor, a piezoelectric element, or an electric stimulator.

[0036] The camera module 180 may capture a still image or moving images. According to an embodiment, the camera module 180 may include one or more lenses, image sensors, image signal processors, or flashes.

[0037] The power management module 188 may manage power supplied to the electronic device 101. According to one embodiment, the power management module 188 may be implemented as at least part of, for example, a power management integrated circuit (PMIC).

[0038] The battery 189 may supply power to at least one component of the electronic device 101. According to an embodiment, the battery 189 may include, for example, a primary cell which is not rechargeable, a secondary cell which is rechargeable, or a fuel cell.

[0039] The communication module 190 may support establishing a direct (e.g., wired) communication channel or a wireless communication channel between the electronic

device 101 and the external electronic device (e.g., the electronic device 102, the electronic device 104, or the server 108) and performing communication via the established communication channel. The communication module 190 may include one or more communication processors that are operable independently from the processor 120 (e.g., the application processor (AP)) and supports a direct (e.g., wired) communication or a wireless communication. According to an embodiment, the communication module 190 may include a wireless communication module 192 (e.g., a cellular communication module, a short-range wireless communication module, or a global navigation satellite system (GNSS) communication module) or a wired communication module 194 (e.g., a local area network (LAN) communication module or a power line communication (PLS) module). A corresponding one of these communication modules may communicate with the external electronic device via the first network 198 (e.g., a short-range communication network, such as Bluetooth™, wireless-fidelity (Wi-Fi) direct, or infrared data association (IrDA)) or the second network 199 (e.g., a long-range communication network, such as a cellular network, the Internet, or a computer network (e.g., LAN or wide area network (WAN))). These various types of communication modules may be implemented as a single component (e.g., a single chip), or may be implemented as multi components (e.g., multi chips) separate from each other. The wireless communication module 192 may identify and authenticate the electronic device 101 in a communication network, such as the first network 198 or the second network 199, using subscriber information (e.g., international mobile subscriber identity (IMSI)) stored in the subscriber identification module 196.

[0040] The antenna module 197 may transmit or receive a signal or power to or from the outside (e.g., the external electronic device) of the electronic device 101. According to an embodiment, the antenna module 197 may include one or more antennas, and, therefrom, at least one antenna appropriate for a communication scheme used in the communication network, such as the first network 198 or the second network 199, may be selected, for example, by the communication module 190 (e.g., the wireless communication module 192). The signal or the power may then be transmitted or received between the communication module 190 and the external electronic device via the selected at least one antenna.

[0041] At least some of the above-described components may be coupled mutually and communicate signals (e.g., commands or data) therebetween via an inter-peripheral communication scheme (e.g., a bus, general purpose input and output (GPIO), serial peripheral interface (SPI), or mobile industry processor interface (MIPI)).

[0042] According to an embodiment, commands or data may be transmitted or received between the electronic device 101 and the external electronic device 104 via the server 108 coupled with the second network 199. Each of the electronic devices 102 and 104 may be a device of a same type as, or a different type, from the electronic device 101. According to an embodiment, all or some of operations to be executed at the electronic device 101 may be executed at one or more of the external electronic devices 102, 104, or 108. For example, if the electronic device 101 should perform a function or a service automatically, or in response to a request from a user or another device, the electronic device 101, instead of, or in addition to, executing the function or

the service, may request the one or more external electronic devices to perform at least part of the function or the service. The one or more external electronic devices receiving the request may perform the at least part of the function or the service requested, or an additional function or an additional service related to the request, and transfer an outcome of the performing to the electronic device 101. The electronic device 101 may provide the outcome, with or without further processing of the outcome, as at least part of a reply to the request. To that end, a cloud computing, distributed computing, or client-server computing technology may be used, for example.

[0043] [text missing or illegible when filed]

[0044] FIG. 2 is a block diagram 200 illustrating the program 140 according to various embodiments. According to an embodiment, the program 140 may include an operating system (OS) 142 to control one or more resources of the electronic device 101, middleware 144, or an application 146 executable in the OS 142. The OS 142 may include, for example, Android™, iOS™, Windows™, Symbian™, Tizen™, or Bada™. At least part of the program 140, for example, may be pre-loaded on the electronic device 101 during manufacture, or may be downloaded from or updated by an external electronic device (e.g., the electronic device 102 or 104, or the server 108) during use by a user.

[0045] The OS 142 may control management (e.g., allocating or deallocation) of one or more system resources (e.g., process, memory, or power source) of the electronic device 101. The OS 142, additionally or alternatively, may include one or more driver programs to drive other hardware devices of the electronic device 101, for example, the input device 150, the sound output device 155, the display device 160, the audio module 170, the sensor module 176, the interface 177, the haptic module 179, the camera module 180, the power management module 188, the battery 189, the communication module 190, the subscriber identification module 196, or the antenna module 197.

[0046] The middleware 144 may provide various functions to the application 146 such that a function or information provided from one or more resources of the electronic device 101 may be used by the application 146. The middleware 144 may include, for example, an application manager 201, a window manager 203, a multimedia manager 205, a resource manager 207, a power manager 209, a database manager 211, a package manager 213, a connectivity manager 215, a notification manager 217, a location manager 219, a graphic manager 221, a security manager 223, a telephony manager 225, or a voice recognition manager 227.

[0047] The application manager 201, for example, may manage the life cycle of the application 146. The window manager 203, for example, may manage one or more graphical user interface (GUI) resources that are used on a screen. The multimedia manager 205, for example, may identify one or more formats to be used to play media files, and may encode or decode a corresponding one of the media files using a codec appropriate for a corresponding format selected from the one or more formats. The resource manager 207, for example, may manage the source code of the application 146 or a memory space of the memory 130. The power manager 209, for example, may manage the capacity, temperature, or power of the battery 189, and determine or provide related information to be used for the operation of the electronic device 101 based at least in part on corre-

sponding information of the capacity, temperature, or power of the battery 189. According to an embodiment, the power manager 209 may interwork with a basic input/output system (BIOS) (not shown) of the electronic device 101.

[0048] The database manager 211, for example, may generate, search, or change a database to be used by the application 146. The package manager 213, for example, may manage installation or update of an application that is distributed in the form of a package file. The connectivity manager 215, for example, may manage a wireless connection or a direct connection between the electronic device 101 and the external electronic device. The notification manager 217, for example, may provide a function to notify a user of an occurrence of a specified event (e.g., an incoming call, message, or alert). The location manager 219, for example, may manage locational information on the electronic device 101. The graphic manager 221, for example, may manage one or more graphic effects to be offered to a user or a user interface related to the one or more graphic effects.

[0049] The security manager 223, for example, may provide system security or user authentication. The telephony manager 225, for example, may manage a voice call function or a video call function provided by the electronic device 101. The voice recognition manager 227, for example, may transmit a user's voice data to the server 108, and receive, from the server 108, a command corresponding to a function to be executed on the electronic device 101 based at least in part on the voice data, or text data converted based at least in part on the voice data. According to an embodiment, the middleware 244 may dynamically delete some existing components or add new components. According to an embodiment, at least part of the middleware 144 may be included as part of the OS 142 or may be implemented as another software separate from the OS 142.

[0050] The application 146 may include, for example, a home 251, dialer 253, short message service (SMS)/multimedia messaging service (MMS) 255, instant message (IM) 257, browser 259, camera 261, alarm 263, contact 265, voice recognition 267, email 269, calendar 271, media player 273, album 275, watch 277, health 279 (e.g., for measuring the degree of workout or biometric information, such as blood sugar), or environmental information 281 (e.g., for measuring air pressure, humidity, or temperature information) application. According to an embodiment, the application 146 may further include an exchanging application (shown) that is capable of supporting information exchange between the electronic device 101 and the external electronic device. The information exchange application, for example, may include a notification relay application adapted to transfer designated information (e.g., a call, message, or alert) to the external electronic device or a device management application adapted to manage the external electronic device. The notification relay application may transfer notification information corresponding to an occurrence of a specified event (e.g., receipt of an email) at another application (e.g., the email application 269) of the electronic device 101 in the external electronic device. Additionally or alternatively, the notification relay application may receive notification information from the external electronic device and provide the notification information to a user of the electronic device 101.

[0051] The device management application may control the power (e.g., turn-on or turn-off) or the function (e.g., adjustment of brightness, resolution, or focus) of the exter-

nal electronic device or some component thereof (e.g., a display device or a camera module of the external electronic device). The device management application, additionally or alternatively, may support installation, delete, or update of an application running on the external electronic device.

[0052] [text missing or illegible when filed]

[0053] FIG. 3 is a block diagram of an electronic device according to various embodiments of the disclosure.

[0054] Referring to FIG. 3, an electronic device 300 (e.g., the electronic device 101 in FIG. 1) according to various embodiments of the disclosure may include a processor 310 (e.g., the processor 120 in FIG. 1), a communication module 320 (e.g., the communication module 190 in FIG. 1), a security module 330, a memory 340 (e.g., the memory 130 in FIG. 1), and a display 350 (e.g., the display device 160 in FIG. 1).

[0055] According to various embodiments of the disclosure, the processor 310 may control the security module 330 so as to change configuration of an applet installed in the security module 330. For example, the processor 310 may display a screen for the user of the electronic device 300 to change the configuration of an applet on the display 350, and may transmit, to the security module 330, a signal requesting changing the configuration of the applet, based on a user input.

[0056] According to various embodiments of the disclosure, the applet installed in the security module 330 may refer to an applet for performing authentication of the electronic device 300 in order to use various functions provided by an external electronic device (e.g., an electronic device 500 in FIG. 5). For example, the applet may denote a key required to use the external electronic device 500. In the case where the external electronic device 500 is a vehicle, the applet installed in the security module 330 may be an applet that manages a key used for authentication of the vehicle. The applet installed in the security module 330 may be provided by the manufacturer of the external electronic device 500.

[0057] According to various embodiments of the disclosure, authentication of the electronic device 300 may denote a procedure of verifying whether or not the electronic device 300 has a valid authority to perform various functions provided by the external electronic device 500. According to various embodiments of the disclosure, the external electronic device 500 may denote a vehicle or any of various electronic devices electrically connected to control the vehicle. The external electronic device 500 will be described in detail below with reference to FIG. 5.

[0058] According to various embodiments of the disclosure, the communication module 320 may establish a communication channel with the external electronic device 500, and may transmit and receive a variety of data to and from the external electronic device 500. The communication module 320 may transmit and receive a variety of data to and from the external electronic device 500 using short-range communication (e.g., Bluetooth, NFC, UWB, etc.), but is not limited thereto, and may transmit and receive a variety of data to and from the external electronic device 500 using a cellular network (e.g., LTE, 5G network, etc.).

[0059] According to various embodiments of the disclosure, the memory 340 may store an application that configures a key of the external electronic device 500.

[0060] According to various embodiments of the disclosure, the security module 330 may be a module that is

physically separate from the processor 310 or the memory (e.g., the memory 130 in FIG. 1), and may encrypt and store data that is stored in the security module 330. According to another embodiment of the disclosure, the security module 330 may be included in an area of the memory 340, and the security module 330 may refer to a portion in which data stored in the memory 340 is encrypted and stored.

[0061] According to various embodiments of the disclosure, in response to reception of a request for accessing data in the security module 330, the security module 330 may verify the access authority of an entity (e.g., various applications installed in the memory 130 or the like) that requests access to the data or integrity thereof, and may permit access to/editing of the data stored in the security module 330, or may transmit the stored data according to the result of the verification.

[0062] According to various embodiments of the disclosure, the security module 330 may include a contactless register service (CRS) for managing an applet used by the external electronic device 500 to perform authentication. The CRS (not shown) may perform modification, addition, or deletion of data assigned to an applet, based on a user request.

[0063] According to various embodiments of the disclosure, the security module 330 may include a proximity vehicle key system environment (PVKSE). The PVKSE (not shown) may monitor operations such as modification, addition, or deletion of data assigned to an applet, and if a change in the data related to the applet is detected, may produce information related to the applet, or may change the produced information related to the applet. The PVKSE may refer to an element implemented in software to be separate from the contactless registry service (CRS) for managing data stored in the security module 330.

[0064] According to various embodiments of the disclosure, the security module 330 may produce an applet identification (application identification) (AID) list that includes AIDs of the respective applets stored in the security module 330. The AID list may be produced and managed by the PVKSE. The security module 330 may transmit the AID list to the external electronic device 500 in response to a request from the external electronic device 500.

