Innovation, Sciences et Développement économique Canada
Office de la propriété intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

Courtoisie - Réception de la requête d'examen
Courtesy - Acknowledgment of Request for Examination

ROBIC
opic.brevets@robic.com

Détails de la lettre
Letter Details

Date de la lettre: Letter Date:	2022/05/24
N° de la demande: Application N°:	**3,154,428**
Votre n° de référence: Your Reference N°:	014211-0023

Date de dépôt/Filing Date:	2020/09/25
Demandeur(s)/Applicant(s):	THALES DIS FRANCE SAS
Inventeur(s)/Inventor(s):	FAHER, MOURAD; BAYLE, CAROLE
Titre de l'invention:	MECANISME DE SECURITE POUR ESPACES DE NOMMAGE UTILISES DANS L'IDENTIFICA...
Title of Invention:	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON M...

Les dossiers du Bureau des brevets indiquent que la requête d'examen et les taxes réglementaires ont été reçues dans le délai réglementaire.

Patent Office records indicate that the request for examination and the prescribed fee(s) have been received within the prescribed time period.

L'examen de la demande se déroulera selon les délais d'usage.

Examination of the application will take place in due course.

Si le demandeur a connaissance de documents non-brevet (p. ex. articles de revues scientifiques, livres, affiches, articles) ou de documents en langue étrangère (p. ex. documents de brevet ou non-brevet) pouvant s'avérer pertinents à la brevetabilité de l'invention revendiquée, il doit envisager de fournir des copies ou des traductions de ces documents pertinents, lorsque ces copies ou traductions pourraient être difficilement accessibles par le Bureau. La remise volontaire de ces renseignements réduira la probabilité qu'une demande officielle soit présentée en vertu de l'art. 85 des *Règles sur les brevets* et peut accélérer le traitement de la demande.

If the applicant is aware of non-patent documents (e.g. journal articles, books, posters, articles) or foreign-language documents (e.g. patent or non-patent documents) that may be relevant to the patentability of the claimed invention, they should consider submitting copies or translations of the relevant documents, where the copies or translations of the documents may not be readily available to the Office. Voluntarily providing this information will reduce the likelihood of a formal requisition being made under s.85 of the *Patent Rules*, and may serve to expedite prosecution.

Pour de plus amples renseignements concernant cette lettre, veuillez consulter le *Recueil des pratiques du Bureau des brevets* (RPBB) accessible au canada.ca/brevets ou téléphoner au 1 819 997-2839.

For more information regarding this letter, please refer to the *Manual of Patent Office Practice* (MOPOP) at canada.ca/patents or phone 1-819-997-2839.

OKTA-1019
Okta, Inc. v. Thales DIS France SAS
IPR2026-00327

21 May 2026 (21-05-2026)

ROBIC AGENCE PI S.E.C./ROBIC IP AGENCY LP
opic.brevets@robic.com

Application No.	**:**	**3,154,428**
PCT No.	**:**	**EP2020076906**
Owner	**:**	THALES DIS FRANCE SAS
Title	**:**	**SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES**
Classification	**:**	G06F 21/62 (2013.01)
Your File No.	**:**	**014211-0023**
Examiner	**:**	Phoenix Bard-Cavers

YOU ARE HEREBY NOTIFIED OF A REQUISITION BY THE EXAMINER IN ACCORDANCE WITH SUBSECTION 86(2) OF THE *PATENT RULES*. IN ORDER TO AVOID ABANDONMENT UNDER PARAGRAPH 73(1)(*a*) OF THE *PATENT ACT*, A WRITTEN REPLY MUST BE RECEIVED WITHIN **FOUR (4)** MONTHS AFTER THE ABOVE DATE.

The applicant's letter of 28 July 2025 (28-07-2025) has been received and the application has been examined having regard to the applicant's arguments. However, the examiner considers that the application still does not comply with the *Patent Act* or *Patent Rules*.

The number of claims in this application is 21.

Documents Cited:

D1:*	US 2016/0294831 A1	Borunda et al.	6 October 2016 (06-10-2016)
D2:*	WO 2015/036957 A1	Renard et al.	19 March 2015 (19-03-2015)
D3:	American Association of Motor Vehicle Administrators (AAMVA), "Mobile Driver's License Functional Needs White Paper", *AAMVA - Public Information*, Version 9, Pages i-23, 7 March 2019 (07-03-2019)		
D4:	US 2017/0046809 A1	Laureano-Osorio	16 February 2017 (16-02-2017)
D5:	WO 2012/083199 A1	Von Behren et al.	12 June 2012 (12-06-2012)

* document cited by a foreign patent office

D1 discloses a system, method, and apparatus for providing digital identification.

D2 discloses a system and method for providing secure digital identification in a mobile digital wallet.

D3 discloses functional and administrative requirements for eIDs, in order for them to be used in

practical, real-world applications.

D4 discloses a method for providing digital identification.

D5 discloses a system and method for partitioning the namespaces of a secure element in contactless smart card devices, in order to provide data security.

Purposive Construction of Claims 1-21

The subject-matter defined by a claim is determined on the basis of a purposive construction of the claim conducted in accordance with the principles set out by the Supreme Court of Canada in *Free World Trust v Électro Santé Inc*., 2000 SCC 66 and *Whirlpool Corp. v Camco Inc*., 2000 SCC 67 (for more information please see the Practice Notice titled “March 2026 Patentable Subject-Matter under the *Patent Act*”).

The purposive construction of a claim is carried out in light of the whole of the specification and takes into account what the person skilled in the art would understand from the whole of the specification to be the nature of the invention.

In view of statements in the description (paragraphs 0001-0014, 0023-0029), the person skilled in the art to whom the application is directed can be characterized as a policy administrator familiar with identity and age verification regulations, including identity documents, and a computer programmer.

The person skilled in the art would possess the following common general knowledge (CGK):

- conventional mobile electronic devices, including processors;
- identity documents, such as government issued identity cards and private institution issued identity cards;
- conventional processors well-known in the art for communicating between electronic devices; and
- conventional processors well-known in the art for hosting electronic wallet applications and the corresponding programming therefor, based on the limited description of programming.

Given reference of interest in electronic wallets (paragraphs 0001-0014, 0023-0029) the person skilled in the art would understand that how to implement the claimed subject-matter on a computer system is CGK.

It is apparent that the disclosed method is an algorithm that is merely processed by the computer system in a conventional manner, and there is no evidence that the processing results in any improvement to the functioning of the computer system.

The skilled person would understand that the nature of the invention in claims 1-21 involves to providing data by determining the potential relevance of the data based on its label, and requiring the requestor of the data to satisfy a corresponding security policy.

There is no use of language in the claims indicating that any of the elements are optional, a

preferred embodiment or one of a list of alternatives. Therefore, all of the elements are considered to be essential according to the intent of the inventor as expressed in the claims.

Response to Applicant's Correspondence

The applicant's remarks of 28 July 2025 (28-07-2025) have been considered, but are not persuasive.

Regarding subsection 27(8) of the *Patent Act*, the examiner has been guided by the Office's examination practice as set out in practice notice titled "March 2026 Patentable Subject-Matter Under the Patent Act" and the relevant jurisprudence. As purposively construed above, the subject-matter defined by claims 1-21 is a computer-implemented abstract algorithm. The applicant states that "claims 1 and 15 recite a method in which a specific architecture having a combination of components with a physical existence is required to perform the method. The actual invention therefore consists of the specific combination of elements defined by the recited architecture (mobile device cooperating with reader in claim 1; mobile device cooperating with reader and verifier in claim 15 (all the components having their processor) and which cooperate together to provide the solution to the problem. In the present case, the actual invention does not reside solely in the processing streps performed by a computer, but rather in the specific cooperation between the components each performing a specific task", and "claim 11 is directed to a mobile device having a memory for storing instructions executable by the processor and including an eID wallet application having instructions to cause the processor to operate in a specific architecture having a combination of components with a physical existence and required for operation of the claimed mobile device. The actual invention therefore consists of the specific combination of elements defined by the recited architecture (mobile device cooperating with reader and which cooperate together to provide the solution to the problem. In the present case, the actual invention does not reside solely in the processing streps performed by the processor of the mobile device, but rather in the mobile device itself and its cooperation with the reader, with the mobile device and the reader each performing specific tasks".

This is not persuasive. The only essential element of the construed claims that has physicality is the computer which receives data and provides output information. The claims on file are not directed to a physical result, such as an improvement to the functioning of the computer.

Regarding section 28.3 of the *Patent Act*, the applicant's arguments against the prior art are not persuasive.

The independent claims of the present applications are:

1. A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device having a processor, the method comprising:
    a. associating, by the processor of the mobile device, security policies with each of a plurality of supported namespaces on the mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS); and
    b. operating a reader having a processor configured for executing a reader module to communicate with the mobile device and to select a namespace satisfying a required level of security (LOS) 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.

11. A mobile device comprising:
    a. a processor; and
    b. 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:
        i. receive a request for supported namespaces from a reader;
        ii. transmit a list of supported namespaces to the reader;
        iii. receive a list of selected namespaces satisfying a required level of security (LOS) from the reader; and
        iv. in response to receiving the list of selected namespaces from the reader,
        v. transmitting security rules associated with each selected namespace according to a defined bytestring template.

15. A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device having a processor, the method comprising:
    a. associating, by the processor of the mobile device, a security policy with each of a plurality of supported namespaces on the mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS);
    b. transmitting, by the processor of the mobile device, a list of supported namespaces and the security policy of each of the plurality of supported namespaces to a reader having a processor and connected to a verifier having a processor;
    c. selecting, by the processor of the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces, and transmitting from the reader to the mobile device, using the processor of
    d. the reader, a list containing the candidate namespaces;
    e. transmitting to the reader by the processor of the mobile device, the security policy associated with each of the selected candidate namespaces;
    f. operating the processor of the verifier to:
        i. determine for which of the candidate namespaces the verifier can satisfy corresponding access rules of the security policy of the namespace;
        ii. and
        iii. if the verifier can satisfy the corresponding access rules of the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which a verifier terminal can satisfy the corresponding access rules of the security policy, to access a data item, and demonstrating satisfaction of the corresponding access rules of the security policy to the mobile device;
        iv. if the verifier cannot satisfy the corresponding access rules of the security policy of any of the candidate namespaces, rejecting access to the data item; and
        v. upon successful demonstration by the reader to the mobile device of satisfaction of the corresponding access rules of the security policy of the selected namespace, granting access to the data item by the processor of the mobile device to the reader.