[0065] According to various embodiments of the disclosure, the external electronic device 500 may select at least one AID to perform authentication from among the AIDs included in the AID list, and may transmit, to the electronic device 300, information indicating the selected AID and a signal requesting information related to the applet corresponding to the selected AID.

[0066] According various embodiments of the disclosure, the signal transmitted by the external electronic device 500 may use a message structure including a command header and a command body defined in Table 60 of ISO 7816-4 (refer to Table 1).

TABLE 1

	Code	Value
Command head	CLA	00
	(defined in 5.4.1 of 7816.4)	
	INS	A4
	P1	04
	(defined in Table 62 of ISO 7816.4)	
	P2	00

TABLE 1-continued

Code		Value
Command body	Lc (Length of command data field)	Od
	Data (2VK.SYS.DDF01)	32564B2E5359532E4444463031
	Lc	00

[0067] According to various embodiments of the disclosure, in response to reception of information indicating the selected AID and information related to the applet corresponding to the selected AID transmitted by the external electronic device 500, the security module 330 may transmit information related to the applet corresponding to the selected AID to the external electronic device 500.

[0068] According to various embodiments of the disclosure, information related to the applet transmitted to the external electronic device 500 by the security module 330 may use a template for file control information (FCI) defined in ISO 7816-4.

TABLE 2

TAG	Values	Y
'6F'	FCI Template (indicating template for file control information)	Y
'84'	'2VK.SYS.DDF01'	Y
'A5'	FCI Proprietary Template	Y
	'BFOC' FCI Issue Discretionary Data (indicating issued discretionary data of security module 330)	Y
	'61' Directory Entry (indicating stored address of applet)	Y
	'4F' DF Name (AID) (indicating applet identification)	Y
	'50' Application label (applet labeling)	N
	'87' Priority indicator (highest) (indicating priority)	N
	'9F30' Application-specific data (specific data)	N
	'61' Directory Entry	N
	'4F' DF Name (AID)	N
	'50' Application label	N
	'87' Priority indicator (lowest)	N
	'9F30' Application-specific data	N

[0069] [text missing or illegible when filed]

[0070] Referring to Table 2, information related to the applet may be implemented in the form of data and a tag indicating the data. In addition, an item indicating the length of data may be added between the tag and data. In the case where a plurality of AIDs is selected by the external electronic device 500, the information related to the applet may include all information related to the applets corresponding to the respective AIDs. If there is a plurality of AIDs, information related to the applets corresponding to the respective AIDs may be transmitted in order of priority. The priority may be configured by the user of the electronic device 300. In addition, the priority may be changed depending on the frequency of use of the external electronic device

500. For example, the higher the frequency of use of the external electronic device 500, the higher the priority may be configured.

[0071] According to various embodiments of the disclosure, the information related to the applet may include an applet identification 4F indicating the identifier of a manufacturer of the external electronic device, an applet label 50 indicating the model of the external electronic device, priority information 87 indicating the priority of the applet, or application-specific data 9F30.

[0072] According to various embodiments of the disclosure, among the information related to the applet, information 6F indicating a template for file control information, a data field 84, a file control information (FCI) proprietary template A5, a portion BFOC indicating issued discretionary data of the security module 330, a portion 61 indicating a stored address of the applet, or an application identification 50 may correspond to an essential element of the information related to the applet. An applet label 50 indicating the model of the external electronic device, priority information 87 indicating the priority of the applet, or application-specific data 9F30 may correspond to an additional element of the information related to the applet.

[0073] According to various embodiments of the disclosure, the information related to the applet may include data indicating the state of the applet at the end of the application-specific data 9F30.

[0074] According to various embodiments of the disclosure, the applet identification 4F may refer to an identifier capable of distinguishing between the applets. For example, the applet identification may denote an identifier of the manufacturer of the external electronic device 500. The identifier of the manufacturer of the external electronic device may be different between respective manufacturers. The external electronic device 500 may identify the applet identification 4F, and may select an AID corresponding to the same manufacturer as the manufacturer of the external electronic device 500.

[0075] According to various embodiments of the disclosure, the applet label 50 may refer to an identifier of a model of the external electronic device or an identifier of the manufacturer of the external electronic device. Even if the external electronic device is manufactured by the same manufacturer, the applet label 50 may be different depending on the model thereof (a mid-sized car or a full-sized car).

[0076] According to various embodiments of the disclosure, the priority information 87 may refer to information on the priority related to the order in which the external electronic device 500 performs authentication. The priority information 87 may be implemented as a number, and the smaller the number, the higher the priority it may have.

[0077] According to various embodiments of the disclosure, the application-specific data 9F30 is an area in which a variety of data on the applet may be included, and a variety of data required for authentication between the external electronic device 500 and the electronic device 300 may be included therein. The application-specific data 9F30 may include an available usage time of the external electronic device 500 (e.g., the time during which driving of the external electronic device 500 is allowed), geofencing limitation data of the external electronic device 500 (e.g., a geographic range in which driving of the external electronic device 500 is allowed), the maximum permissible speed of the external electronic device 500, data indicating whether

or not various devices included in the external electronic device 500 (e.g., a trunk, a console box, and the like) or various functions available for the external electronic device 500 (e.g., lane maintenance assistance, lane departure notification, cruise control, adaptive cruise control, or engine availability) are allowed, and the like.

[0078] According to various embodiments of the disclosure, referring to Table 3, data indicating the state of the applet may indicate one of three states (the state indicating the occurrence of an error in a message requesting information related to the applet, the state indicating that there is no applet, and the state indicating the success of transmission of information related to the applet) in a rough way.

TABLE 3

Field	Length	Value		
Status Word	2	Value	Type	Meaning
		'6A86'	Error	Incorrect P1/P2
		'6A82'	Error	Application not found
		'9000'	Normal	Successful Processing

[0079] [text missing or illegible when filed]

[0080] The signal, produced with reference to Table 1, through which the external electronic device 500 makes a request to the electronic device 300 for the AID list, may be implemented as, for example, '00A404000D32564B2E5359532E444446303100'. The data related to the applet transmitted from the electronic device 300 to the external electronic device 500 may be implemented according to the above description, and a specific example thereof will be shown in FIG. 10.

[0081] Referring to FIG. 10, the data related to the applet may be implemented as shown in Table 4 using the format defined in Table 2. Table 4 is a specific example of data related to the applet implemented using the format defined in Table 2, and provides a detailed description of the data related to the applet shown in FIG. 10.

TABLE 4

Tag	Description	Example
'6F'	FCI Template (indicating template for file control information)	6F
'84'	'2VK.SYS.DDF01'	32564B2E5 359532E444 4463031
'A5'	FCI Proprietary Template	A5
'BF0C'	FCI Issue Discretionary Data (indicating issued discretionary data of security module 330)	BF0C
'61'	Directory Entry (indicating stored address of applet)	61
'4F'	DF Name (AID) (indicating applet identification)	D286000159 01140001
'50'	Application label (applet labeling)	424D57205835
'87'	Priority indicator (highest)	01
	(indicating priority)	
'9F30'	Application-specific data (specific data)	—

[0082] [text missing or illegible when filed]

[0083] According to various embodiments of the disclosure, the external electronic device 500 may perform authentication for the electronic device 300 using data related to the applet transmitted from the electronic device 300. In response to the completion of authentication of the electronic device 300, the external electronic device 500 may provide functions that can be performed by the external electronic device 500 within an authenticated range. For example, in response to the completion of authentication of the electronic device 300, the external electronic device 500 may release the door lock of the external electronic device 500, and may release the on/off control lock for start-up of the external electronic device 500.

[0084] According to various embodiments of the disclosure, information related to the applet used in authentication of the external electronic device 500 may be stored in the security module 330 of the electronic device 300. The security module 330 may provide a separate security solution so that information related to security-sensitive applets may be safely stored, and may be safely used. A detailed example in which the information related to the applet is stored in the security module 330 will be described below with reference to FIG. 4.

[0085] [text missing or illegible when filed]

[0086] FIG. 4 is a block diagram illustrating a security module in an electronic device according to various embodiments of the disclosure.

[0087] Referring to FIG. 4, the security module 330 of the electronic device 300 according to various embodiments of the disclosure may be divided into an issued security domain (ISD) 481 and a supplementary security domain (SSD) 482.

[0088] According to various embodiments of the disclosure, a PVKSE 410 and a CRS 420 may be provided in the ISD 481. The PVKSE 410 may refer to a software element capable of managing at least one applet 430, 440, 450, 460, or 470 installed in the SSD 482. The security module 330 according to various embodiments of the disclosure may include the CRS 420 that manages at least one applet 430,

440, 450, 460, or 470, and may manage at least one applet 430, 440, 450, 460, or 470 under the control of the CRS 420.

[0089] According to various embodiments of the disclosure, the CRS 420 may denote a software element that manages files installed in the security module 330. The CRS 420 may manage a variety of data stored in the security module 330 (e.g., encryption of data or decryption of encrypted data), based on a request by a processor (e.g., the processor 310 in FIG. 3), and may transfer the data stored in the security module 330 to a memory (e.g., the memory 130 in FIG. 1).

[0090] In order to perform authentication of the electronic device 300, the external electronic device 500 may make a request to the electronic device 300 for transmitting an AID list stored in the security module 330. For example, the transmission of the AID list stored in the security module 330 may be performed using an instruction defined as SELECT PVKSE. The PVKSE 410 may produce and transmit an AID list in response to reception of the instruction defined as SELECT PVKSE.

[0091] According to various embodiments of the disclosure, the PVKSE 410 may monitor changes in a variety of data on the applet, and if a change in the data is detected, may produce or change information related to the applet reflecting the change in the data. In response to a request from the external electronic device 500, the PVKSE 410 may transmit information related to the applet corresponding to at least one AID selected by the external electronic device 500.

[0092] According to various embodiments of the disclosure, the external electronic device 500 may transmit, to the security module 330, information indicating the selected AID using an instruction defined as SELECT AID. For example, in response to the reception of the instruction defined as SELECT AID, the PVKSE 410 of the security module 330 may transmit information related to the applet corresponding to the at least one AID selected by the external electronic device 500.

[0093] According to various embodiments of the disclosure, each of the one or more applets 430, 440, 450, 460, and 470 may be stored in the SSD 482. The SSD 482 may be divided into spaces according to manufacturers of the external electronic device 500, and the applets corresponding to respective manufacturers may be stored in the corresponding spaces of the SSD 482 divided for the respective manufacturers. For example, the applets 450 and 460 corresponding to manufacturer 1 may be stored in an SSD space 484 corresponding to manufacturer 1, and the applet 470 corresponding to manufacturer 2 may be stored in an SSD space 485 corresponding to manufacturer 2. The SSD 482 may further include an SSD space 483 for separately storing the applets 430 and 440 for sharing keys available for the external electronic device shared by various users (e.g., a vehicle that is a target to be shared as car sharing).

[0094] According to various embodiments of the disclosure, each of the one or more applets 430, 440, 450, 460, and 470 may include data 430-a, 440-a, 450-a, 460-a, or 470-a indicating whether or not the applet is activated. The activated applet (e.g., 430, 440, 460, or 470) may denote an applet capable of performing authentication of the electronic device 300 with the external electronic device 500, and the deactivated applet (e.g., 450) may denote an applet that is unable to perform authentication of the electronic device 300 with the external electronic device 500. Activation or deactivation of the applet may be determined by an input

from the user of the electronic device 300, and a detailed description of performing the activation of the applet will be described later with reference to FIG. 8A.

[0095] According to various embodiments of the disclosure, each of the one or more applets 430, 440, 450, 460, and 470 may include data 430-b, 440-b, 450-b, 460-b, or 470-b indicating the priority of the applet. The priority may be configured by the user of the electronic device 300. In addition, the priority may be changed depending on the frequency of use of the external electronic device 500. For example, the higher the frequency of use of the external electronic device 500, the higher the priority may be configured. A detailed description of configuration of the priority of the applet will be described later with reference to FIG. 8B.

[0096] According to various embodiments of the disclosure, each of the one or more applets 430, 440, 450, 460, and 470 may include information related to the applet, and the information related to the applet may include an applet identification 4F indicating an identifier of the manufacturer of the external electronic device, an applet label 50 indicating the model of the external electronic device, priority information 87 indicating the priority of the applet, and application-specific data 9F30. The information related to the applet may include data indicating the state of the applet at the end of the application-specific data 9F30.

[0097] [text missing or illegible when filed]

[0098] FIG. 5 is a block diagram of an electronic device according to various embodiments of the disclosure.

[0099] Referring to FIG. 5, an electronic device 500 (e.g., the electronic device 102 or the electronic device 104 in FIG. 1) according to various embodiments of the disclosure may include a processor 510, a communication module 520, and a security module 530. The electronic device 500 illustrated in FIG. 5 may be the external electronic device described with reference to FIG. 3. The electronic device 500 may denote a vehicle or any of various electronic devices electrically connected to control the vehicle. It is possible to perform at least some of the various functions that can be performed by the electronic device 500 (e.g., a function of releasing the door lock of the electronic device 500 and a function of starting an engine of the electronic device 500) through authentication of the electronic device 500 shown in FIG. 5 with an external electronic device (e.g., the electronic device 300 illustrated in FIG. 3).

[0100] According to various embodiments of the disclosure, the communication module 520 may establish a communication channel with the external electronic device 300, and may transmit and receive a variety of data to and from the external electronic device 300. The communication module 520 may transmit and receive a variety of data to and from the external electronic device 300 using short-range communication (e.g., Bluetooth, NFC, UWB, etc.), but is not limited thereto, and may transmit and receive a variety of data to and from the external electronic device 300 using a cellular network (e.g., LTE, 5G network, etc.).

[0101] According to various embodiments of the disclosure, the security module 530 may be a module that is physically separate from the processor 510 or the memory (e.g., the memory 130 in FIG. 1), and may encrypt and store data that is stored in the security module 530. According to another embodiment of the disclosure, the security module 530 may be included in an area of the memory 130, and the

security module 530 may refer to a portion in which data stored in the memory 130 is encrypted and stored.

[0102] According to various embodiments of the disclosure, in response to reception of a request for accessing data in the security module 530, the security module 530 may verify the access authority of an entity (e.g., various applets installed in the memory 130) that requests access to the data and integrity thereof, and may permit access to/editing of the data stored in the security module 330, or may transmit the stored data according to the result of the verification. The security module 530 may store a variety of data transmitted from the external electronic device 300 (e.g., information related to the applet, applet list, and data required for authentication transmitted by the external electronic device 300 (public key)) or data required for authentication with the external electronic device 300 (a secret key).

[0103] According to various embodiments of the disclosure, the processor 510 may control the communication module 520 so as to broadcast a connection request signal for a connection with the external electronic device 300. The processor 510 may establish a communication channel with the external electronic device 300 that responds to the broadcast connection request signal.

[0104] According to various embodiments of the disclosure, the processor 510 may receive, from the external electronic device 300, a request signal for activating at least some of the various functions that can be performed by the electronic device 500. For example, the external electronic device 300 may produce a signal making a request for performing some functions of the electronic device 500 (e.g., a function of releasing the door lock of the electronic device 500, a function of turning on the lights of the electronic device 500, or a function of automatically pulling out the electronic device 500), based on an input from the user of the external electronic device 300, and may transmit the produced signal to the electronic device 500. In response to reception of the signal making a request for performing some functions of the electronic device 500, the processor 510 may initiate authentication with the external electronic device 300. In the case where there is a plurality of applets installed in the external electronic device 300 (which may denote the applets for authentication with the electronic device 500), if authentication is performed on the respective applets, it may take a long time for authentication. According to various embodiments of the disclosure, the processor 510 may transmit, to the external electronic device 300, a signal making a request for transmitting an AID list before performing authentication, instead of performing authentication for all of the plurality of applets.

[0105] According to various embodiments of the disclosure, the signal requesting the AID list may be implemented as the message structure shown in Table 1.

[0106] According to various embodiments of the disclosure, the processor 510 may select at least one AID from among the AIDs included in the AID list transmitted from the external electronic device 300.

[0107] According to various embodiments of the disclosure, the processor 510 may select AIDs in a manner of selecting one or more AIDs remaining after filtering out applets having AIDs that are not supported by the electronic device 500 from among the AIDs included in the AID list.

[0108] According to another embodiment of the disclosure, the processor 510 may select AIDs in a manner of

selecting applets having the same AID as the manufacturer of the electronic device 500 from among the AIDs included in the AID list.

[0109] According to another embodiment of the disclosure, the processor 510 may select AIDs in a manner of selecting applets having the same AID as the manufacturer of the electronic device 500 from among the AIDs included in the AID list and selecting one or more AIDs remaining after filtering out the applets having AIDs that are not supported by the electronic device 500 from among the AIDs corresponding to a sharing key.

[0110] According to various embodiments of the disclosure, the processor 510 may transmit information indicating the selected AIDs to the external electronic device 300. For example, the processor 510 may produce a list of the selected AIDs, and may transmit the produced AID list to the external electronic device 300.

[0111] According to various embodiments of the disclosure, the processor 510 may transmit a signal requesting information related to the applet corresponding to at least one selected AID to the external electronic device 300. The information related to the applet may be implemented using a template for control information defined in ISO 7816-4, and is shown in Table 2. The information related to the applet may include an applet identification 4F indicating an identifier of the manufacturer of the external electronic device, an applet label 50 indicating the model of the external electronic device, priority information 87 indicating the priority of the applet, and application-specific data 9F30. The information related to the applet may include data indicating the state of the applet at the end of the application-specific data 9F30. The detailed description of the information related to the applet has been made with reference to FIG. 3.

[0112] According to various embodiments of the disclosure, the processor 510 may receive the information related to the applet from the external electronic device 300. The processor 510 may perform authentication with the external electronic device 300 using the information related to the applet.

[0113] According to various embodiments of the disclosure, the processor 510 may determine the applet pm which authentication is preferentially performed based on the priority information included in the information related to the applet. For example, if the processor 510 selects a plurality of AIDs, the processor 510 may priority information corresponding to each of the plurality of AIDs. The processor 510 may perform authentication with the external electronic device 300 using an applet having the highest priority. If the processor 510 fails to perform authentication while performing authentication with the external electronic device 300 using the applet having the highest priority, the processor 510 may perform authentication with the external electronic device 300 using an applet having the next highest priority.

[0114] The electronic device 500 according to various embodiments of the disclosure may receive an AID list, may select applets by which authentication is to be performed from the AID list, and may then perform authentication using the selected applets, instead of performing authentication for all of the applets stored in the external electronic device 300. If authentication with the external electronic device 300 having a plurality of applets is performed using the method described above, the time required for authentication may be reduced.

[0115] According to various embodiments of the disclosure, at least some of the functions performed by the processor 510 may also be performed by the security module 530.

[0116] In response to completion of authentication of the external electronic device 300, the electronic device 500 may provide functions that can be performed by the electronic device 500 within an authenticated range. For example, in response to completion of authentication of the external electronic device 300, the electronic device 500 may release the door lock of the electronic device 500, and may release the on/off control lock of startup of the electronic device 500.

[0117] [text missing or illegible when filed]

[0118] An electronic device according to various embodiments of the disclosure may include: a communication module (e.g., the communication module 320 in FIG. 3) configured to communicate with an external electronic device; and a security module (e.g., the security module 330 in FIG. 3) configured to monitor a change in data related to applets for managing keys used for authentication of the external electronic device, manage information related to the applet, and store an applet identification (AID) list including one or more AIDs and the applets, wherein the security module may be configured to receive, from the external electronic device (e.g., the electronic device 400 in FIG. 4), a signal making a requester transmitting the AID (application identifier) list, in response to reception of the request signal, transmit the AID list to the external electronic device 400 through the communication module 320, receive, from the external electronic device 400, a signal requesting information related to an applet associated with at least one AID selected from among the AIDs included in the AID list by the external electronic device 400, and transmit the information related to the applet corresponding to the selected AID to the external electronic device 400.

[0119] According to various embodiments of the disclosure, the information related to the applet may include at least one of an address in which the applet is stored, the AID, a model identifier of the external electronic device, data indicating whether or not to activate the applet, priority assigned to each of the applets, or application-specific data.

[0120] According to various embodiments of the disclosure, the application-specific data may include an available usage time of the external electronic device, geofencing limitation data of the external electronic device, or information indicating whether or not at least one of various functions that can be executed by the external electronic device is allowed.

[0121] According to various embodiments of the disclosure, the AID list may be sorted based on the priority assigned to each of the applets.

[0122] According to various embodiments of the disclosure, the security module 330 may further include: a CRS (e.g., the CRS 420 in FIG. 4) configured to manage data stored in the security module; and a proximity vehicle key system environment (PVKSE) (e.g., the PVKSE 410 in FIG. 4) configured to monitor a change in data related to the applet and manage information related to the applet, wherein the CRS 420, in response to a signal making a request for changing configuration of the applet, may change configuration of at least one applet and transmit a signal indicating the change in the data to the PVKSE 410, and wherein the

PVKSE 410, in response to reception of the signal indicating the change in the data, may change the data related to the applet.

[0123] According to various embodiments of the disclosure, the PVKSE 410 and the CRS 420 may be configured to be stored in an issued security domain (e.g., the ISD 481 in FIG. 4) of the security module, and the applet may be configured to be stored in a supplementary security domain (e.g., the SSD 482 in FIG. 4) thereof.

[0124] According to various embodiments of the disclosure, the information related to the applet may be configured to be stored in a supplementary secure domain separated for each applet.

[0125] According to various embodiments of the disclosure, the PVKSE 410 may be configured to change the information related to the applet if a change in the applet is detected.

[0126] [text missing or illegible when filed]

[0127] An electronic device according to various embodiments of the disclosure may include: a memory; a security module (e.g., the security module 530 in FIG. 5) configured to store data used for authentication with an external electronic device; a communication module (e.g., the communication module 520 in FIG. 5); and a processor (e.g., the processor 510 in FIG. 5), wherein the security module 530 may be configured to broadcast a connection request signal for a connection with the external electronic device (e.g., the electronic device 300 in FIG. 3); establish a communication channel with the external electronic device 300 that responds to the broadcast signal; transmit a signal making a request for transmitting an AID list including one or more AIDs (application identifiers) stored in the external electronic device 300; select at least one AID from among the AIDs included in the AID list transmitted by the external electronic device 300; transmit, to the external electronic device 300, information indicating an applet corresponding to the selected AID and a signal requesting information related to the applet and perform authentication with the external electronic device using the information related to the applet received from the external electronic device 300.

[0128] According to various embodiments of the disclosure, the security module 530 may be configured to perform authentication, based on the priority assigned to the applet.

[0129] According to various embodiments of the disclosure, the security module 530 may be configured to perform authentication for the external electronic device 300 using the information related to the applet, in response to identifying that the authentication has failed, select an AID having a lower priority than the AID on which the authentication has been performed, and request information related to an applet corresponding to the selected AID.

[0130] According to various embodiments of the disclosure, the security module 530 may be configured to select an AID corresponding to a manufacturer of the electronic device 400 from among the AIDs included in the AID list.

[0131] According to various embodiments of the disclosure, the security module 530 may be configured to select an AID having the highest priority from AIDs corresponding to manufacturer of the electronic device 400, among the AIDs included in the AID list.

[0132] According to various embodiments of the disclosure, the AID list may include at least one AID correspond-

ing to the external electronic device 300 and at least one AID corresponding to an external electronic device 300 shared by other users.

[0133] According to various embodiments of the disclosure, the information related to the applet may include at least one of an address in which the applet is stored, the AID, a model identifier of the electronic device 400, data indicating whether or not to activate the applet, priority assigned to each applet, or application-specific data.

[0134] According to various embodiments of the disclosure, the application-specific data may include an available usage time of the electronic device 400, geofencing limitation data of the electronic device 400, or information indicating whether or not at least one of various functions that can be executed by the electronic device 400 is allowed.

[0135] According to various embodiments of the disclosure, the security module 530 may be configured to determine a function to be activated among functions that can be provided by the electronic device 400, based on the application-specific data.

[0136] According to various embodiments of the disclosure, the electronic device 400 may be a vehicle, or may be electrically connected to a vehicle.

[0137] [text missing or illegible when filed]

[0138] FIG. 6 is an operational flowchart illustrating an operating method of an electronic device according to various embodiments of the disclosure.

[0139] Referring to FIG. 6, an operating method of an electronic device according to various embodiments of the disclosure may be performed between a first electronic device (e.g., the electronic device 300 in FIG. 3) and a second electronic device (e.g., the electronic device 500 in FIG. 5).