The claims, as written, do not define how the reader is aware of the security policies associated

with namespaces. It is also not defined what may be the use of security policies (which are undefined) beyond the fact that they participate to the namespace selection. Thus, an actual technical effect of the differentiating feature is not apparent.

While the language of the claims is to be construed in view of the specification as a whole, during examination, the language of the claims is interpreted by giving each term its plain and usual meaning in the art to which the invention pertains, unless it is clear from the description that a term in the claims is to be given a different meaning. Further, reference to the description cannot be used to vary the scope of the claims. Whenever an applicant desires to act as their own lexicographer in an application, it is incumbent on them to make this clear from the language of the description. In the present case, the applicant appears to rely on narrower interpretations of the claim language, by referring to the description.

The claims, as written, encompass the associated policies being generic policies also locally known from the requester for predefined kinds of eIDs. This policies may be deemed to be any kind of rules which may even be of business nature (paragraphs 0025-0029 of the present application provide such examples). It is maintained that selecting a namespace satisfying a required level of security (LOS) 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, is an obvious design choice, as the LOS and security policies are very broadly defined in the claims. The definition of LOS 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 (see paragraph 0005 of the present description).

D3, as a white paper, would motivate the person of ordinary skill in the art to use namespaces to satisfy an LOS as described in the present application, as the use case in present paragraphs 0025-0029 is analogous to the example in D3, point 2.6.1. Applicant has taken the definition of a “White Paper” from section 1 of D3; the rest of that section states “This document can be considered to be a White Paper. That is, this document is by no means the definitive and final word on mDL functional requirements. It is fully recognized that this topic will likely see significant growth in the months and years to come. Consequently this document intends to serve as a basis for further discussion, investigation and research”. One skilled in the art would therefore understand that D3 is meant to be read in the context of that state of the art as a whole, and would consider its teachings to be incorporated into the art of eIDs and electronic wallets. Additionally, the concept of data minimization is considered to be a security policy; restricting the data presented to “something about a field rather than the field itself”, as in the D3 example “the mDL holder should be able to release only the fact that the holder is above a certain age, rather than the actual date of birth” is considered to be a policy for securing a person’s birthdate information.

Allowable Claims

None of the claims on file are found to be allowable.

Summary of Defects

Claims 1-21 do not comply with section 2 of the *Patent Act*, and are prohibited by subsection 27(8) of the *Patent Act*.

Claims 1-21 do not comply with section 28.3 of the *Patent Act*.

The examiner has identified the following defects in the application:

Subject Matter

Claims 1-21 are directed to subject-matter that that lies outside the definition of “invention” and does not comply with section 2 of the *Patent Act* and is prohibited by subsection 27(8) of the *Patent Act*.

As purposively construed, the subject-matter defined by claims 1-21 is a computer-implemented abstract algorithm. The only essential element of the construed claims that has physicality is the computer which receives data and provides output information. It is therefore appropriate to ask the *Schlumberger* question, which compares the invention under consideration to *Schlumberger Canada Ltd. v. Commissioner of Patents*, 1981 CanLII 4718 (FCA), [1982] 1 FC 845), wherein a mathematical calculation was simply programmed into a computer and was not considered to constitute patentable subject-matter, and asks if the situations can be distinguished.

As evident from the purposive construction, the skilled person would understand that the claims encompass a well-known computer, which is used in a conventional manner, without imparting anything more, such as an improvement to the functioning of the computer. The claims cannot be distinguished from *Schlumberger* where an algorithm was merely programmed into a well-known computer as a bare practical application. As in *Schlumberger*, nothing other than an algorithm has been discovered and nothing physical results from processing the algorithm.

The subject-matter defined by the claims does not meet the physicality requirement implicit in the definition of invention and therefore lies outside the definition of “invention” and does not comply with section 2 of the *Patent Act* and is prohibited by subsection 27(8) of the *Patent Act*.

Obviousness

The claims on file do not comply with section 28.3 of the *Patent Act*. These claims are directed to subject-matter that does not require any degree of inventiveness and would have been obvious at the claim date to a person skilled in the art or science to which it pertains.

In *Apotex Inc. v. Sanofi-Synthelabo Canada Inc*., 2008 SCC 61 (“Sanofi”), the Supreme Court of Canada set forth a four-step approach that provides a framework for objectively assessing obviousness. These four steps have been applied to the claims on file as follows:

(**1)(a) – Identify the notional “person skilled in the art”.**
The person skilled in the art to whom the application is directed can be characterized as a policy administrator familiar with identity and age verification regulations, including identity documents, and a computer programmer.

(1)(b) – Identify the relevant common general knowledge of that person.
The common general knowledge of the person skilled in the art includes mobile communication devices, programming on generic computer systems, and electronic identification (eID) wallet

applications.

The common general knowledge of the person skilled in the art, as demonstrated in D1-D5, includes eIDs, levels of security corresponding to identification documents including eIDs, methods for maintaining data security, and

(2) – Identify the inventive concept of the claims in question or if that cannot readily be done, construe it.
The inventive concept of claims 1-14 pertains to a method and device comprising:

- associating security policies with each of a plurality of supported namespaces on a mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS); and
- operating a reader communicate with the mobile device and to select a namespace satisfying a required level of security (LOS) 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

The dependent claims also set out further limitations. However, as these limitations do not contribute anything substantial to the inventive concept, all of the claims are considered to share the same common inventive concept.

The inventive concept of claims 15-21 pertains to a method comprising:

- associating security policies with each of a plurality of supported namespaces on a mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS);
- transmitting a list of supported namespaces and the security policy of each of the plurality of supported namespaces to a reader having a processor and connected to a verifier;
- selecting by the verifier, at least one of the namespaces satisfying a required level of security (LOS) 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;
- determining, by the verifier, which of the candidate namespaces the verifier can satisfy corresponding access rules of the security policy of the namespace,
    - in the case that the verifier can satisfy the corresponding access rules of the security policy of at least one candidate namespace:
        - selecting one of the candidate namespaces for which a verifier terminal can satisfy the corresponding access rules of the security policy, to access a data item, and demonstrating satisfaction of the corresponding access rules of the security policy to the mobile device;
        - granting access to the data item by the processor of the mobile device to the reader; and
    - in the case that the verifier cannot satisfy the corresponding access rules of the security policy of any of the candidate namespaces:
        - rejecting access to the data item.

The dependent claims also set out further limitations. However, as these limitations do not contribute anything substantial to the inventive concept, all of the claims are considered to share the same common inventive concept.

(3) – Identify what, if any, differences exist between the matter cited as forming part of the "state of the art" and the inventive concept of the claims or the claims as construed.
D3 is considered to be the closest prior art and discloses a mobile driver's license (mDL) (2.1 Functional Requirement Summary), which may be stored in an electronic wallet on a mobile device (2.13 Wallet Solutions), and electronically secured so that the personally identifiable information related to the mDL is only when certain conditions are met (2.6 Data Privacy and Protection). D3 also discusses LOS being associated with the mDL (2.3 Trust Establishment, 2.4 Identity Confirmation, 2.14 Use Case Examples).

(4) – Do those differences constitute steps which would have been obvious to the person skilled in the art or do they require any degree of invention?
The differences would have been obvious to a person skilled in the art.

D3 is a White Paper, outlining requirements for digital identity systems (1. Introduction), and forms part of the common general knowledge. One skilled in the art would therefore look to prior art documents D1, D2, or D4 for detailed implementation.

D4 discloses a method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

- associating security policies (paragraphs 0008-0017, claim 1) with each of a plurality of supported namespaces on the mobile device (paragraph 0009), each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS) (implicit to all namespaces representing IDs, as each ID will either satisfy or not the level of security set by the authority using the reader; see claim 1, abstract: "plastic id cards, such as driver license, health insurance and others"); and
- operating a reader executing a reader module (claim 7) to communicate with the mobile device and to select a namespace satisfying a required level of security (LOS) 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 (paragraph 0013: "the invention may provide a user with the capability of sharing information with other users from within their own--MyPIDs---virtual folder. Moreover, a user may have the capability to define and individually control other users rights to data contained to be shared. The invention will be provided with read only access to prevent remote users affect others files placed in--MyPIDs--folder.").

While D4 does not explicitly disclose selecting a namespace satisfying a required level of security (LOS) 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, this is an obvious design choice; based on the requirements set in D3, the reader should not select a namespace that does not meet its own level of security, as this personal information is not relevant to the reader.

D1 discloses a similar method (paragraphs 0005-0008, 0021-0034, fig. 1, 2), as does D2 (abstract, page 1 line 25-page 3 line 18, page 6 line 28-page 13 line 32, fig. 1, 2, 3A, 3B). D1

and D2 do not disclose the use of namespaces, however, D4 demonstrates the use of namespaces for representing the stored data in a mobile wallet (paragraph 0009). For the sake of completeness, it is noted that D5 discloses the use of namespaces for security purposes in mobile wallet applications (abstract, paragraphs 0040-0045).

Regarding the steps of determining, by the verifier, which of the candidate namespaces the verifier can satisfy corresponding access rules of the security policy of the namespace,

- in the case that the verifier can satisfy the corresponding access rules of the security policy of at least one candidate namespace:
    - selecting one of the candidate namespaces for which a verifier terminal can satisfy the corresponding access rules of the security policy, to access a data item, and demonstrating satisfaction of the corresponding access rules of the security policy to the mobile device;
    - granting access to the data item by the processor of the mobile device to the reader; and
- in the case that the verifier cannot satisfy the corresponding access rules of the security policy of any of the candidate namespaces:
    - rejecting access to the data item,

these are all obvious design choices. One skilled in the art would consider it to be a requirement that the data items stored in an electronic identification (eID) wallet are only released when 1) the requestor can determine that the data items are relevant and 2) that the requestor can meet data security requirements, as each of documents D1-D5 pertain to personally identifiable information.