[0140] In operation 601, the second electronic device 500 may broadcast a discovery signal. In operation 603, the first electronic device 300 may receive the discovery signal, and may transmit information for establishing a communication channel to the second electronic device 500. In operation 605, the second electronic device 500 may establish a communication channel with the first electronic device 300 that responds to the discovery signal. According to various embodiments of the disclosure, the communication channel may refer to a channel implemented between the first electronic device 300 and the second electronic device 500 using a short-range communication method, but the communication channel may also be implemented using a cellular network communication method.

[0141] In operation 607, the second electronic device 500 may transmit, to the first electronic device 300, a signal making a request for transmitting an AID list for authentication with the first electronic device 300.

[0142] According to various embodiments of the disclosure, the second electronic device 500 may receive, from the first electronic device 300, a request signal for activating at least some of the various functions that can be performed by the second electronic device 500. In response to reception of the request signal for activating at least some of the functions, the second electronic device 500 may transmit, to the first electronic device 300, a signal making a request for transmitting an AID list.

[0143] In operation 609, the first electronic device 300 may transmit an AID list to the second electronic device 500 in response to the request for transmission of the AID list. The AID list may include a list of identifications of respec-

tive applets stored in the security module (e.g., the security module 330 in FIG. 3) of the first electronic device 300. The applet may include a variety of information for performing authentication between the first electronic device 300 and the second electronic device 500.

[0144] In operation 611, the second electronic device 500 may select at least one AID from the AIDs included in the AID list.

[0145] According to various embodiments of the disclosure, the second electronic device 500 may select AIDs in a manner of selecting one or more AIDs remaining after filtering out applets having AIDs that are not supported by the second electronic device 500 from among the AIDs included in the AID list.

[0146] According to an embodiment of the disclosure, the second electronic device 500 may select AIDs in a manner of selecting applets having the same AID as the manufacturer of the second electronic device 500 from among the AIDs included in the AID list.

[0147] According to an embodiment of the disclosure, the second electronic device 500 may select AIDs in a manner of selecting applets having the same AID as the manufacturer of the second electronic device 500 from among the AIDs included in the AID list and selecting one or more AIDs remaining after filtering out the applets having AIDs that are not supported by the second electronic device 500 from among the AIDs corresponding to a sharing key.

[0148] In operation 613, the second electronic device 500 may transmit, to the first electronic device 300, a list of the selected AIDs and a signal making a request for transmitting data related to the applets corresponding to the selected AIDs, respectively. In operation 615, the first electronic device 300 may transmit data related to the applets to the second electronic device 500.

[0149] According to various embodiments of the disclosure, the information related to the applet may be implemented using a template for file control information defined in ISO 7816-4, and is shown in Table 2. The information related to the applet may include an applet identification 4F indicating an identifier of the manufacturer of an external electronic device, an applet label 50 indicating the model of an external electronic device, priority information 87 indicating the priority of the applet, and application-specific data 9F30. The information related to the applet may include data indicating the state of the applet at the end of the application-specific data 9F30. The detailed description of the information related to the applet has been described with reference to FIG. 3.

[0150] In operation 617, the second electronic device 500 may perform an authentication procedure with the first electronic device 300 using the information related to the applets.

[0151] The second electronic device 500 according to various embodiments of the disclosure may receive an AID list, may select applets on which authentication is to be performed from the AID list, and may then perform authentication using the selected applets, instead of performing authentication for all of the applets stored in the first electronic device 300. In the case of performing authentication with the first electronic device 300 having a plurality of applets using the method described above, the time required for authentication may be reduced.

[0152] According to various embodiments of the disclosure, in response to completion of authentication of the first

electronic device 300, the second electronic device 500 may provide functions that can be performed by the second electronic device 500 within an authenticated range. For example, in response to completion of authentication of the first electronic device 300, the second electronic device 500 may release the door lock of the second electronic device 500, and may release the on/off control lock of start-up of the second electronic device 500.

[0153] [text missing or illegible when filed]

[0154] FIG. 7 is an operational flowchart illustrating an operation of installing an applet used for authentication of an electronic device in a security module in an operating method of an electronic device according to various embodiments of the disclosure.

[0155] The operation illustrated in FIG. 7 shows an operation of installing an applet for performing authentication with an external electronic device (e.g., the electronic device 500 in FIG. 5) and a PVKSE (e.g., the PVKSE 410 in FIG. 4) for managing the applet in a security module (e.g., the security module 330 in FIG. 3) of an electronic device (e.g., the electronic device 300 in FIG. 3).

[0156] In operation 710, a processor the processor 310 in FIG. 3) may install the PVKSE 410 in the security module 330. According to various embodiments of the disclosure, the PVKSE 410 may be installed in the ISD 481 of the security module 330. As the applet for configuring a key of the external electronic device 500 is installed in the memory (e.g., the memory 130 in FIG. 1), the PVKSE 410 may be installed in the ISD 481 when the key of the external electronic device 500 is installed in the SSD 482 of the security module 330.

[0157] According to various embodiments of the disclosure, the PVKSE 410 may be pre-installed during the manufacturing of the electronic device 300, and in this case, operation 710 may be omitted.

[0158] In operation 720, the CRS 420 may install an applet related to the key used for authentication of the external electronic device 500 in the security module 330.

[0159] According to various embodiments of the disclosure, the PVKSE 410 may receive a message defined in the form shown in Table 5 below, and the CRS 420 may install the applet in the SSD 482 of the security module 330 using the received message.

TABLE 5

Tag	Length	Value	Description
'4F'	AID Length of PVKSE	AID of PVKSE	

[0160] Referring to Table 5, the message received by the PVKSE 410 may include a tag 4F indicating addition of an applet, the length of an AID, and an AID. According to various embodiments of the disclosure, the PVKSE 410 may receive an applet label, applet priority, and application-specific data, as well as the AID, and the CRS 420 may add the received data to the SSD 482. Table 6 below shows a specific example of the message received by the PVKSE 410 for installing the applet.

TABLE 6

A3 0F /			
4F 0D 32564B2E5359532E4444463031 //Add the PVKSE to the CREL list			
A6 19 /			
BF0C 16 /			
61 14 /			
4F 09 D28600015901140001			
AID=			
D28600015901140001			
50 06 424D57205835// Application Label =			
'BMW X5'			
87 01 01 / Priority indicator = 01			

[0161] In operation 730, the CRS 420 may define whether or not to activate the applet of the external electronic device 500 or the priority of the applet. A description of operation 730 will be made below with reference to FIGS. 8A and 8B.

[0162] [text missing or illegible when filed]

[0163] FIG. 8A is an operational flowchart illustrating an operation of activating an applet used for authentication of an electronic device in an operating method of an electronic device according to various embodiments of the disclosure.

[0164] Referring to FIG. 8A, an operation of activating or deactivating an applet used for authentication of an electronic device (e.g., the electronic device 300) may be performed through the operation of an application management user interface (AMUI) 801, a contactless request service (CRS) 803, an applet 805, and a PVKSE 807.

[0165] According to various embodiments of the disclosure, the AMUI 801 may denote an interface implemented between a user and the applet 805. The interface implemented between the user and the applet 805 may include visual elements, and the user may input a request for activation of the applet 805 through input onto the AMUI 801. The CRS 803 (e.g., the CRS 420 in FIG. 4) may denote an element for managing the files and the applets installed in the security module (e.g., the security module 330 in FIG. 3). The applet 805 (e.g., the applet 430, 440, 450, 460, or 470 in FIG. 4) may denote data used for authentication with the external electronic device (e.g., the electronic device 500 in FIG. 5). The PVKSE 807 (e.g., the PVKSE 410 in FIG. 4) may denote a software element capable of monitoring a change in at least one applet 805 and producing and managing information related to the applet 805.

[0166] In operation 809, the AMUI 801 may execute an application that manages a key used for authentication with the external electronic device 500. The application managing the key used for authentication with the external electronic device 500 may be installed in a memory (e.g., the memory 340 in FIG. 3) of the electronic device (e.g., the electronic device 300 in FIG. 3). The execution of the application may be triggered by a user input to the electronic device 300.

[0167] In operation 811, the AMUI 801 may make a request to the CRS 803 for applet information 811 used for authentication of the external electronic device 500. In operation 813, the CRS 803 may retrieve the applet information from the SSD of the security module 330 (e.g., the SSD 482 in FIG. 5), and may transmit the applet information based on the retrieved result to the AMUI 801.

[0168] In operation 815, the AMUI 801 may display the applet information received from the CRS 803 on a display device (e.g., the display device 160 in FIG. 1). In operation 817, the AMUI 801 may activate an applet selected based on

a user selection for the displayed applet information. In applet operation 819, the AMUI 801 may transmit a request for activating the selected applet to the CRS 803.

[0169] In operation 821, the CRS 803 may control the applet 805 such that the selected applet is activated. According to various embodiments of the disclosure, the CRS 803 may control the applet 805 such that the selected applet is activated by changing the data indicating activation or deactivation of the applet, which is included in the selected applet. The activated applet may refer to an applet capable of performing authentication of the electronic device 300 with the external electronic device 500, and the deactivated applet may refer to an applet that is unable to perform authentication of the electronic device 300 with the external electronic device 500.

[0170] In operation 823, the applet 805 may transmit the data indicating a change in the activation state of the applet 805 to the PVKSE 807. In operation 825, the PVKSE 807 may produce or change information related to the applet, based on whether or not the activation state of the applet 805 is changed. For example, if the applet 805 is changed to the activation state, the PVKSE 807 may change the information related to the applet by adding the information on the activated applet 805 (an AID, an applet label, priority information, application-specific data, etc.) to the template shown in Table 2.

[0171] In operation 827, the applet 805 may transmit, to the CRS 803, a message indicating the success of the change in the activation state of the applet 805, and in operation 829, the CRS 803 may transmit, to the AMUI 801, the message indicating the success of the change in the activation state of the applet 805.

[0172] [text missing or illegible when filed]

[0173] FIG. 8B is an operational flowchart illustrating an operation of configuring the priority of an applet used for authentication of an electronic device in an operating method of an electronic device according to various embodiments of the disclosure.

[0174] Referring to FIG. 8B, an operation of configuring the priority assigned to an applet used for authentication of an electronic device (e.g., the electronic device 300) may be performed through the operation of an application management user interface (AMUI) 801, a contactless register service (CRS) 803, an applet 805, and a PVKSE 807.

[0175] According to various embodiments of the disclosure, the AMUI 801 may denote an interface implemented between a user and the applet 805. The CRS 803 (e.g., the CRS 420 in FIG. 4) may denote an element for managing the files and the applets installed in the security module (e.g., the security module 330 in FIG. 3). The applet 805 (e.g., the applet 430, 440, 450, 460, or 470 in FIG. 4) may denote data used for authentication with the external electronic device (e.g., the electronic device 500 in FIG. 5). The PVKSE 807 (e.g., the PVKSE 410 in FIG. 4) may denote a software element capable of monitoring a change in at least one applet 805 and producing and managing information related to the applet 805.

[0176] In operation 831, the AMUI 801 may execute an application that manages a key used for authentication with the external electronic device 500. The application managing the key used for authentication with the external electronic device 500 may be installed in a memory (e.g., the memory 340 in FIG. 3) of the electronic device (e.g., the

electronic device 300 in FIG. 3). The execution of the application may be triggered by a user input to the electronic device 300.

[0177] In operation 833, the AMUI 801 may make a request to the CRS 803 for applet information used for authentication of the external electronic device 500. In operation 835, the CRS 803 may retrieve the applet information from the SSD 482 of the security module 330, and may transmit the applet information based on the retrieved result to the AMUI 801.

[0178] In operation 837, the AMUI 801 may display the applet information received from the CRS 803 on a display device (e.g., the display device 160 in FIG. 1), and may select an applet the priority of which is to be changed based on a user input onto the displayed applet information. The AMUI 801 may receive a user input making a request for configuring priority of the selected applet. Configuring priority of the applet may indicate an operation of assigning priority to the applet that has no priority or an operation of changing the priority that has been assigned to the applet.

[0179] In operation 839, the AMUI 801 may transmit a signal making a request for configuring priority of the selected applet to the CRS 803.

[0180] In operation 841, the CRS 803 may control the applet 805 so as to perform an operation of configuring priority of the selected applet. According to various embodiments of the disclosure, the applet 805 may change or produce priority information indicating the priority included in the selected applet based on the control of the CRS 803, thereby configuring the priority of the selected applet. The priority may represent the order in which authentication is performed on the external electronic device 500.

[0181] In operation 843, the applet 805 may transmit, to the PVKSE 807, a message indicating that the priority has been configured. In operation 845, the PVKSE 807 may produce or change information related to the applet in response to reception of the message indicating the priority configuration. If the priority of the applet 805 is changed, the PVKSE 807 may change the information related to the applet by changing the priority information included in the information on the activated applet 805 in the template shown in Table 2.

[0182] In operation 847, the applet 805 may transmit, to the CRS 803, a message notifying that the priority configuration is successful. In operation 849, the CRS 803 may transmit, to the AMUI 801, a message indicating that the priority configuration is successful. In operation 851, the AMUI 801 may update the applet list. The applet list may be updated based on the changed priority, and the applet list may be sorted according to the priority configured in each of the applets (e.g., the applets are arranged in descending order of the priority).

[0183] [text missing or illegible when filed]

[0184] FIG. 9 is an operational flowchart illustrating an operation of performing authentication of an electronic device in an electronic device shown in FIG. 5 in an operating method of an electronic device according to various embodiments of the disclosure.

[0185] In operation 901, a processor (e.g., the processor 510 in FIG. 5) of an electronic device (e.g., the electronic device 500 in FIG. 5) may receive a first AID list.

[0186] For example, the first AID list including identifications of activated applets among the applets stored in the security module 330 shown in FIG. 4 may include Vendor1

Vehicle Key2 (Vendor 1 VK2)/Vendor2 Vehicle Key1 (Vendor 2 VK1)/Sharing Key1 (SK1)/Sharing Key2 (SK2).

[0187] According to various embodiments of the disclosure, the processor 510 of the electronic device 500 may receive, from an external electronic device (e.g., the electronic device 300 in FIG. 3), a signal making a request for activating at least some of the various functions that can be executed by the electronic device 500. For example, the external electronic device 300 may produce a signal making a request for performing some functions of the electronic device 500 (e.g., a function of releasing the door lock of the electronic device 500, a function of turning on the lights of the electronic device 500, or a function of automatically pulling out the electronic device 500), based on a user input to the external electronic device 300, and may transmit the produced signal to the electronic device 500. In response to reception of the signal making a request for performing some functions of the electronic device 500, which is transmitted from the external electronic device 300, the processor 510 may initiate authentication with the external electronic device 300.

[0188] According to various embodiments of the disclosure, the first AID list may be produced by a PVKSE (e.g., the PVKSE 410 in FIG. 4) implemented in the security module 330 of the external electronic device 300.

[0189] In operation 903, the processor 510 may select one or more AIDs supported by the electronic device 500 from among the AIDs included in the first AID list, may produce a second AID list including the one or more selected AIDs, and may transmit the second AID list to the external electronic device 300.

[0190] According to various embodiments of the disclosure, the processor 510 may select the AIDs in a manner of selecting one or more AIDs remaining after filtering out applets having AIDs that are not supported by the electronic device 500 from among the AIDs included in the first AID list.

[0191] According to another embodiment of the disclosure, the processor 510 may select the AIDs in a manner of selecting the applets having the same AID as the manufacturer of the electronic device 500 from among the AIDs included in the first AID list.

[0192] According to still another embodiment of the disclosure, the processor 510 may select the AIDs in a manner of selecting the applets having the same AID as the manufacturer of the electronic device 500 from among the AIDs included in the first AID list and selecting one or more AIDs remaining after filtering out the applets having AIDs that are not supported by the electronic device 500 from among the AIDs corresponding to a sharing key.

[0193] For example, in the case where the electronic device 500 is manufactured by manufacturer 1, Vendor1 Vehicle Key2 (Vendor 1 VK2)/Sharing Key1 (SK1) that are the remaining AIDs, excluding Vendor2 Vehicle Key1 (Vendor 2 VK1) corresponding to manufacturer 2 and Sharing Key2 (SK2) corresponding to manufacturer 3, may be selected from among Vendor1 Vehicle Key2 (Vendor 1 VK2)/Vendor2 Vehicle Key1 (Vendor 2 VK1)/Sharing Key1 (SK1)/Sharing Key2 (SK2), which are the AIDs included in the first AID list.

[0194] According to various embodiments of the disclosure, the PVKSE 410 of the external electronic device 300 may receive the second AID list, and may transmit, to the electronic device 500, information related to the applets

corresponding to the respective AIDs included in the second AID list. The electronic device 500 may receive the information related to the applets transmitted from the PVKSE 410.

[0195] For example, the second AID list may include the AIDs selected by the electronic device 500, and the second AID list may include Vendor1 Vehicle Key2 (Vendor 1 VK2)/Sharing Key1 (SK1).

[0196] In operation 905, the processor 510 may select an AID having the highest priority from among the AIDs included in the second AID list. In operation 907, the processor 510 may perform authentication using information related to the applet corresponding to the AID having the highest priority.

[0197] In operation 909, the processor 510 may determine whether or not authentication is successful, and if the authentication fails, in operation 911, the processor 510 may select an AID having the highest priority among the AIDs that are included in the second AID list and have not yet been used in authentication, and may repeat authentication described in operation 907.

[0198] [text missing or illegible when filed]

[0199] An operating method of an electronic device according to various embodiments of the disclosure may include letting a communication module (the communication module 520 in FIG. 5) broadcast a connection request signal for a connection with an external electronic device (e.g., the electronic device 300 in FIG. 3) and establish a communication channel with the external electronic device 300 that responds to the broadcast signal, letting a security module (e.g., the security module 530 in FIG. 5) transmit a signal making a request for transmitting an AID list including one or more AIDs (application identifiers) stored in the external electronic device 300, letting the security module 530 select at least one AID from among the AIDs included in the AID list transmitted from the external electronic device 300, letting the security module 530 make a request to the external electronic device 300 for information indicating an applet corresponding to the selected AID and information related to the applet corresponding to the selected AID, and letting the security module 530 perform authentication with the external electronic device 300 using the information related to the applet received from the external electronic device 300.

[0200] According to various embodiments of the disclosure, the selecting at least one AID may include letting the security module 530 select the remaining AIDs, excluding AIDs corresponding to manufacturers other than the manufacturer of the electronic device (e.g., the electronic device 500 in FIG. 5), from among the AIDs included in the AID list, and the performing authentication with the external electronic device 400 may include performing authentication, based on the priority assigned to the AID.

[0201] [text missing or illegible when filed]

[0202] The electronic device according to various embodiments may be one of various types of electronic devices. The electronic devices may include, for example, a portable communication device (e.g., a smart phone), a computer device, a portable multimedia device, a portable medical device, a camera, a wearable device, or a home appliance. According to an embodiment of the disclosure, the electronic devices are not limited to those described above.

[0203] It should be appreciated that various embodiments of the disclosure and the terms used therein are not intended

to limit the technological features set forth herein to particular embodiments and include various changes, equivalents, or replacements for a corresponding embodiment. With regard to the description of the drawings, similar reference numerals may be used to refer to similar or related elements. It is to be understood that a singular form of a noun corresponding to an item may include one or more of the things, unless the relevant context clearly indicates otherwise. As used herein, each of such phrases as “A or B,” “at least one of A and B,” “at least one of A or B,” “A, B, or C,” “at least one of A, B, and C,” and “at least one of A, B, or C,” may include all possible combinations of the items enumerated together in a corresponding one of the phrases. As used herein, such terms as “1st” and “2nd,” or “first” and “second” may be used to simply distinguish a corresponding component from another, and does not limit the components in other aspect (e.g., importance or order). It is to be understood that if an element (e.g., a first element) is referred to, with or without the term “operatively” or “communicatively”, as “coupled with,” “coupled to,” “connected with,” or “connected to” another element (e.g., a second element), it means that the element may be coupled with the other element directly (e.g., wiredly), wirelessly, or via a third element.

[0204] As used herein, the term “module” may include a unit implemented in hardware, software, or firmware, and may interchangeably be used with other terms, for example, “logic,” “logic block,” “part,” or “circuitry”. A module may be a single integral component, or a minimum unit or part thereof, adapted to perform one or more functions. For example, according to an embodiment, the module may be implemented in a form of an application-specific integrated circuit (ASIC).

[0205] Various embodiments as set forth herein may be implemented as software (e.g., the program 140) including one or more instructions that are stored in a storage medium (e.g., internal memory 136 or external memory 138) that is readable by a machine (e.g., the electronic device 101). For example, a processor (e.g., the processor 120) of the machine (e.g., the electronic device 101) may invoke at least one of the one or more instructions stored in the storage medium, and execute it, with or without using one or more other components under the control of the processor. This allows the machine to be operated to perform at least one function according to the at least one instruction invoked. The one or more instructions may include a code generated by a compiler or a code executable by an interpreter. The machine-readable storage medium may be provided in the form of a non-transitory storage medium. Wherein, the term “non-transitory” simply means that the storage medium is a tangible device, and does not include a signal (e.g., an electromagnetic wave), but this term does not differentiate between where data is semi-permanently stored in the storage medium and where the data is temporarily stored in the storage medium.

[0206] According to an embodiment, a method according to various embodiments of the disclosure may be included and provided in a computer program product. The computer program product may be traded as a product between a seller and a buyer. The computer program product may be distributed in the form of a machine-readable storage medium (e.g., compact disc read only memory (CD-ROM)), or be distributed (e.g., downloaded or uploaded) online via an application store (e.g., Play Store™), or between two user

devices (e.g., smart phones) directly. If distributed online, at least part of the computer program product may be temporarily generated or at least temporarily stored in the machine-readable storage medium, such as memory of the manufacturer's server, a server of the application store, or a relay server.

[0207] According to various embodiments, each component (e.g., a module or a program) of the above-described components may include a single entity or multiple entities. According to various embodiments, one or more of the above-described components may be omitted, or one or more other components may be added. Alternatively or additionally, a plurality of components (e.g., modules or programs) may be integrated into a single component. In such a case, according to various embodiments, the integrated component may still perform one or more functions of each of the plurality of components in the same or similar manner as they are performed by a corresponding one of the plurality of components before the integration. According to various embodiments, operations performed by the module, the program, or another component may be carried out sequentially, in parallel, repeatedly, or heuristically, or one or more of the operations may be executed in a different order or omitted, or one or more other operations may be added.

1. An electronic device comprising:

a communication module configured to communicate with an external electronic device; and

a security module configured to monitor a change in data related to applets for managing keys used for authentication of the external electronic device, manage information related to the applet, and store an applet identification (AID) list comprising one or more AIDs and the applets.

wherein the security module is configured to:

receive, from the external electronic device, a signal making a request for transmitting the AID (application identifier) list;

in response to reception of the request signal, transmit the AID list to the external electronic device through the communication module;

receive, from the external electronic device, a signal requesting information related to an applet associated with at least one AID selected from among the AIDs included in the AID list by the external electronic device; and

transmit the information related to the applet corresponding to the selected AID to the external electronic device.

2. The electronic device of claim 1, wherein the information related to the applet comprises at least one of an address in which the applet is stored, the AID, a model identifier of the external electronic device, data indicating whether or not to activate the applet, priority assigned to each of the applets, or application-specific data.

3. The electronic device of claim 2, wherein the application-specific data comprises an available usage time of the external electronic device, geofencing limitation data of the external electronic device, or information indicating whether or not at least one of various functions that can be executed by the external electronic device is allowed.

4. The electronic device of claim 1, wherein the AID list is sorted based on the priority assigned to each of the applets.

5. The electronic device of claim 1, wherein the security module further comprises:

a CRS configured to manage data stored in the security module; and

a proximity vehicle key system environment (PVKSE) configured to monitor a change in data related to the applet and manage information related to the applet, wherein the CRS, in response to a signal making a request for changing configuration of the applet, changes configuration of at least one applet and transmits a signal indicating the change in the data to the PVKSE, and wherein the PVKSE, in response to reception of the signal indicating the change in the data, changes the data related to the applet.

6. The electronic device of claim 5, wherein the PVKSE and the CRS are configured to be stored in an issued security domain of the security module, and

wherein the applet is configured to be stored in a supplementary security domain thereof.

7. The electronic device of claim 1, wherein the information related to the applet is configured to be stored in a supplementary secure domain separated for each applet.

8. The electronic device of claim 5, wherein the PVKSE is configured to change the information related to the applet if a change in the applet is detected.

9. An electronic device comprising:

a memory;

a security module configured to store data used for authentication with an external electronic device;

a communication module; and

a processor,

wherein the security module is configured to:

broadcast a connection request signal for a connection with the external electronic device;

establish a communication channel with the external electronic device that responds to the broadcast signal;

transmit a signal making a request for transmitting an application identifier (AID) list comprising one or more AIDs stored in the external electronic device;

select at least one AID from among the AIDs included in the AID list transmitted by the external electronic device;

transmit, to the external electronic device, information indicating an applet corresponding to the selected AID and a signal requesting information related to the applet; and

perform authentication with the external electronic device using the information related to the applet received from the external electronic device.