Conclusion

In view of the above, the claims on file are directed to subject-matter that does not require any degree of invention and would have been obvious at the claim date to a person skilled in the art, and do not comply with section 28.3 of the *Patent Act*. In view of the above , the claims on file are directed to an abstract algorithm, and do not comply with section 2 of the *Patent Act*, and are prohibited by subsection 27(8) of the *Patent Act*.

Examiner Requisitions

If the defects referred to in the requisition are not overcome, the application may be rejected in a **FINAL ACTION**.

In view of the foregoing defects, the applicant is requisitioned, under subsection 86(2) of the *Patent Rules*, to amend the application in order to comply with the *Patent Act* and the *Patent Rules* or to provide arguments as to why the application does comply.

Under section 102 of the *Patent Rules*, any amendment made in response to this requisition must be accompanied by a statement explaining the purpose of the amendment and identifying the differences between the new page and the replaced page.

Phoenix Bard-Cavers
Patent Examiner
819-965-5094

As per CIPO Client Service Standards, a response to a telephone enquiry or voice mail should be provided by the end of the next business day. In the event that attempts to reach the examiner are unsuccessful, the examiner's Section Head, Chaza Nasrallah, can be reached at 819-635-4148

For general inquiries: 1-866-997-1936 or for more options see http://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/wr00006.html.

The Examination Search Report is provided for reference only and is not part of any requisition made by the examiner in accordance with the *Patent Act* or *Rules*. The applicant is not required to respond to the information contained in the Examination Search Report.

Examination Search Report

Box I: General Information			
Application No.	3,154,428	Search Report Date	2026-05-21
Title	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		
Examiner	Phoenix Bard-Cavers	Search Conducted?	No
No search was conducted for the following reasons :			
- Search deferred - see report for reasoning (lack of unity, excluded subject matter etc.)			N/A
- Relied on previous search results (CIPO and/or by Foreign Office)			Yes

Box II: Family Prosecution		
Family Member	File Wrapper Reviewed	Status of Prosecution
WO2021073853A1	2025-01-15	Completed
US12254103B2	2026-05-20	In Progress
EP3809358A1	2025-01-14	Abandoned
EP4046126A1	2026-05-20	In Progress
AU2020367942A8	2025-01-15	Abandoned
AU2024201900A1	2026-05-20	In Progress
KR20220082904A	NO	
AU2026201983A1	2026-05-20	Not Started

Box III: Search History
No Search Conducted

CIPO Search Record - Version 10

ROBIC
1892

July 28, 2025

CANADIAN INTELLECTUAL PROPERTY OFFICE

Inventor(s):	FAHER, Mourad et al.
Applicant(s):	THALES DIS FRANCE SAS
Patent application N° :	3,154,428
Title:	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
Our file.:	014211-0023

COMMISSIONER OF PATENTS
GATINEAU, QUEBEC, K1A 0C9

RESPONSE TO A NOTICE UNDER SUBSECTION 86(2) OF THE *PATENT RULES*

Commissioner:

In response to the Examination Report of March 26, 2025, please amend the above-identified patent application as follows.

IN THE DESCRIPTION:

Please cancel pages 17-21 presently on file and substitute therefor enclosed new pages 17-22.

IN THE CLAIMS:

Please cancel the set of claims presently on file, and substitute therefor the enclosed new set of 21 claims.

REMARKS

Please examine the present patent application in view of the following remarks.

Modifications to the description

The description has been amended to reflect the subject matter as claimed.

Modifications to the claims

The claims are amended to better define the subject matter of the claims and/or for clarity purposes.

ROBIC
www.robic.ca
info@robic.com

MONTREAL
630 René-Lévesque Boulevard West
20th Floor
Montreal, Quebec, Canada H3B 1S6
Tel.: +1 514 987-6242 Fax: +1 514 845-7874

QUEBEC
Le Delta Building
2875 Laurier Boulevard, Delta 3 - suite 700
Quebec, Quebec, Canada G1V 2M2
Tel.: +1 418 653-1888 Fax.: +1 418 653-0006

Date reçue / Received date 2025-07-28

The Applicant submits that the present amendments are made solely to facilitate prosecution of the present application, without any admission regarding the characterization of the claims.

A marked-up copy of the set of claims which details each of the amendments made to the claims is enclosed for the Examiner's convenience.

Reply to the rejections under subsection 27(8) of the *Patent Act*

The Applicant has noted the Examination Report's objections to former claims 1-21 for allegedly defining an actual invention that is excluded subject-matter under subsection 27(8) of the *Patent Act* and not being patentable subject-matter.

Independent claims 1, 11 and 15 respectively recite:

Claim 1:

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

associating, by the processor of the mobile device, security policies with each of a plurality of supported namespaces on the mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS); and

operating a reader having a processor configured for executing a reader module to communicate with the mobile device and to select a namespace satisfying a required level of security (LOS) 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.

Claim 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 request for supported namespaces from a reader;

transmit a list of supported namespaces to the reader;

receive a list of selected namespaces satisfying a required level of security (LOS) from the reader; and

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.

Claim 15 :

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

asssociating, by the processor of the mobile device, a security policy with each of a plurality of supported namespaces on the mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS);

transmitting, by the processor of the mobile device, a list of supported namespaces and the security policy of each of the plurality of supported namespaces to a reader having a processor and connected to a verifier having a processor;

selecting, by the processor of the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces, and transmitting from the reader to the mobile device, using the processor of the reader, a list containing the candidate namespaces;

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

operating the processor of the verifier to:

determine for which of the candidate namespaces the verifier can satisfy corresponding access rules of the security policy of the namespace; and

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

if the verifier cannot satisfy the corresponding access rules of 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 corresponding access rules of the security policy of the selected namespace, granting access to the data item by the processor of the mobile device to the reader.

At least in view of the amendments to above-mentioned features of each one of claims 1, 11 and 15 provided in the presently submitted set of claims, the Applicant respectfully submits that the subject matter of the claims on file is directed to an actual invention that has physical existence.

Indeed, each one of independent method claims 1 and 15 recite a method in which a specific architecture having a combination of components with a physical existence is required to perform

the method. The actual invention therefore consists of the specific combination of elements defined by the recited architecture (mobile device cooperating with reader in claim 1; mobile device cooperating with reader and verifier in claim 15 (all the components having their processor) and which cooperate together to provide the solution to the problem. In the present case, the actual invention does not reside solely in the processing streps performed by a computer, but rather in the specific cooperation between the components each performing a specific task.

Similarly, independent claim 11 is directed to a mobile device having a memory for storing instructions executable by the processor and including an eID wallet application having instructions to cause the processor to operate in a specific architecture having a combination of components with a physical existence and required for operation of the claimed mobile device. The actual invention therefore consists of the specific combination of elements defined by the recited architecture (mobile device cooperating with reader and which cooperate together to provide the solution to the problem. In the present case, the actual invention does not reside solely in the processing streps performed by the processor of the mobile device, but rather in the mobile device itself and its cooperation with the reader, with the mobile device and the reader each performing specific tasks.

As indicated in the practice notice of the Canadian Intellectual Property Office (CIPO) titled *Patentable Subject-Matter under the Patent* from 2020, which is still current : *Where an actual invention consists of a combination of elements cooperating together, all of the elements of the combination must be considered as a whole when considering whether there is patentable subject-matter and whether the prohibition under subsection 27(8) of the Patent Act is applicable.*

Still in accordance with the principles of the practice notice : *An actual invention that includes a disembodied idea, a scientific principle or an abstract theorem is not patentable unless the disembodied idea, scientific principle or abstract theorem is part of a combination of elements that cooperate together and that combination has physical existence or manifests a discernible physical effect or change and relates to the manual or productive arts*. Consequently, even if the claimed subject matter was directed to an actual invention including a disembodied idea, a scientific principle or an abstract theorem, which the Applicant does not concede, it would be considered patentable for being part of a combination of elements which has a physical existence. The applicant also notes that in claims 1 and 15, all of the recited elements form part of the actual

invention, as they have a material effect on the working of the invention and cooperate with other elements of the claimed invention to achieve the desired result.

Consequently, the Applicant respectfully submits that independent claims 1, 11 and 15 are patentable under with subsection 27(8).

Dependent claims 2-10, 12-14 and 16-21 are dependent claims which depend directly or indirectly from one of claims 1, 11 and 15 and are also directed to patentable subject matter at least in view of their dependency.

In view of the above, withdrawal of the rejections under with subsection 27(8) of the *Patent Act* is thus respectfully requested.

Reply to the rejections under section 28.3 of the *Patent Act*

Applicant has taken note of the Examiner's rejection of former claims 1 -21 for allegedly lacking an inventive step having regard to either D1 (US 2016/0294831) or D2 (WO 2015/036957), in view of D4 (US 2017/0046809) or D5 WO 2012/083199, and the common general knowledge.

The Applicant has noted that the Examination describes D3 (NPL document titled *"Mobile Driver's License Functional Needs White Paper"* from the American Association of Motor Vehicle Administrators (AAMVA)) as a White Paper, outlining requirements for digital identity systems, and forming part of the common general knowledge and indicates that one skilled in the art would look to prior art documents D1, D2, or D4 for implementation.

Upon a thorough review of the cited prior art documents, the Applicant respectfully submits that the subject matter of currently submitted claims 1-21 is novel and inventive in view of the cited prior art documents. To that effect, the Applicant would like to offer the following remarks.

As mentioned in the Examination Report, document D3 is a White Paper of the AAMVA disclosing a mobile driver's license (mDL) that can be stored in a digital wallet, for example residing on a smartphone. (See point 2.13 of D3) D3 raises the security, privacy and user interface requirements set by the issuing authority (see again point 2.13) and the data privacy issues (see point 2.6). In point 2.6.1 of D3, it is specified that:

> "*a consumer should be able to read a mDL only if the mDL holder expressly agrees to such use. In addition, when the mDL holder is interacting with a non-*

> *official mDL consumer (e.g. a private establishment selling alcohol), the mDL holder should be able to control what data is released, and should have the option to limit the information to something about a field rather than the field itself. For example, the mDL holder should be able to release only the fact that the holder is above a certain age, rather than the actual date of birth. This concept is sometimes referred to as data minimization"*.

In short, document D3 thus describes a mDL stored in a digital wallet of a smartphone, with this mDL storing private data, and establishes that release of these private data has to be protected.

As document D3 is a white paper, which by its essence is not intended to propose solutions. Indeed, a white paper states requirements and formulates questions (without providing answers) on issues that require further investigation, analysis and discussion. The Examination Report relies on D1, D2, or D4 as allegedly teaching the implementation details as claimed in each one of independent claims 1, 11 and 15.

The Applicant respectfully disagrees.

Document D4 provides a description of an invention that was seen in a dream by the inventor (see abstract). In D4, the inventor proposes a personal folder (MyPIDs) allowing a user to generate and store some of his identification cards. At [0009], D4 discloses:

> "[a mobile phone] *with capacity to create a secure separate folder for -MyPIDs- with executable instructions that, when executed to perform a method of separating data and stored in a namespace, comprised the functions of:*
>
> - *creating a personal users folder configured to store ids profiles digital data and security certificates for a plurality users;*
> - *creating a folder with the design menu for this purpose to storing personal information to be shared with other users. -- MyPIDs folder being a subfolder under users folder category saved by the user. "*

At [0010] D4 teaches that the documents are created by the user.

However, upon a close review D4, the Applicant cannot follow the Examination Report's statement that document D4 discloses the claimed features of former claim 1.

Indeed, the Applicant respectfully submits that the teachings of D4 relating to the function of *creating a personal users folder configured to store ids profiles digital data and security certificates for a plurality users,* relative to the *method of separating data and stored in a namespace* is distinct from the claimed feature of *associating* […] *security policies with each of a plurality of supported namespaces on the mobile device, as* security certificates are distinct from the levels of security claimed in claim 1. *Hence,* D4 is absolutely silent associating namespaces and level of security. D4 merely discloses at [0013] that "*a user may have the capability to define and individually control other users rights to data contained to be shared. The invention will be provided with read only access to prevent remote users affect others files placed in MyPIDs-folder",* which is again distinct from the claimed feature of *associating […] security policies with each of a plurality of supported namespaces on the mobile device*.

The Applicant notes that the Examination Report states that "*While D4 does not explicitly disclose selecting a namespace satisfying a required level of security (LOS) 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, this is an obvious design choice; based on the requirements set in D3, the reader should not select a namespace that does not meet its own level of security, as this personal information is not relevant to the reader*."

It is respectfully submitted that the consideration that *selecting a namespace satisfying a required level of security (LOS) 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, is an obvious design choice* is not based on the teaching of D3 and/or D4, but rather a general statement not grounded on the prior art. Indeed, as discussed above, none of the cited prior art discloses associating security policies to namespaces and therefore, it cannot follow that it would be an *obvious design choice* to *select a namespace satisfying a required level of security.*

Thus, the Applicant stresses that the person of ordinary skills in the art would not find any technical solution in D3 and/or D4 for the claimed features of claim 1, encompassing security policies, namespaces, the association of security policies to namespaces, nor the selection of a namespace satisfying a Level of Security (LOS) based on securities policies.

The Examination Report also contends that "*D1 discloses a similar method*".

D1 discloses a method for "*comparing the location of a requester of a digital identification to the location of an owner of the digital identification. The method also includes providing information about the digital identification to the requester based at least in part on determining that the requester and the owner are within a predetermined distance*." (See abstract).

The Examination Report firstly cites [0005] to [0008] of D1. Upon review, the Applicant believes that the most relevant paragraph is [0008] which states:

> "*Providing information about the digital identification may be further based on receiving authorization to share the information from the owner. The methods may include the actions of receiving a pre-authorization to share the digital identification, and storing the pre-authorization. The pre-authorization may expire after a predetermined period of time. The location of the owner of the digital identification may be obtained without notifying the owner. The methods may include the actions of receiving a license plate number associated with a vehicle of the owner, identifying the owner based on the license plate number, and contacting a user device of the owner requesting the digital driver's license*."

The Examination Report also cites [0021] to [0034] of D1. D1 discloses at these paragraphs a digital wallet that can be interrogated by a requester of the age of the digital wallet holder for example. The owner of the digital wallet can decide to share the requested information or not.

Similarly to D3 and D4, The Applicant respectfully submits that, D1 is however silent about security policies, namespaces, the association of security policies to namespaces, and the selection of a namespace satisfying a Level of Security (LOS) based on securities policies.

Finally, D2 is a document similar to D3, the disclosure being based on the concept of *data minimization* (see abstract). At page 2 lines 16-18, this concept is named "minimum-required-subset of the personal ID information" stored in a secure element or in a secured wallet stored at a server (see Figure 2).

Once again, it is respectfully submitted that, In D2, there are no notions of security policies, namespaces, association of security policies to namespaces, nor a selection of a namespace satisfying a Level of security (LOS) based on securities policies.

In view of the above, the Applicant therefore submits that none of the cited documents discloses the steps of the method of claim 1 and 15, or the instructions stored in memory and causing the processor of the mobile device of claim 11 to perform the claimed steps.

Consequently, the Applicant respectfully submits that independent claims 1, 11 and 15 are new and inventive and conform to section 28.3 of the *Patent Act*. Dependent claims 2-10. 11-14 and 15-21 are dependent claims which depend directly or indirectly from one of claims 1, 11 and 15 and are also new and inventive at least in view of their dependency.

As a result, withdrawal of the rejections under section 28.3 of the *Patent Act* is thus respectfully requested.

Subsection 63(1) of the *Patent Rules*

Regarding the objection to claim 15 for allegedly not comply with subsection 63(1) of the *Patent Rules* for having been drafted as an independent claim, the Applicant disagrees with the Examination Report contention.

Indeed, the Applicant respectfully submits that claim 15 at least does not include the recited feature of claim 1 relative to *a reader having a processor configured for executing a reader module to communicate with the mobile device.*

In view of the above, the Applicant submits that claim 15 does not include all the features of claim 1 and therefore cannot be drafted as a dependent claim in accordance with subsection 63(1) of the *Patent Rules.*

In view of the above, withdrawal of the rejections under subsection subsection 63(1) of the *Patent Rules* is thus respectfully requested.

Good standing

It is believed that the present application is in good standing. If, however, it appears that the application is deemed abandoned, or if CIPO considers that this application is deemed abandoned, we request that CIPO informs us in writing immediately.

Should the amount(s) indicated in this letter be insufficient to cover all of the fee(s) for which payment(s) is(are) explicitly or implicitly requested by this letter, or if a fee payment cannot be

charged to the designated credit card, CIPO is hereby **unconditionally, clearly and unequivocally authorized** to debit any amount required to pay or complete any applicable fee from our deposit account **600000233**, in order to keep the present application in good standing.

CONCLUSION

In view of the above, it is submitted that all rejections and objections raised by the Examiner have been addressed and overcome by the present response and that the application now complies with the *Patent Act* and *Patent Rules.* Allowance of the claims and issuance of a Notice of Allowance are therefore respectfully solicited.

The Examiner is invited to call us if any further amendment will expedite allowance of the application or if the Examiner has any suggestions or questions concerning this application.

Respectfully submitted,



ROBIC AGENCE PI S.E.C. / ROBIC IP AGENCY LP
Patent and Trademark agents

Patent Agent : Jean-Francois Journault
+1 418-653-1829

JFJ/mlt

Encl. new pages 17-22 of the description;
Amended set of 21 claims; and
Marked up version of the amended set of claims.

[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] The following aspects are also disclosed herein:

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

   associating, by the processor of the mobile device, security policies with each of a plurality of supported namespaces on the mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS); and

   operating a reader having a processor configured for executing a reader module to communicate with the mobile device and to select a namespace satisfying a required level of security (LOS) 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 of aspect 1, comprising:

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

   selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces satisfying the required level of security (LOS) 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.

Date reçue / Received date 2025-07-28

3. The method of aspect 1, comprising:

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

   selecting, by the verifier module, at least one candidate namespace satisfying the required level of security (LOS) by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

4. The method of aspect 1 or 2, further comprising:

   prior to transmitting the list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that a 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 of any one of aspects 1 to 4, comprising:

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

6. The method of any one of aspects 1 to 5, 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 of any one of aspects 1 to 6, wherein a 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 of aspect 1, further comprising 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 a verifier associates with each namespace in the plurality of supported namespaces.

Date reçue / Received date 2025-07-28

9. The method of any one of aspects 1 to 8, further comprising 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 of aspect 1, 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 a 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 request for supported namespaces from a reader;

transmit a list of supported namespaces to the reader;

receive a list of selected namespaces satisfying a required level of security (LOS) from the reader; and

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 aspect 11, wherein the eID wallet application further comprises instructions to cause the processor to:

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

13. The mobile device of aspect 11 or 12, wherein the eID wallet application further comprises instructions to cause the processor to:

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

14. The mobile device of aspect 11, 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.

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

asssociating, by the processor of the mobile device, a security policy with each of a plurality of supported namespaces on the mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS);

transmitting, by the processor of the mobile device, a list of supported namespaces and the security policy of each of the plurality of supported namespaces to a reader having a processor and connected to a verifier having a processor;

selecting, by the processor of the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces, and transmitting from the reader to the mobile device, using the processor of the reader, a list containing the candidate namespaces;

Date reçue / Received date 2025-07-28

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

operating the processor of the verifier to:

determine for which of the candidate namespaces the verifier can satisfy corresponding access rules of the security policy of the namespace; and

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

if the verifier cannot satisfy the corresponding access rules of 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 corresponding access rules of the security policy of the selected namespace, granting access to the data item by the processor of the mobile device to the reader.

16. The method of aspect 15, wherein selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces is performed 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.