10. The electronic device of claim 9, wherein the security module is configured to perform authentication, based on the priority assigned to the applet.

11. The electronic device of claim 10, wherein the security module is configured to:

perform authentication for the external electronic device using the information related to the applet;

in response to identifying that the authentication has failed, select an AID having a lower priority than the AID on which the authentication has been performed; and

request information related to an applet corresponding to the selected AID.

12. The electronic device of claim 9, wherein the security module is configured to select an AID corresponding to a manufacturer of the electronic device from among the AIDs included in the AID list.

13. The electronic device of claim 9, wherein the security module is configured to select an AID having the highest priority from AIDs corresponding to manufacturer of the electronic device, among the AIDs included in the AID list.

14. The electronic device of claim 9, wherein the AID list comprises at least one AID corresponding to the external electronic device and at least one AID corresponding to an external electronic device shared by other users.

15. The electronic device of claim 9, wherein the information related to the applet comprises at least one of an address in which the applet is stored, the AID, a model identifier of the electronic device, data indicating whether or not to activate the applet, priority assigned to each applet, or application-specific data.

□ * * * □

Search Notes 	Application/Control No. 17/767,153	Applicant(s)/Patent Under Reexamination FAHER et al.
	Examiner RICHARD G KEEHN	Art Unit 2444

CPC - Searched*		
Symbol	Date	Examiner
G06F21/62	05/07/2024	rkeehn
H04L63/101	05/07/2024	rkeehn
H04L63/20	05/07/2024	rkeehn
G06Q50/265	05/07/2024	rkeehn
G06Q20/3227,326,363,367,3825,3827,4014	05/07/2024	rkeehn

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor/Applicant search.	05/07/2024	rkeehn
Prior-art searches in PE2E-Search and Innovation Q+.	05/07/2024	rkeehn
Updated and interference searches.	08/19/2024	rkeehn
Updated searches.	11/04/2024	rkeehn

/RICHARD G KEEHN/ Primary Examiner, Art Unit 2444	
--	--

<i>Search Notes</i> 	Application/Control No. 17/767,153	Applicant(s)/Patent Under Reexamination FAHER et al.
	Examiner RICHARD G KEEHN	Art Unit 2444

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
G06F21	62	08/19/2024	rkeehn
H04L63	101	08/19/2024	rkeehn
H04L63	20	08/19/2024	rkeehn
G06Q50	265	08/19/2024	rkeehn
G06Q20	3227,326,363,367,3825,3827,4014	08/19/2024	rkeehn
G06F21	62	11/04/2024	rkeehn
H04L63	101	11/04/2024	rkeehn
H04L63	20	11/04/2024	rkeehn
G06Q50	265	11/04/2024	rkeehn
G06Q20	3227,326,363,367,3825,3827,4014	11/04/2024	rkeehn

/RICHARD G KEEHN/ Primary Examiner, Art Unit 2444	
--	--

Issue Classification 	Application/Control No. 17/767,153	Applicant(s)/Patent Under Reexamination FAHER et al.
	Examiner RICHARD G KEEHN	Art Unit 2444

CPC						
Symbol					Type	Version
G06F	/	21	/	62	F	2013-01-01
H04L	/	63	/	101	I	2013-01-01
H04L	/	63	/	20	I	2013-01-01
G06Q	/	50	/	265	A	2013-01-01

CPC Combination Sets					
Symbol				Type	Set
/		/			

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	16	
/RICHARD G KEEHN/ Primary Examiner, Art Unit 2444	04 November 2024	Q.G. Print Claim(s)	Q.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification 	Application/Control No. 17/767,153	Applicant(s)/Patent Under Reexamination FAHER et al.
	Examiner RICHARD G KEEHN	Art Unit 2444

INTERNATIONAL CLASSIFICATION			
CLAIMED			
G06F21/62	/	21	/ 62
H04L9/40	/	9	/ 40
G06Q50/26	/	50	/ 26
NON-CLAIMED			
	/		/

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	16	
/RICHARD G KEEHN/ Primary Examiner, Art Unit 2444	04 November 2024	Q.G. Print Claim(s)	Q.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification 	Application/Control No. 17/767,153	Applicant(s)/Patent Under Reexamination FAHER et al.
	Examiner RICHARD G KEEHN	Art Unit 2444

☐ Claims renumbered in the same order as presented by applicant
 ☐ CPA
 ☐ T.D.
 ☐ R.1,47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	4	10												
2	2	11	11												
5	3	12	12												
6	4	13	13												
7	5	14	14												
8	6	15	15												
9	7	16	16												
3	8														
10	9														

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 16	
/RICHARD G KEEHN/ Primary Examiner, Art Unit 2444 (Primary Examiner) _____ (Date) _____		04 November 2024 (Date) _____	Q.G. Print Claim(s) _____ 1
			Q.G. Print Figure _____ 3

Bibliographic Data

Application No: 17/767,153

Foreign Priority claimed: ☒ Yes ☐ No

35 USC 119 (a-d) conditions met: ☒ Yes ☐ No ☐ Met After Allowance

Verified and Acknowledged: /RICHARD G KEEHN/

Examiner's Signature

Initials

Title:

SECURITY MECHANISM FOR NAMESPACES USED IN
ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
04/07/2022	726	2444	GMT4110US/WO MQ/MB
RULE			

APPLICANTS

THALES DIS FRANCE SAS, MEUDON, FRANCE

INVENTORS

Mourad FAHER, MEUDON, FRANCE

Carole BAYLE, MEUDON, FRANCE

CONTINUING DATA

This application is a 371 of PCT/EP2020/076906 09/25/2020

FOREIGN APPLICATIONS

EPO EP19306357.5 10/18/2019

IF REQUIRED, FOREIGN LICENSE GRANTED**

08/12/2022

STATE OR COUNTRY

FRANCE

ADDRESS

THALES DIS CPL USA, INC.

Intellectual Property

900 South Pine Island Road

Suite 710

PLANTATION, FL 33324

UNITED STATES

FILING FEE RECEIVED

\$1,660

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17767153
	Filing Date	2022-04-07
	First Named Inventor	Mourad FAHER
	Art Unit	2444
	Examiner Name	RICHARD G KEEHN
	Attorney Docket Number	GMT4110US/WO MQ/MB

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.G.K/

U.S. PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	
	1						
If you wish to add additional U.S. Patent citation information please click the Add button.							Add
U.S. PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	
/R.G.K/	1	2020/0391695	A1	2020-12-17	Samsung Electronics Co.	Submitted with IDS 10/25/24	
		20160029403	A1	2016-10-05	United Services Automobile Association (USAA) -US	Type, not relevant prior art & applicant does not match.	
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add
FOREIGN PATENT DOCUMENTS							Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
/R.G.K/	1	1020190115361	KR	A	2019-10-11	Samsung Electronics co ltd	
If you wish to add additional Foreign Patent Document citation information please click the Add button.							Add
NON-PATENT LITERATURE DOCUMENTS							Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.					T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17767153
Filing Date	2022-04-07
First Named Inventor	Mourad FAHER
Art Unit	2444
Examiner Name	RICHARD G KEEHN
Attorney Docket Number	GMT4110US/WO MQ/MB

1		☐
---	--	--------------------------

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/RICHARD G KEEHN/	Date Considered	11/02/2024
--------------------	-------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17767153
Filing Date	2022-04-07
First Named Inventor	Mourad FAHER
Art Unit	2444
Examiner Name	RICHARD G KEEHN
Attorney Docket Number	GMT4110US/WO MQ/MB

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Adam F. Lewental/	Date (YYYY-MM-DD)	2024-10-25
Name/Print	Adam F. LEWENTAL	Registration Number	73527

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	1	"20220374533"	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/03 12:39 PM
L2	136	((("THALES") near3 ("DIS") near3 ("FRANCE") near3 ("SAS"))).AS,AANM,	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:06 PM
L4	14	((("FAHER") near3 ("Mourad")) OR ((("BAYLE") near3 ("Carole"))).INV	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:07 PM
L5	147	2 4	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:07 PM
L6	2	5 AND wallet.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:08 PM
L7	1	6 AND eid.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/06 05:08 PM
L8	0	6 AND eid.clm.	(USPAT)	OR	ON	ON	2024/05/06 05:08 PM
L9	208115	(G06F21/62 OR H04L63/101 OR H04L63/20 OR G06Q50/265 OR G06Q20/3227,326,363, 367,3825,3827,4014).c pc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/06 05:10 PM
L10	168211	9 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/06 05:11 PM
L11	476	(namespace "name space") WITH security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:42 PM
L12	2	(namespace "name space") WITH security WITH (rule policy procedure) WITH reader	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:42 PM
L13	19	(namespace "name space") WITH security WITH (rule policy procedure) WITH (select\$4 choos\$4)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:43 PM
L14	0	13 AND 10	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:43 PM
L15	3	13 AND (@ad	(US-PGPUB; USPAT;	OR	ON	ON	2024/05/07

		@prad)<20191018	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)				01:43 PM
L16	141	(EID "electronic identification") WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:46 PM
L17	11	11 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:47 PM
L18	0	17 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:47 PM
L19	4815	(namespace "name space") WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:47 PM
L20	11	19 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:48 PM
L21	0	20 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:48 PM
L22	262497	security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:48 PM
L23	11	16 WITH 22	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:49 PM
L24	0	23 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:49 PM
L25	476	(namespace "name space") WITH security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:49 PM
L26	476	22 AND 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:50 PM
L27	476	22 SAME 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:50 PM
L28	476	22 WITH 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	ON	2024/05/07 01:50 PM

L29	11	28 AND 16	JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:52 PM
L30	0	29 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:52 PM
L31	49	28 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:53 PM
L32	32	31 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:53 PM
L33	433	(select\$4 choos\$4) WITH namespace WITH access\$4	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:56 PM
L34	5841	namespace WITH (rule policy procedure check\$4 algorithm)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:57 PM
L35	159	33 AND 34	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:57 PM
L36	95	35 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:58 PM
L37	23024057	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:59 PM
L38	77	36 AND 37	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 01:59 PM
L39	77	38 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:00 PM
L40	19	38 AND (@ad @prad)<20191018 AND 9	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:00 PM
L41	1159	(mobile wireless portable cell cellular phone tablet ipad ipod	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2024/05/07 02:20 PM

L42	65	notebook radio) WITH namespace 41 AND wallet	IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:21 PM
L43	50	42 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:21 PM
L44	40942	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:51 PM
L45	1159	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH namespaces	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:52 PM
L46	51	44 AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:52 PM
L47	36	46 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 02:52 PM
L48	65	wallet AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:13 PM
L49	50	48 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:13 PM
L50	881	45 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:32 PM
L51	50	45 AND (@ad @prad)<20191018 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:32 PM
L52	66	45 AND (@ad @prad)<20191018 AND (eid wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:33 PM
L53	16	52 NOT 51	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:33 PM
L54	43457	(mobile wireless	(US-PGPUB; USPAT;	OR	ON	ON	2024/05/07

L55	40942	portable cell cellular phone tablet ipad ipod notebook radio) WITH (eid wallet)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	03:35 PM
L56	28	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH (wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:35 PM
L57	9	55 AND ((rule policy procedure safeguard) WITH namespace)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:36 PM
L58	8	56 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:36 PM
L59	3	((US-10922386-B1 OR US-11973758-B2).did. AND USPT.dbnm.) OR ((US-20090006642-A1 OR US-20160055248- A1 OR US- 20150040180-A1 OR US-20060265508-A1 OR US-20120159195- A1 OR US- 20220374533-A1).did. AND PGPB.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:40 PM
L60	289	58 AND 10	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:40 PM
L61	14	45 AND reader	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:54 PM
L61	14	45 AND (reader WITH wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	ON	2024/05/07 03:55 PM