17. The method of aspect 15, wherein selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate

Date reçue / Received date 2025-07-28

namespaces is performed by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

18. The method of any one of aspects 15 to 17, further comprising:

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

19. The method of any one of aspects 15 to 18, 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.

20. The method of any one of aspects 15 to 19, wherein a required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

21. The method of aspect 15, 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 a verifier terminal.

Date reçue / Received date 2025-07-28

CLAIMS

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

    associating, by the processor of the mobile device, security policies with each of a plurality of supported namespaces on the mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS); and

    operating a reader having a processor configured for executing a reader module to communicate with the mobile device and to select a namespace satisfying a required level of security (LOS) 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 of claim 1, comprising:

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

    selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces satisfying the required level of security (LOS) 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 of claim 1, comprising:

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

selecting, by the verifier module, at least one candidate namespace satisfying the required level of security (LOS) by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

4. The method of claim 1 or 2, further comprising:

prior to transmitting the list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that a 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 of any one of claims 1 to 4, comprising:

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

6. The method of any one of claims 1 to 5, 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 of any one of claims 1 to 6, wherein a 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 of claim 1, further comprising 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 a verifier associates with each namespace in the plurality of supported namespaces.

9. The method of any one of claims 1 to 8, further comprising 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 of claim 1, 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 a 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 request for supported namespaces from a reader;

transmit a list of supported namespaces to the reader;

receive a list of selected namespaces satisfying a required level of security (LOS) from the reader; and

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 11, wherein the eID wallet application further comprises instructions to cause the processor to:

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

13. The mobile device of claim 11 or 12, wherein the eID wallet application further comprises instructions to cause the processor to:

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

14. The mobile device of claim 11, 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.

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

asssociating, by the processor of the mobile device, a security policy with each of a plurality of supported namespaces on the mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS);

transmitting, by the processor of the mobile device, a list of supported namespaces and the security policy of each of the plurality of supported namespaces to a reader having a processor and connected to a verifier having a processor;

selecting, by the processor of the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces, and

transmitting from the reader to the mobile device, using the processor of the reader, a list containing the candidate namespaces;

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

operating the processor of the verifier to:

determine for which of the candidate namespaces the verifier can satisfy corresponding access rules of the security policy of the namespace; and

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

if the verifier cannot satisfy the corresponding access rules of 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 corresponding access rules of the security policy of the selected namespace, granting access to the data item by the processor of the mobile device to the reader.

16. The method of claim 15, wherein selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces is performed 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.

17. The method of claim 15, wherein selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces is performed by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

18. The method of any one of claims 15 to 17, further comprising:

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

19. The method of any one of claims 15 to 18, 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.

20. The method of any one of claims 15 to 19, wherein a required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

21. The method of claim 15, 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 a verifier terminal.

CLAIMS

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

associating, by the processor of the mobile device, security policies with each of a plurality of supported namespaces on the mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS); and

operating a reader having a processor configured for executing a reader module to communicate with the mobile device and to select a namespace satisfying a required level of security (LOS) 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 of claim 1, comprising:

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

selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces satisfying the required level of security (LOS) 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.

Date reçue / Received date 2025-07-28

3. The method of claim 1, comprising:

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

selecting, by the verifier module, at least one candidate namespace satisfying the required level of security (LOS) by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

4. The method of claim 1 or 2, further comprising:

prior to transmitting the list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that a 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 of any one of claims 1 to 4, comprising:

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

6. The method of any one of claims 1 to 5, 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.

Date reçue / Received date 2025-07-28

7. The method of any one of claims 1 to 6, wherein a 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 of claim 1, further comprising 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 a verifier associates with each namespace in the plurality of supported namespaces.

9. The method of any one of claims 1 to 8, further comprising 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 of claim 1, 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 a verifier terminal.

Date reçue / Received date 2025-07-28

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 request for supported namespaces from a reader;

transmit a list of supported namespaces to the reader;

receive a list of selected namespaces satisfying a required level of security (LOS) from the reader; and

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 11, wherein the eID wallet application further comprises instructions to cause the processor to:

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

Date reçue / Received date 2025-07-28

13. The mobile device of claim 11 or 12, wherein the eID wallet application further comprises instructions to cause the processor to:

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

14. The mobile device of claim 11, 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.

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

asssociating, by the processor of the mobile device, a security policy with each of a plurality of supported namespaces on thea mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS);

transmitting, by the processor of the mobile device, a list of supported namespaces and the security policy of each of the plurality of supported namespaces to a reader having a processor and connected to a verifier having a processor;

selecting, by the processor of the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces, and

Date reçue / Received date 2025-07-28

transmitting from the reader to the mobile device, using the processor of the reader, a list containing the candidate namespaces;

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

operating the processor of the verifier to:

determine for which of the candidate namespaces the verifier can satisfy corresponding access rules of the security policy of the namespace; and

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

if the verifier cannot satisfy the corresponding access rules of 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 corresponding access rules of the security policy of the selected namespace, granting access to the data item by the processor of the mobile device to the reader.

Date reçue / Received date 2025-07-28

16. The method of claim 15, wherein selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces is performed 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.

17. The method of claim 15, wherein selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces is performed by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

18. The method of any one of claims 15 to 17, further comprising:

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

19. The method of any one of claims 15 to 18, 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.

Date reçue / Received date 2025-07-28

20. The method of any one of claims 15 to 19, wherein a required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

21. The method of claim 15, 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 a verifier terminal.

Date reçue / Received date 2025-07-28

26 March 2025 (26-03-2025)

ROBIC AGENCE PI S.E.C./ROBIC IP AGENCY LP
opic.brevets@robic.com

Application No.	**:**	**3,154,428**
PCT No.	**:**	**EP2020076906**
Owner	**:**	THALES DIS FRANCE SAS
Title	**:**	**SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES**
Classification	**:**	G06F 21/62 (2013.01)
Your File No.	**:**	**014211-0023**
Examiner	**:**	Phoenix Bard-Cavers

YOU ARE HEREBY NOTIFIED OF A REQUISITION BY THE EXAMINER IN ACCORDANCE WITH SUBSECTION 86(2) OF THE *PATENT RULES*. IN ORDER TO AVOID ABANDONMENT UNDER PARAGRAPH 73(1)(*a*) OF THE *PATENT ACT*, A WRITTEN REPLY MUST BE RECEIVED WITHIN **FOUR (4)** MONTHS AFTER THE ABOVE DATE.

The applicant's letter of 11 June 2024 (11-06-2024) has been received and the application has been examined having regard to the applicant's arguments. However, the examiner considers that the application still does not comply with the *Patent Act* or *Patent Rules*.

The number of claims in this application is 21.

Documents Cited:

D1:*	US 2016/0294831 A1	Borunda et al.	6 October 2016 (06-10-2016)
D2:*	WO 2015/036957 A1	Renard et al.	19 March 2015 (19-03-2015)
D3:	American Association of Motor Vehicle Administrators (AAMVA), "Mobile Driver's License Functional Needs White Paper", *AAMVA - Public Information*, Version 9, Pages i-23, 7 March 2019 (07-03-2019)		
D4:	US 2017/0046809 A1	Laureano-Osorio	16 February 2017 (16-02-2017)
D5:	WO 2012/083199 A1	Von Behren et al.	12 June 2012 (12-06-2012)

* document cited by a foreign patent office

Response to Applicant's Correspondence

The applicant's remarks of 11 June 2024 (11-06-2024) and 25 August 2023 (25-08-2023) have been considered, but are not persuasive.

According to the letter of 11 June 2024 (11-06-2024), the claims were amended to better define

the subject matter of the claims and/or for clarity purposes. Applicant submits that the amended claims 1,11 and 15 provide the information regarding the relationship between the security policies (or the details of the policies), and data items stored on the mobile device, overcoming the previously identified defects with regard to section 60 of the *Patent Rules*, and that the arguments regarding novelty and obviousness submitted with the letter of 25 August 2023 (25-08-2023) are applicable.

In the applicant's letter of 25 August 2023 (25-08-2023), applicant states:

> In section 2.2.1, the IPRP considers that claim 16 is just a description of a verifier (reader) accreditation principle that sorts out the mobile data into categories such as "acceptable" or "not acceptable".
>
> Thus, with respect to the subject matter of instant claim 1 (and consequently also instant claim 16), the Applicant considers that it is more than this administrative policy and, actually, the claimed subject matter defines the configuration by identification data issuers of security rules applying to data, which are determined at the mobile interface only by their names or labels.
>
> Namely, the feature so-called LOS (i.e., level of security) is not just an administrative accreditation to access data, but it is in practice a specific coding of security conditions that cannot be by default bore by labels because labels are not structures or containers pre-determined by existing standards, with known (to the skilled person in the art) fields or sub-containers dedicated to host security rules with known coding language, etc. So, this one aspect is where the claimed subject matter is laid: informing about security mechanisms attached to unstructured labels or names that are not files, dedicated files, data objects, records, byte strings or so.
>
> They are only names of data with absolutely no hint about actual data structure that can be any. The absence of structure does not allow for attachment of security rules to a part of the structure, whereby it does not offer either a pre-existing or by-default discovery mechanism, thus it requires specific design and this is what the claimed subject matter describes; and it describes as well how such design can be exploited to allow:
>
> 1. the reader / verifier to discover the security policy assigned by the issuer and
> 2. the reader I verifier to ask the mobile for data meeting a given LOS.
>
> Points (1) and (2) are specified nowhere for namespaces.
>
> Therefore, the subject matter of instant claim 1 is not defining mere data stored on a database with index and tables and named data with their corresponding security rules but, rather, it defines a discoverability mechanism of security policies for non-structured data.
>
> Therefore, contrary to the assertions in sections 2.2.2 and 2.2.3 of the IPRP that the only alleged features would be the mobile device communicating with the reader, the features mentioned above are not ‘‘administrative aspects", these relate with technical discoverability and coding language for security policies. Namely, they implement a (1) coding and assignment of security policies to non-structured identification data, (2)

discoverability of such policies, and (3) granularity of policies to the level of a namespace.

These arguments are not persuasive. Current claim 15 recites:

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

1. associating a security policy with each of a plurality of supported namespaces on a mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS);
2. transmitting a list of supported namespaces and the security policy of each of the plurality of supported namespaces to a reader connected to a verifier;
3. selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces, and transmitting from the reader to the mobile device, a list containing the candidate namespaces;
4. transmitting to the reader by the mobile device, the security policy associated with each of the selected candidate namespaces;
5. operating the verifier to:
    a) determine for which of the candidate namespaces the verifier can satisfy corresponding access rules of the security policy of the namespace; and
    b) if the verifier can satisfy the corresponding access rules of the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which a verifier terminal can satisfy the corresponding access rules of the security policy, to access a data item, and demonstrating satisfaction of the corresponding access rules of the security policy to the mobile device;
    c) if the verifier cannot satisfy the corresponding access rules of the security policy of any of the candidate namespaces, rejecting access to the data item; and
    d) upon successful demonstration by the reader to the mobile device of satisfaction of the corresponding access rules of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

The term “level of security” does not have a common meaning. Referring to the description (paragraphs 0050-0051), “level of security” refers to an administrative practice; the example given in the description is “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”. The limitation of “each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS)” in step 1 is therefore, simply a statement that each namespace would be considered acceptable or not acceptable under some administrative policy. The applicant’s argument that “the feature so-called LOS (i.e., level of security) is not just an administrative accreditation to access data, but it is in practice a specific coding of security conditions that cannot be by default bore by labels” is not followed; simply stating that the namespaces either meet an arbitrary condition or not is not a specific coding (ex. Does the namespace correspond to an ID that is accepted for a given policy?). Based on the description (paragraphs 0005, 0050-0051), the level of security is not a specific coding of security conditions that cannot be by default bore by labels, but an administrative practice to determine whether the labels (namespaces) correspond to accepted forms of identification; these “security

conditions” do not have any inherent features causing them to not be borne by labels, as a label such as “driver’s licence” clearly indicates a “level of security” as defined in the description.

Therefore, a level of security is understood as a required level of accreditation and a namespace as a category/kind of user identification information. The security policy associated with each namespace is used to control access to an unspecified data item by a verifier. Consequently, the level of security is simply used to determine potential relevance of data, based on a related namespace. Namespaces are commonly known in the art as a namespace is a set of signs (names) that are used to identify and refer to objects of various kinds. Therefore, determining whether namespaces satisfy a level of security (ie. whether they refer to relevant data) is not inventive. Requiring the verifier to satisfy access rules of the security policy of at least one candidate namespace in order to access a data item is also not inventive; it is common practice to utilize security policies to protect personal data.

Purposive Construction of Claims 1-21

The subject-matter defined by a claim is determined on the basis of a purposive construction of the claim conducted in accordance with the principles set out by the Supreme Court of Canada in *Free World Trust v Électro Santé Inc*., 2000 SCC 66 and *Whirlpool Corp. v Camco Inc*., 2000 SCC 67 (for more information please see the Practice Notice published on 3 November 2020 (03-11-2020) titled “Patentable Subject-Matter under the *Patent Act*” and the *Manual of Patent Office Practice* section 12.02).

The purposive construction of a claim is carried out in light of the whole of the specification and takes into account what the person skilled in the art would understand from the whole of the specification to be the nature of the invention.

In view of statements in the description (paragraphs 0001-0010), the person skilled in the art to whom the application is directed, which may be a team of people, is skilled in the field of mobile devices, mobile applications, and mobile data management. The person skilled in the art is also skilled in the art of general purpose computing, cloud based computing, and cyber security.

This person’s common general knowledge (CGK) would include the use of computers, networks, computing devices, servers, databases, memories, and processors. Thus, the exchange of signals, or, in claim’s language, of “transmitting” and “communicating” within and between computer systems, including computers, computing devices, servers, processors, memories, databases, networks, and websites, is also part of the CGK. This person’s CGK would also include knowledge of administrative practices regarding personal identification.

The originally filed specification does not provide any details regarding the hardware and the software platforms used to develop the claimed invention. As such, they are considered conventional and part of the CGK.

As there is no indication otherwise in the claims, all elements of claims 1-21 are essential.

The examiner has identified the following defects in the application:

Subject Matter

Claims 1-21 define an actual invention that is excluded subject-matter under subsection 27(8) of the *Patent Act* and is not patentable subject-matter.

As is evident from the specification itself and the CGK, data exchanges within and between computer systems including computers, computing devices, memories, and processors in the form of signals, called in the claims “transmitting” and “communicating” represent generic input/output steps of a computer-implemented process. In such a case, all of the remaining essential elements correspond only to the processing of data to provide a scheme for providing data by means of a generic computer. It is important to note though that the mere fact that a computer is identified to be an essential element of the claimed invention does not necessarily mean that the subject-matter defined by the claims is patentable subject-matter and outside of the prohibition under subsection 27(8) of the *Patent Act*.

It is therefore necessary to ascertain whether the computer forms part of the actual invention. There is no evidence in the originally filed specification that the problem that is solved by a scheme for providing data is a computer problem. In the present case, the computing device processes the instructions for the scheme in a well-known manner. From the specification, it is clear that the processing of the instructions for the scheme on the computer does not solve any problems in the functioning of the computer. Thus, the computing device and the scheme do not form part of a single actual invention that solves a problem related to the manual or productive arts. As the disclosure is focused on the scheme for providing data, the actual invention is considered to be the scheme per se, which has no physical existence and does not manifest a discernible physical effect or change.

Independent claim 15 represents the scheme, directed to a set of steps for providing data comprising:

1. associating a security policy with each of a plurality of supported namespaces on a mobile device (storage of data), each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS) (administrative policy);
2. transmitting a list of supported namespaces and the security policy of each of the plurality of supported namespaces to a reader connected to a verifier (input and output of data);
3. selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces (analysis of data), and transmitting from the reader to the mobile device, a list containing the candidate namespaces (input and output of data);
4. transmitting to the reader by the mobile device, the security policy associated with each of the selected candidate namespaces (input and output of data);
5. operating the verifier to:
    a) determine for which of the candidate namespaces the verifier can satisfy corresponding access rules of the security policy of the namespace (analysis of data); and
    b) if the verifier can satisfy the corresponding access rules of the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which a verifier terminal can satisfy the corresponding access rules of the security policy, to access a data item, and demonstrating satisfaction of the corresponding access rules of the

security policy to the mobile device (input and output of data);

c) if the verifier cannot satisfy the corresponding access rules of the security policy of any of the candidate namespaces, rejecting access to the data item (input and output of data); and
d) upon successful demonstration by the reader to the mobile device of satisfaction of the corresponding access rules of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader (input and output of data).

As the method is directed to providing data by determining the potential relevance of the data based on its label, and requiring the requestor of the data to satisfy a corresponding security policy (both well known functions of general computers), there is no evidence that the functioning of the computer is being improved by the disclosed method, and no physical steps outside of the computer are present. None of the dependent, or other independent, claims add physicality to the subject matter.

Obviousness

Claims 1-21 do not comply with section 28.3 of the *Patent Act*. These claims are directed to subject-matter that lacks an inventive step and would have been obvious at the claim date to a person skilled in the art or science to which it pertains having regard to either D1 or D2, in view of D4 or D5, and the common general knowledge.

Regarding independent claim 1, D3 discloses a mobile driver's license (mDL) (2.1 Functional Requirement Summary), which may be stored in an electronic wallet on a mobile device (2.13 Wallet Solutions), and electronically secured so that the personally identifiable information related to the mDL is only when certain conditions are met (2.6 Data Privacy and Protection). D3 is a White Paper, outlining requirements for digital identity systems (1. Introduction), and forms part of the common general knowledge. One skilled in the art would therefore look to prior art documents D1, D2, or D4 for implementation. D4 discloses a method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:

- associating security policies (paragraphs 0008-0017, claim 1) with each of a plurality of supported namespaces on the mobile device (paragraph 0009), each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS) (implicit to all namespaces representing IDs, as each ID will either satisfy or not the level of security set by the authority using the reader; see claim 1, abstract: "plastic id cards, such as driver license, health insurance and others"); and
- operating a reader executing a reader module (claim 7) to communicate with the mobile device and to select a namespace satisfying a required level of security (LOS) 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 (paragraph 0013: "the invention may provide a user with the capability of sharing information with other users from within their own--MyPIDs---virtual folder. Moreover, a user may have the capability to define and individually control other users rights to data contained to be shared. The invention will be provided with read only access to prevent remote users affect others files placed in--MyPIDs--folder.").

While D4 does not explicitly disclose selecting a namespace satisfying a required level of security (LOS) 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, this is an obvious design choice; based on the requirements set in D3, the reader should not select a namespace that does not meet its own level of security, as this personal information is not relevant to the reader.

D1 discloses a similar method (paragraphs 0005-0008, 0021-0034, fig. 1, 2), as does D2 (abstract, page 1 line 25-page 3 line 18, page 6 line 28-page 13 line 32, fig. 1, 2, 3A, 3B). D1 and D2 do not disclose the use of namespaces, however, D4 demonstrates the use of namespaces for representing the stored data in a mobile wallet (paragraph 0009). For the sake of completeness, it is noted that D5 discloses the use of namespaces for security purposes in mobile wallet applications (abstract, paragraphs 0040-0045). Claim 1 is therefore obvious.

Independent claim 11 recites a mobile device corresponding to the method of claim 1, and is obvious for the same reasons. The additional feature of using a defined bytestring template is simply a design choice; bytestrings are well known in the art. Claim 11 is therefore obvious.

Regarding independent claim 15, this claim recites the same subject matter as claim 1, which is discussed above. The additional features recited in claim 15 are obvious, as the steps of:

- determining for which of the candidate namespaces the verifier can satisfy corresponding access rules of the security policy of the namespace; and
- if the verifier can satisfy the corresponding access rules of the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which a verifier terminal can satisfy the corresponding access rules of the security policy, to access a data item, and demonstrating satisfaction of the corresponding access rules of the security policy to the mobile device;
- if the verifier cannot satisfy the corresponding access rules of 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 corresponding access rules of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader,

are all obvious design choices. One skilled in the art would consider it to be a requirement that the data items stored in an electronic identification (eID) wallet are only released when 1) the requestor can determine that the data items are relevant and 2) that the requestor can meet data security requirements, as each of documents D1-D5 pertain to personally identifiable information. Claim 15 is therefore obvious.