L62	12	61 AND (@ad @prad)<20191018	JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 03:56 PM
L63	16	(list\$4 roster) WITH namespaces WITH (reader cardreader)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 05:46 PM
L64	10	(bytestring "byte string") WITH template WITH (rules policies)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 05:47 PM
L65	1	63 AND 64	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 05:47 PM
L66	0	65 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/07 05:47 PM
L67	1	"20220374533"	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L68	159	((("THALES") near3 ("DIS") near3 ("FRANCE") near3 ("SAS"))).AS,AANM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L69	16	((("FAHER") near3 ("Mourad")) OR (("BAYLE") near3 ("Carole"))).INV.	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L70	170	2 4	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L71	2	5 AND wallet.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L72	1	6 AND eid.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L73	0	6 AND eid.clm.	(USPAT)	OR	ON	ON	2024/08/19 08:10 AM
L74	212175	(G06F21/62 OR H04L63/101 OR H04L63/20 OR G06Q50/265 OR G06Q20/3227,326,363, 367,3825,3827,4014).c pc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L75	168724	9 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L76	489	(namespace "name space") WITH security	(US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	ON	2024/08/19 08:10 AM

L77	2	WITH (rule policy procedure) (namespace "name space") WITH security WITH (rule policy procedure) WITH reader	JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L78	19	(namespace "name space") WITH security WITH (rule policy procedure) WITH (select\$4 choos\$4)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L79	0	13 AND 10	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L80	3	13 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L81	143	(EID "electronic identification") WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L82	11	11 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L83	0	17 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L84	4935	(namespace "name space") WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L85	11	19 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L86	0	20 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L87	268396	security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L88	11	16 WITH 22	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L89	0	23 AND (@ad	(US-PGPUB; USPAT;	OR	ON	ON	2024/08/19

		@prad)<20191018	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)				08:10 AM
L90	489	(namespace "name space") WITH security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L91	489	22 AND 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L92	489	22 SAME 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L93	489	22 WITH 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L94	11	28 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L95	0	29 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L96	49	28 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L97	32	31 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L98	442	(select\$4 choos\$4) WITH namespace WITH access\$4	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L99	5989	namespace WITH (rule policy procedure check\$4 algorithm)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L100	163	33 AND 34	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L101	95	35 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L102	23295819	(mobile wireless portable cell cellular	(US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	ON	2024/08/19 08:10 AM

L103	77	phone tablet ipad ipod notebook radio) 36 AND 37	JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L104	77	38 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L105	19	38 AND (@ad @prad)<20191018 AND 9	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L106	1186	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH namespace	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L107	65	41 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L108	50	42 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L109	42090	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L110	1186	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH namespaces	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L111	51	44 AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L112	36	46 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L113	65	wallet AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L114	50	48 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM

L115	882	45 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L116	50	45 AND (@ad @prad)<20191018 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L117	66	45 AND (@ad @prad)<20191018 AND (eid wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L118	16	52 NOT 51	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L119	44641	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH (eid wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L120	42090	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH (wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L121	28	55 AND ((rule policy procedure safeguard) WITH namespace)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L122	9	56 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L123	8	((US-10922386-B1 OR US-11973758-B2).did. AND USPT.dbnm.) OR ((US-20090006642-A1 OR US-20160055248-A1 OR US-20150040180-A1 OR US-20060265508-A1 OR US-20120159195-A1 OR US-20220374533-A1).did. AND PGPB.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L124	3	58 AND 10	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA,	OR	ON	ON	2024/08/19 08:10 AM

			EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L125	274	45 AND reader	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L126	14	45 AND (reader WITH wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L127	12	61 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L128	16	{list\$4 roster) WITH namespaces WITH (reader cardreader)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L129	10	(bytestring "byte string") WITH template WITH (rules policies)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L130	1	63 AND 64	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L131	0	65 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/19 08:10 AM
L132	2	"20160029483"	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 10:16 PM
L133	0	"1020190115361"	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 10:18 PM
L134	2	"1020190115361"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 10:18 PM
L135	2	"1020190115361"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 10:52 PM
L136	1	"20220374533"	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM

L137	170	((("THALES") near3 ("DIS") near3 ("FRANCE") near3 ("SAS"))).AS,AANM,	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L138	16	((("FAHER") near3 ("Mourad")) OR ((("BAYLE") near3 ("Carole"))).INV.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L139	181	2 4	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L140	2	5 AND wallet.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L141	1	6 AND eid.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L142	0	6 AND eid.clm.	(USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L143	214830	(G06F21/62 OR H04L63/101 OR H04L63/20 OR G06Q50/265 OR G06Q20/3227,326,363, 367,3825,3827,4014).c pc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L144	169034	9 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L145	503	(namespace "name space") WITH security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L146	2	(namespace "name space") WITH security WITH (rule policy procedure) WITH reader	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L147	20	(namespace "name space") WITH security WITH (rule policy procedure) WITH (select\$4 choos\$4)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L148	0	13 AND 10	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L149	3	13 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L150	147	(EID "electronic identification") WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM

L151	11	11 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L152	0	17 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L153	5025	(namespace "name space") WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L154	11	19 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L155	0	20 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L156	272670	security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L157	11	16 WITH 22	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L158	0	23 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L159	503	(namespace "name space") WITH security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L160	503	22 AND 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L161	503	22 SAME 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L162	503	22 WITH 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L163	11	28 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L164	0	29 AND (@ad	(US-PGPUB; USPAT;	OR	ON	ON	2024/11/02

		@prad)<20191018	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)				11:27 PM
L165	49	28 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L166	32	31 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L167	451	(select\$4 choos\$4) WITH namespace WITH access\$4	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L168	6105	namespace WITH (rule policy procedure check\$4 algorithm)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L169	167	33 AND 34	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L170	95	35 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L171	23478438	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L172	77	36 AND 37	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L173	77	38 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L174	19	38 AND (@ad @prad)<20191018 AND 9	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L175	1203	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH namespace	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L176	65	41 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L177	50	42 AND (@ad	(US-PGPUB; USPAT;	OR	ON	ON	2024/11/02

		@prad)<20191018	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)				11:27 PM
L178	42875	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L179	1203	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH namespaces	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L180	51	44 AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L181	36	46 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L182	65	wallet AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L183	50	48 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L184	883	45 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L185	50	45 AND (@ad @prad)<20191018 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L186	66	45 AND (@ad @prad)<20191018 AND (eid wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L187	16	52 NOT 51	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L188	45453	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH (eid wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L189	42875	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH (	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM

L190	28	wallet) 55 AND ((rule policy procedure safeguard) WITH namespace)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L191	9	56 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L192	8	((US-10922386-B1 OR US-11973758-B2).did. AND USPT.dbnm.) OR ((US-20090006642-A1 OR US-20160055248- A1 OR US- 20150040180-A1 OR US-20060265508-A1 OR US-20120159195- A1 OR US- 20220374533-A1).did. AND PGPB.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L193	3	58 AND 10	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L194	274	45 AND reader	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L195	14	45 AND (reader WITH wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L196	12	61 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L197	16	(list\$4 roster) WITH namespaces WITH	(US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	ON	2024/11/02 11:27 PM

L198	10	(reader cardreader) (bytestring "byte string") WITH template WITH (rules policies)	JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L199	1	63 AND 64	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L200	0	65 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L201	1	"20220374533"	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L202	170	((("THALES") near3 ("DIS") near3 ("FRANCE") near3 ("SAS"))).AS,AANM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L203	16	((("FAHER") near3 ("Mourad")) OR (("BAYLE") near3 ("Carole"))).INV.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L204	181	2 4	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L205	2	5 AND wallet.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L206	1	6 AND eid.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L207	0	6 AND eid.clm.	(USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L208	214830	(G06F21/62 OR H04L63/101 OR H04L63/20 OR G06Q50/265 OR G06Q20/3227,326,363, 367,3825,3827,4014).c pc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L209	169034	9 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L210	503	(namespace "name space") WITH security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L211	2	(namespace "name space") WITH security WITH (rule policy procedure) WITH reader	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L212	20	(namespace "name	(US-PGPUB; USPAT;	OR	ON	ON	2024/11/02

		space") WITH security WITH (rule policy procedure) WITH (select\$4 choos\$4)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)				11:27 PM
L213	0	13 AND 10	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L214	3	13 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L215	147	(EID "electronic identification") WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L216	11	11 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L217	0	17 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L218	5025	(namespace "name space") WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L219	11	19 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L220	0	20 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L221	272670	security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L222	11	16 WITH 22	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L223	0	23 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L224	503	(namespace "name space") WITH security WITH (rule policy procedure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L225	503	22 AND 25	(US-PGPUB; USPAT;	OR	ON	ON	2024/11/02

L226	503	22 SAME 25	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	11:27 PM 2024/11/02 11:27 PM
L227	503	22 WITH 25	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L228	11	28 AND 16	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L229	0	29 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L230	49	28 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L231	32	31 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L232	451	(select\$4 choos\$4) WITH namespace WITH access\$4	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L233	6105	namespace WITH (rule policy procedure check\$4 algorithm)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L234	167	33 AND 34	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L235	95	35 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L236	23478438	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L237	77	36 AND 37	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L238	77	38 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	ON	2024/11/02 11:27 PM

L239	19	38 AND (@ad @prad)<20191018 AND 9	JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L240	1203	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH namespace	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L241	65	41 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L242	50	42 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L243	42875	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L244	1203	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH namespaces	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L245	51	44 AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L246	36	46 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L247	65	wallet AND 45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L248	50	48 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L249	883	45 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L250	50	45 AND (@ad @prad)<20191018 AND wallet	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM

L251	66	45 AND (@ad @prad)<20191018 AND (eid wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L252	16	52 NOT 51	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L253	45453	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH (eid wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L254	42875	(mobile wireless portable cell cellular phone tablet ipad ipod notebook radio) WITH (wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L255	28	55 AND ((rule policy procedure safeguard) WITH namespace)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L256	9	56 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L257	8	((US-10922386-B1 OR US-11973758-B2).did. AND USPT.dbnm.) OR ((US-20090006642-A1 OR US-20160055248-A1 OR US-20150040180-A1 OR US-20060265508-A1 OR US-20120159195-A1 OR US-20220374533-A1).did. AND PGPB.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L258	3	58 AND 10	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA,	OR	ON	ON	2024/11/02 11:27 PM

L259	274	45 AND reader	VN); FPRS; EPO; JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L260	14	45 AND (reader WITH wallet)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L261	12	61 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L262	16	(list\$4 roster) WITH namespaces WITH (reader cardreader)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L263	10	(bytestring "byte string") WITH template WITH (rules policies)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L264	1	63 AND 64	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L265	0	65 AND (@ad @prad)<20191018	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L266	2	"20160029483"	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L267	0	"1020190115361"	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
L268	2	"1020190115361"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM
L269	2	"1020190115361"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/02 11:27 PM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N1	75477	(G06F21/62 OR H04L63/101 OR H04L63/20 OR G06Q50/265 OR G06Q20/3227,326,363,	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:08 AM

N2	3337	367,3825,3827,4014).c pc. N1 AND wallet.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:09 AM
N3	5	N2 AND ("electronic identification" eid).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:09 AM
N4	1	N3 AND namespace.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/19 08:10 AM
N5	0	N3 AND namespace.clm.	(USPAT)	OR	ON	ON	2024/08/19 08:10 AM
N6	76900	(G06F21/62 OR H04L63/101 OR H04L63/20 OR G06Q50/265 OR G06Q20/3227,326,363, 367,3825,3827,4014).c pc.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
N7	3454	N1 AND wallet.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
N8	5	N2 AND ("electronic identification" eid).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
N9	1	N3 AND namespace.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/02 11:27 PM
N10	0	N3 AND namespace.clm.	(USPAT)	OR	ON	ON	2024/11/02 11:27 PM



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

180929 7590 11/20/2024
THALES DIS CPL USA, INC.
Intellectual Property
900 South Pine Island Road
Suite 710
PLANTATION, FL 33324

EXAMINER

KEEHN, RICHARD G

ART UNIT

PAPER NUMBER

2444

DATE MAILED: 11/20/2024

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/767,153	04/07/2022	Mourad FAHER	GMT4110US/WO MQ/MB	2044

TITLE OF INVENTION: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1200	\$0.00	\$0.00	\$1200	02/20/2025

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

180929 7590 11/20/2024
THALES DIS CPL USA, INC.
Intellectual Property
900 South Pine Island Road
Suite 710
PLANTATION, FL 33324

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17767.153	04/07/2022	Mourad FAHER	GMT4110US/WO MQ/MB	2044

TITLE OF INVENTION: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1200	\$0.00	\$0.00	\$1200	02/20/2025

EXAMINER	ART UNIT	CLASS-SUBCLASS
KEEHN, RICHARD G	2444	726-004000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1	_____
2	_____
3	_____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required)

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☐ Electronic Payment (via the USPTO patent electronic filing system) ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____	Date _____
Typed or printed name _____	Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/767,153	04/07/2022	Mourad FAHER	GMT4110US/WO MQ/MB	2044
180929 7590 11/20/2024 THALES DIS CPL USA, INC. Intellectual Property 900 South Pine Island Road Suite 710 PLANTATION, FL 33324			EXAMINER KEEHN, RICHARD G	
			ART UNIT 2444	PAPER NUMBER
DATE MAILED: 11/20/2024				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.** Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013).