Regarding dependent claims 2-10, 12-14, and 16-21 these claims do not add anything of inventive significance to the subject matter of their independent claims because they represent further implementation details which would fall within the normal competence of a skilled person, or would become apparent to that person following from the teachings of D1 or D2, in view of D4 or D5, and the common general knowledge in the art.

Claim Defects

Claim 15 has been drafted as an independent claim and does not comply with subsection 63(1) of the *Patent Rules*. Said claim includes at least all of the features of claim 1, and consequently must refer thereto, in consideration of subsection 63(2) of the *Patent Rules*, and define only the

additional features claimed.

Examiner Requisitions

In view of the foregoing defects, the applicant is requisitioned, under subsection 86(2) of the *Patent Rules*, to amend the application in order to comply with the *Patent Act* and the *Patent Rules* or to provide arguments as to why the application does comply.

Under section 102 of the *Patent Rules*, any amendment made in response to this requisition must be accompanied by a statement explaining the purpose of the amendment and identifying the differences between the new page and the replaced page.

Phoenix Bard-Cavers
Patent Examiner
873-354-9901

As per CIPO Client Service Standards, a response to a telephone enquiry or voice mail should be provided by the end of the next business day. In the event that attempts to reach the examiner are unsuccessful, the examiner's Section Head, Chaza Nasrallah, can be reached at 819-635-4148.

For general inquiries: 1-866-997-1936 or for more options see http://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/wr00006.html.

CIPO values your feedback and invites you to complete a short and anonymous ongoing survey on patent examination products and services. You can access the survey at the following link: https://form.simplesurvey.com/f/s.aspx?s=91e23402-ee27-4868-a230-ab5c819f9d1c.

The Examination Search Report is provided for reference only and is not part of any requisition made by the examiner in accordance with the *Patent Act* or *Rules*. The applicant is not required to respond to the information contained in the Examination Search Report.

Examination Search Report

Box I: General Information			
Application No.	3,154,428	Search Report Date	2025-01-15
Title	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		
Examiner	Phoenix Bard-Cavers	Search Conducted?	Yes

Box II: Family Prosecution		
Family Member	File Wrapper Reviewed	Status of Prosecution
WO2021073853A1	2025-01-15	Completed
US2022374533A1	2025-01-14	In Progress
EP3809358A1	2025-01-14	Abandoned
EP4046126A1	2025-01-14	Not Started
AU2020367942A8	2025-01-15	Abandoned
AU2024201900A1	2025-01-14	Not Started
KR20220082904A	NO	

Box III: Search History			
Claims Searched	1, 11, 15	Date of Search	2025-01-14

Type of Search Conducted (select all that apply):

Canadian first to file search	■	Supplemental/top up search	■
Inventor/applicant search	□	Non laid open search	□
Comprehensive search	□	In-house searcher	□

Search History from Databases Consulted:

```
##### CANADIAN PATENT DATABASE/INTELLECT ##########

1 1222 filing-date:[2015-09-25 TO 2021-12-10] AND ipc:(G06Q\ 50/26 OR G06Q\
20/32 OR G06Q\ 20/36 OR G06F\ 21/62 OR G06F\ 21/30)

2 257 (filing-date:[2015-09-25 TO 2021-12-10] AND ipc:(G06Q\ 50/26 OR G06Q\
20/32 OR G06Q\ 20/36 OR G06F\ 21/62 OR G06F\ 21/30)) AND (namespace OR name-
space OR "name space")
```

```
3 75 ((filing-date:[2015-09-25 TO 2021-12-10] AND ipc:(G06Q\ 50/26 OR G06Q\
20/32 OR G06Q\ 20/36 OR G06F\ 21/62 OR G06F\ 21/30)) AND (namespace OR name-
space OR "name space")) AND (wallet)

4 65 (((filing-date:[2015-09-25 TO 2021-12-10] AND ipc:(G06Q\ 50/26 OR G06Q\
20/32 OR G06Q\ 20/36 OR G06F\ 21/62 OR G06F\ 21/30)) AND (namespace OR name-
space OR "name space")) AND (wallet)) AND (mobile AND secur*)

5 61 ((((filing-date:[2015-09-25 TO 2021-12-10] AND ipc:(G06Q\ 50/26 OR
G06Q\ 20/32 OR G06Q\ 20/36 OR G06F\ 21/62 OR G06F\ 21/30)) AND (namespace OR
name-space OR "name space")) AND (wallet)) AND (mobile AND secur*)) AND
(identification OR "ID")

6 22 (((((filing-date:[2015-09-25 TO 2021-12-10] AND ipc:(G06Q\ 50/26 OR
G06Q\ 20/32 OR G06Q\ 20/36 OR G06F\ 21/62 OR G06F\ 21/30)) AND (namespace OR
name-space OR "name space")) AND (wallet)) AND (mobile AND secur*)) AND
(identification OR "ID")) AND (licence OR license)

7 1 ((((((filing-date:[2015-09-25 TO 2021-12-10] AND ipc:(G06Q\ 50/26 OR
G06Q\ 20/32 OR G06Q\ 20/36 OR G06F\ 21/62 OR G06F\ 21/30)) AND (namespace OR
name-space OR "name space")) AND (wallet)) AND (mobile AND secur*)) AND
(identification OR "ID")) AND (licence OR license)) AND (namespace)

##### QUESTEL-ORBIT ##########

1 1 (CA3154428)/PN/AP/PR

2 100 SIMILARITY SEARCH  93724460 MAXSIM 100

3 42 2 AND (WALLET)/TI/AB/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX

4 476 ((WALLET)/TI/AB/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX AND
(MOBILE)/TI/AB/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX AND
(NAMESPACE)/TI/AB/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX)

5 455 ((WALLET)/TI/AB/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX AND
(MOBILE)/TI/AB/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX AND
(NAMESPACE)/TI/AB/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX AND
(IDENTIFICATION)/TI/AB/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX)

6 155 (((WALLET)/TI/AB/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX AND
(MOBILE)/TI/AB/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX AND
(NAMESPACE)/TI/AB/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX AND
(IDENTIFICATION)/TI/AB/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX) AND (EPD < 2019-10-
19))

##### GOOGLE ##########
```

1 ~420 ISO/IEC CD2 18013-5:2019, Personal Identification — ISO-Compliant Driving Licence — Part 5: Mobile Driving Licence (mDL) application

2 ~103 aamva mdl implementation guidelines (Before Oct 18, 2019)

3 ~4280 Mobile Driver’s License (mDL) implementation (Before Oct 18, 2019)

CIPO Search Record - Version 10

008
R

General Correspondence (Patent)

Date: June 11, 2024 4:45:38 PM

Application Number

3154428

Title of invention

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Applicant(s) or Inventor Name(s)

Applicant or Inventor Name

Sender

Family Name:
First Name:
Initial:
Name of Corporation or Firm: ROBIC
Address Line 1: 630 Rene-Levesque West Boulevard
Address Line 2: 20th Floor
Address Line 3:
City/Town: Montreal
Province/State: Québec
Country: Canada
Postal/Zip Code: H3B 1S6
Telephone Number: (514) 987-6242
Fax Number: (514) 845-7874
Email Address: opic.brevets@robic.com
Communicate by: Electronic Mail (Non secure)

Date Reçue/Date Received 2024-06-11

Correspondence Instructions

Commissioner, please find enclosed the following documents in response to the Examination Report issued on February 14, 2024, with respect to the present patent application: response letter, pages 17 to 21 of the description, claims 1 to 21 and marked-up copy of the claims. Respectfully submitted,

Description of Fee

No fee has been entered.
Total Fee Payment: $0.00

Payment method

No Charge

Attachments

1. 2024-06-11 Response letter - 014211-0023.pdf
Other
Response to the Examination Report

2. 2024-06-11 Description pages 17 to 21 - 014211-0023.pdf
Description
Pages 17 to 21 of the description

3. 2024-06-11 Amended claims (21) - 014211-0023.pdf
Claim
Claims 1 to 21

4. 2024-06-11 Marked-up claims - 014211-0023.pdf
Other
Claims 1 to 21 (Marked-up)

Transmission Identifier: pgc_MarieLouissaint1_20240611164538767

Date: June 11, 2024 4:45:38 PM

Commissioner of Patents
50 Victoria Street
Place du Portage
Phase I
Gatineau, Quebec
Canada
K1A 0C9

Application Number: 3154428
Title of invention: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
Applicant(s) or Inventor(s) Name(s): THALES DIS FRANCE SAS
THALES DIS FRANCE SAS
Reference Number: 014211-0023

Instructions: Commissioner, please find enclosed the following documents in response to the Examination Report issued on February 14, 2024, with respect to the present patent application: response letter, pages 17 to 21 of the description, claims 1 to 21 and marked-up copy of the claims. Respectfully submitted,

Attached are the following documents:
1. 2024-06-11 Response letter - 014211-0023.pdf
Response to the Examination Report
Other
2. 2024-06-11 Description pages 17 to 21 - 014211-0023.pdf
Pages 17 to 21 of the description
Description
3. 2024-06-11 Amended claims (21) - 014211-0023.pdf
Claims 1 to 21
Claim
4. 2024-06-11 Marked-up claims - 014211-0023.pdf
Claims 1 to 21 (Marked-up)
Other

,
ROBIC
630 Rene-Levesque West Boulevard
20th Floor
Montreal
Québec
Canada
H3B 1S6
Tel: (514) 987-6242

Date Reçue/Date Received 2024-06-11

Fax: (514) 845-7874
Email:opic.brevets@robic.com

Transmission Identifier: pgc_MarieLouissaint1_20240611164538767

Date Reçue/Date Received 2024-06-11

ROBIC
1892

June 11, 2024

CANADIAN INTELLECTUAL PROPERTY OFFICE

Inventor(s):	FAHER, Mourad et al.
Applicant(s):	THALES DIS FRANCE SAS
Patent application N° :	3.154.428
Title:	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
Our file.:	014211-0023

COMMISSIONER OF PATENTS
GATINEAU, QUEBEC, K1A 0C9

RESPONSE TO A NOTICE UNDER SUBSECTION 86(2) OF THE *PATENT RULES*

Commissioner:

In response to the Examination Report of February 14, 2024, please amend the above-identified patent application as follows.