<https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf>

Routine uses of the information in this record may include disclosure to:

- 1) law enforcement, in the event that the system of records indicates a violation or potential violation of law;
- 2) a federal, state, local, or international agency, in response to its request;
- 3) a contractor of the USPTO having need for the information in order to perform a contract;
- 4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record;
- 5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record;
- 6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations;
- 7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals;
- 8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c));
- 9) the Office of Personnel Management (OPM) for personnel research purposes; and
- 10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Notice of Allowability	Application No. 17/767,153	Applicant(s) FAHER et al.	
	Examiner RICHARD G KEEHN	Art Unit 2444	AIA (FITF) Status Yes

– The MAILING DATE of this communication appears on the cover sheet with the correspondence address–

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 10/25/2024.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 1-16. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
Certified copies:
a) ☒ All b) ☐ Some* c) ☐ None of the:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)	5. ☐ Examiner's Amendment/Comment
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date <u>10/25/2024</u> .	6. ☐ Examiner's Statement of Reasons for Allowance
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.	7. ☒ Other <u>Detailed Action</u> .
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.	

/RICHARD G KEEHN/ Primary Examiner, Art Unit 2444	
--	--

DETAILED ACTION

- 1. Claims 1-16 are pending and have been examined.**
- 2. There are no new, nor canceled claims.**

Notice of Pre-AIA or AIA Status

- 3. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.**

Continued Examination Under 37 CFR 1.114

- 4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after allowance or after an Office action under *Ex Parte Quayle*, 25 USPQ 74, 453 O.G. 213 (Comm'r Pat. 1935). Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, prosecution in this application has been reopened pursuant to 37 CFR 1.114. **Applicant's submission filed on 10/25/2024 has been entered.****

Information Disclosure Statement

- 5. The information disclosure statement (IDS) submitted on 10/25/2024 was filed after the mailing date of the Notice of Allowance on 8/28/2024. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.**

6. The IDS submitted 10/25/2024 lists US PG Publication 2016/0029483. Upon inspection of this reference, Examiner determined that the reference is directed to prior art far removed from that of the instant application's classifications and field of endeavor. Examiner reasonably concludes that listing the reference was a mistake, since Applicant also submitted US 2020/0391695 A1 which was not listed on the IDS. Examiner has reviewed the both US 2020/0391695 A1 and an English translation of submitted foreign reference KR-1020190115361-A; and finds neither changes Examiner's position on allowance. Examiner has annotated the 10/25/2024 IDS as such.

Allowable Subject Matter

7. Claims 1-16 are allowed.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to RICHARD G KEEHN whose telephone number is (571)270-5007. The examiner can normally be reached M-F 9:00am - 5:00pm Eastern.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A Follansbee can be reached on 571-272-3964. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/RICHARD G KEEHN/
Primary Examiner, Art Unit 2444

STATEMENT UNDER 37 CFR 3.73(c)First Named Inventor/Patent Owner: THALES DIS FRANCE SASApplication No./Patent No.: 17/767,153Filed/Issue Date: April 7 2022Titled: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
THALES DIS FRANCE SAS, a Corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):1. ☒ The assignee of the entire right, title, and interest.2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):☐ The extent (by percentage) of its ownership interest is ____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 059566, Frame 0702, or for which a copy thereof is attached*.B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached*.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached*.

[Page 1 of 2]

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0031. Public burden for this form is estimated to average 12 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached*.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached*.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached*.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached*.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ *As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Marc BOILLOT

Signature

/Marc BOILLOT/

Printed or Typed Name

February 17 2025

Date

56164

Title or Registration Number

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013). <https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf>

Routine uses of the information in this record may include disclosure to:

- 1) law enforcement, in the event that the system of records indicates a violation or potential violation of law;
- 2) a federal, state, local, or international agency, in response to its request;
- 3) a contractor of the USPTO having need for the information in order to perform a contract;
- 4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record;
- 5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record;
- 6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations;
- 7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals;
- 8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c));
- 9) the Office of Personnel Management (OPM) for personnel research purposes; and
- 10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION # 17/767,153	RECEIPT DATE / TIME 02/17/2025 09:46:00 AM Z ET	ATTORNEY DOCKET # GMT4110US/WO MQ/MB
------------------------------------	---	--

Title of Invention

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Application Information

APPLICATION TYPE	Utility - U.S. National Stage under 35 USC 371	PATENT #	-
CONFIRMATION #	2044	FILED BY	GHEZALI Djouher
PATENT CENTER #	69207671	AUTHORIZED BY	Marc Boillot
CUSTOMER #	180929	FILING DATE	04/07/2022
INTL. APPLICATION #	-	INTL. FILING DATE	-
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Mourad FAHER

Payment Information

PAYMENT METHOD DA / 604092	PAYMENT TRANSACTION ID E20252G046469508	PAYMENT AUTHORIZED BY GHEZALI Djouher
-------------------------------	--	--

FEE CODE	DESCRIPTION	ITEM PRICE(\$)	QUANTITY	ITEM TOTAL(\$)
1501	UTILITY ISSUE FEE	1200.00	1	1200.00
TOTAL AMOUNT:				\$1,200.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PART B – FEE(S) TRANSMITTAL

Complete and send this form, together with the applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By fax, send to: (571) 273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

THALES DIS CPL USA, Inc.
Intellectual Property
900 South Pine Island Road - Suite 710
Plantation, Florida 33324 - USAemail: us.intellectualproperty@thalesgroup.com
phone : 954-658-0418

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/767,153	April 7 2022	Mourad FAHER	GMT4110US/WO MQ/MB	2044

TITLE OF INVENTION:

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
Non Provisional	UNDISCOUNTED	\$1200	\$0.00	\$0.00	\$1200	February 20 2025

EXAMINER	ART UNIT	CLASS-SUBCLASS
RICHARD G KEEHN	2444	726/004.000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363)

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/ALA/47 or PTO/SB/47; Rev 03-09 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively, 1.
- (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2.
- 3.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE or COUNTRY)

THALES DIS FRANCE SAS

Meudon

France

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government4a. Fees Submitted: ☒ Issue Fee ☐ Publication Fee (if required)

4b. Method of Payment (Please first reapply any previously paid fee shown above):

- ☒ Electronic Payment via the USPTO patent electronic filing system ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 604092

5. Change of Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29.
- ☐ Applicant asserting small entity status. See 37 CFR 1.27.
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid Certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken as a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken as a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Marc BOILLOT/

Date February 17 2025

Typed or printed name Marc BOILLOT

Registration No. 56164

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013). <https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf>

Routine uses of the information in this record may include disclosure to:

- 1) law enforcement, in the event that the system of records indicates a violation or potential violation of law;
- 2) a federal, state, local, or international agency, in response to its request;
- 3) a contractor of the USPTO having need for the information in order to perform a contract;
- 4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record;
- 5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record;
- 6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations;
- 7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals;
- 8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c));
- 9) the Office of Personnel Management (OPM) for personnel research purposes; and
- 10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.



UNITED STATES
PATENT AND TRADEMARK OFFICE

Page 1 of 2
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION # 17/767,153	RECEIPT DATE / TIME 02/17/2025 09:46:00 AM Z ET	ATTORNEY DOCKET # GMT4110US/WO MQ/MB
------------------------------------	---	--

Title of Invention

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Application Information

APPLICATION TYPE	Utility - U.S. National Stage under 35 USC 371	PATENT #	-
CONFIRMATION #	2044	FILED BY	GHEZALI Djouher
PATENT CENTER #	69207671	FILING DATE	04/07/2022
CUSTOMER #	180929	FIRST NAMED INVENTOR	Mourad FAHER
INTL. APPLICATION #	-	INTL. FILING DATE	-
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Marc Boillot

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
GMT4110US_Statement_37 CFR3_73.pdf	3	Assignee showing of ownership per 37 CFR 3.73	224 KB
GMT4110US_Issue_FeeTransmittal.pdf	2	Issue Fee Payment (PTO-85B)	248 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
GMT4110US_Statement_37CFR3_73.pdf	C39817FF2FD7F0764571703F094A28D281545C1EFF1F95EF3C6FED68DA464AA2E9A9626298F1521A74E498580B9BA27C943

589A185FCAC0BBD538F50649668B5

GMT4110US_Issue_FeeTrans
mittal.pdf3C71BE61F9CE616831E69DDFF790797AF854D2E82C0868460
116AA55FFFCECEAD5EEAF0926F6368D787E0E16B47F4163A
4107FBAAC888A3B6E381E1110DBAE6A

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17767153
	Filing Date	2022-04-07
	First Named Inventor	Mourad FAHER
	Art Unit	2444
	Examiner Name	RICHARD G KEEHN
	Attorney Docket Number	GMT4110US/WO MQ/MB

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.G.K./

U.S. PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S. PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
Change(s) applied to document, /R.G.K./ /J.H./ 2/21/2025	1	2020/0391695	A1	2020-12-17	Yang et al.	Submitted with IDS 10/25/24		
		20160029403	A1	2016-10-05	Samsung Electronics Co., Ltd. United Services Automobile Association (USAA) -US	Type, not relevant prior art & applicant does not match.		
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
/R.G.K./	1	1020190115361	KR	A	2019-10-11	Samsung Electronics co ltd		☒
If you wish to add additional Foreign Patent Document citation information please click the Add button.							Add	
NON-PATENT LITERATURE DOCUMENTS							Remove	
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.					T ⁵	



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/767,153	03/18/2025	12254103	GMT4110US/WO MQ/MB	2044

180929 7590 02/26/2025
THALES DIS CPL USA, INC.
Intellectual Property
900 South Pine Island Road
Suite 710
PLANTATION, FL 33324

ISSUE NOTIFICATION

The projected patent number and issue date are specified above. The patent will issue electronically. The electronically issued patent is the official patent grant pursuant to 35 U.S.C. § 153. The patent may be accessed on or after the issue date through Patent Center at <https://patentcenter.uspto.gov/>. The patent will be available in both the public and the private sides of Patent Center. Further assistance in electronically accessing the patent, or about Patent Center, is available by calling the Patent Electronic Business Center at 1-888-217-9197.

The USPTO is implementing electronic patent issuance with a transition period, during which period the USPTO will mail a ceremonial paper copy of the electronic patent grant to the correspondence address of record. Additional copies of the patent (i.e., certified and presentation copies) may be ordered for a fee from the USPTO's Certified Copy Center at <https://certifiedcopycenter.uspto.gov/index.html>. The Certified Copy Center may be reached at (800)972-6382.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment is 272 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Center (<https://patentcenter.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PATENT CENTER site <https://patentcenter.uspto.gov> for additional inventors):

Mourad FAHER, MARLY LE ROI, FRANCE;
Carole BAYLE, MARSEILLE, FRANCE;

APPLICANT(s) (Please see PATENT CENTER site <https://patentcenter.uspto.gov> for additional applicants):

THALES DIS FRANCE SAS, MEUDON, FRANCE;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/767,153	04/07/2022	Mourad FAHER	GMT4110US/WO MQ/MB	2044
180929	7590	03/18/2025	EXAMINER	
THALES DIS CPL USA, INC. Intellectual Property 900 South Pine Island Road Suite 710 PLANTATION, FL 33324			KEEHN, RICHARD G	
			ART UNIT	PAPER NUMBER
			2444	
			NOTIFICATION DATE	DELIVERY MODE
			03/18/2025	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

adam.lewental@thalesgroup.com
marc.boillot@thalesgroup.com
us.intellectualproperty@thalesgroup.com

APPLICATION NO.	ISSUE DATE	PATENT NO.
17/767,153	18-Mar-2025	12254103

THALES DIS CPL USA, INC.
Intellectual Property
900 South Pine Island Road
PLANTATION, FL 33324

EGRANT NOTIFICATION

Your electronic patent grant (eGrant) is now available, which can be accessed via Patent Center at <https://patentcenter.uspto.gov>

The electronic patent grant is the official patent grant under 35 U.S.C. 153. For more information, please visit <https://www.uspto.gov/electronicgrants>