IN THE DESCRIPTION:

Please cancel page 17 presently on file and substitute therefor enclosed new pages 17 to 21.

IN THE CLAIMS:

Please cancel the set of claims presently on file, and substitute therefor the enclosed new set of 21 claims.

REMARKS

Please examine the present patent application in view of the following remarks.

Modifications to the description

The description has been amended to reflect the subject matter as claimed.

Modifications to the claims

The claims are amended to better define the subject matter of the claims and/or for clarity

ROBIC
www.robic.ca
info@robic.com

MONTREAL
630 René-Lévesque Boulevard West
20th Floor
Montreal, Quebec, Canada H3B 1S6
Tel.: +1 514 987-6242 Fax: +1 514 845-7874

QUEBEC
Le Delta Building
2875 Laurier Boulevard, Delta 3 - suite 700
Quebec, Quebec, Canada G1V 2M2
Tel.: +1 418 653-1888 Fax.: +1 418 653-0006

Date Reçue/Date Received 2024-06-11

purposes.

More specifically, independent claim 1 is hereby amended to recite:

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 the mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS); and

operating a reader executing a reader module to communicate with the mobile device and to select a namespace satisfying a required level of security (LOS) 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.

Independent claim 11 is amended to now recite:

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 request for supported namespaces from a reader;

transmit a list of supported name spaces to the reader;

receive a list of selected namespaces satisfying a required level of security (LOS) from the reader; and

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.

Independent claim 15 (former claim 16) is amended to now recite:

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

associating a security policy with each of a plurality of supported namespaces on a mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS);

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

selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) 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 verifier to:

determine for which of the candidate namespaces the verifier can satisfy corresponding access rules of the security policy of the namespace; and

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

if the verifier cannot satisfy the corresponding access rules of 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 corresponding access rules of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

Former claim 12 is deleted, the content of which now being included in independent claim 11. The claim numbering and claim dependencies are adjusted accordingly.

New dependent claims 16-21 are added and depend from claim 15 which is now drafted as an independent claim.

Additional amendments are performed throughout the claims to take into account the above noted amendments and/or to correct or prevent clarity issue in the claims.

The Applicant submits that the present amendments are made solely to facilitate prosecution of the present application, without any admission regarding the characterization of the claims.

A marked-up copy of the set of claims which details each of the amendments made to the claims

is enclosed for the Examiner's convenience.

Lack of support

In response to the examination report, independent claims 1, 11 and 15 are hereby amended as described in more details below.

In view of the present amendments independent claim 1 now explicitly recites at least the features of "*each of the plurality of supported namespaces either satisfy or not satisfy a level of security (LOS)"* and "*selecting a namespace satisfying a required level of security (LOS)".*

Independent claim 11 now explicitly recites at least the feature of *"receiving a list of selected namespaces satisfying a required level of security (LOS) from the reader".*

Independent claim 15 now explicitly recites the at least the features of *"each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS)"* and *"selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces".*

In view of the above, independent claims 11, 15 and 11 now explicitly recite the LOS, which is specific coding of security conditions that cannot be by default bore by labels because labels are not structures or containers pre-determined by existing standards, with known (to the skilled person in the art) fields or sub-containers dedicated to host security rules with known coding language, etc. as detailed in the previously submitted response.

At least in view of the present amendments, the Applicant respectfully submits that amended claims 1, 11 and 15 provide the information regarding the relationship between the security policies (or the details of the policies), and data items stored on the mobile device. The Applicant respectfully submits that amended claims 1, 11 and 15 also define the configuration by identification data issuers of security rules applying to data, which the Examination report deemed absent from former claims 1, 11 and 16 and on which the Examination report relied for rejecting the previously submitted arguments regarding non-obviousness of the claims.

The Applicant submits that the previously submitted arguments therefore apply regarding novelty and/or obviousness to the currently standing claims. Consequently, the Applicant submits that independent claims 1, 11 and 15 are new and non-obvious in view of the previously cited prior art documents, at least in view of the remarks submitted in the previous response. Dependent claims

2-10, 12-14 and 16-21 depend directly or indirectly from one of claims 1-, 11 and 15 and are also new and non-obvious at least in view of their dependencies.

Reply to the rejections raised under section 60 of the *Patent Rules and* subsection 27(4) of the *Patent Act*

The Applicant has noted the rejection of former claims 1, 11 and 16 for allegedly lacking support as they are allegedly directed to the desired result rather than to the combination necessary to achieve that result.

The Applicant has also noted the rejections of former claims 1, 11 and 16 for allegedly being unclear in view of the above-mentioned rejection based on the alleged lack of support.

At least in view of the present amendments, the Applicant respectfully submits that amended claims 1, 11 and 15 recite the combination of features necessary to achieve the result and are therefore fully supported by the description.

In view of the present amendment, it is clear in independent claim 1 that the reader selects a namespace based on the namespace satisfying a required level of security (LOS), thereby satisfying the requirements of section 60 of the *Patent Rules*.

Regarding independent claim 11, the claim now includes the features of former claim 12, which where indicated in the Examination report as providing the required details as to how the reader selects namespaces. Furthermore, the claim recites *"receive a list of selected namespaces satisfying a required level of security (LOS) from the reader"* further defining how the reader selects namespaces and thereby satisfying the requirements of section 60 of the *Patent Rules*.

.Regarding independent claim 15, it is clear in independent claim 15 that the reader selects a namespace based on the namespace satisfying a required level of security (LOS), thereby satisfying the requirements of section 60 of the *Patent Rules*.

Furthermore, claim 15 is amended to recite *"transmitting a list of supported namespaces and the security policy of each of the plurality of supported namespaces to a reader connected to a verifier"* prior to *"selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces"* such that the list of supported namespaces is

available to the verifier for selection of the at least one of the namespaces.

Finally, claim 15 is amended to clarify that the *verifier* is responsible for satisfying the *corresponding access rules of the security policy* thereby reciting how the security policy is satisfied (by satisfying the corresponding access rules of the security policy) and alleviating any confusion between which of the reader or the verifier is responsible for satisfying the corresponding access rules of the security policy.

In view of the above, the Applicant respectfully submits that claim 1, 11 and 15 comply with section 60 of the *Patent Rules* and respectfully requests withdrawal of the objections. The applicant also submits that amended claims 1, 11 and 15 are clear and respectfully request withdrawal of the rejections under subsection 27(4) of the *Patent Act* relative to these claims.

Reply to the rejections raised under subsection 27(4) of the *Patent Act*

In response to the Examiner's objections under subsection 27(4) of the *Patent Act*, the claims have been amended to correct the deficiencies identified by the Examiner.

More specifically, claim 15 (former claim 16) has been amended to be drafted as an independent claim, such that the rejection based on subsection 27(4) of the Patent Act is now moot.

Objected claim 12 is hereby deleted and the content included in claim 11 has been adjusted to prevent antecedent issue.

Objected Claim 4 and 12 (former claims 14) have been amended to correct the noted antecedent issues.

In view of the above, withdrawal of the rejections under subsection 27(4) of the *Patent Act* is thus respectfully requested.

Good standing

It is believed that the present application is in good standing. If, however, it appears that the application is deemed abandoned, or if CIPO considers that this application is deemed abandoned, we request that CIPO informs us in writing immediately.

Should the amount(s) indicated in this letter be insufficient to cover all of the fee(s) for which payment(s) is(are) explicitly or implicitly requested by this letter, or if a fee payment cannot be

charged to the designated credit card, CIPO is hereby **unconditionally, clearly and unequivocally authorized** to debit any amount required to pay or complete any applicable fee from our deposit account **600000233**, in order to keep the present application in good standing.

CONCLUSION

In view of the above, it is submitted that all rejections and objections raised by the Examiner have been addressed and overcome by the present response and that the application now complies with the *Patent Act* and *Patent Rules.* Allowance of the claims and issuance of a Notice of Allowance are therefore respectfully solicited.

The Examiner is invited to call us if any further amendment will expedite allowance of the application or if the Examiner has any suggestions or questions concerning this application.

Respectfully submitted,



ROBIC AGENCE PI S.E.C. / ROBIC IP AGENCY LP
Patent and Trademark agents

Patent Agent : Vincent Boucher
+1 514 987-8897

Contact Patent Agent: Jean-Francois Journault
+1 418 653-1829

VBO/JFJ/mlt

Encl. new pages 17 to 21 of the description;
new set of 21 claims; and
marked-up copy of the set of claims.

[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] The following aspects are also disclosed herein:

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 the mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS); and

operating a reader executing a reader module to communicate with the mobile device and to select a namespace satisfying a required level of security (LOS) 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 of aspect 1, comprising:

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

selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces satisfying the required level of security (LOS) 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 of aspect 1, comprising:

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

selecting, by the verifier module, at least one candidate namespace satisfying the required level of security (LOS) by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

4. The method of aspect 1 or 2, further comprising:

Date Reçue/Date Received 2024-06-11

prior to transmitting the list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that a 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 of any one of aspects 1 to 4, comprising:

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

6. The method of any one of aspects 1 to 5, 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 of any one of aspects 1 to 6, wherein a 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 of aspect 1, further comprising 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 a verifier associates with each namespace in the plurality of supported namespaces.

9. The method of any one of aspects 1 to 8, further comprising 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 of aspect 1, 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

Date Reçue/Date Received 2024-06-11

comprising operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to a 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 request for supported namespaces from a reader;

transmit a list of supported namespaces to the reader;

receive a list of selected namespaces satisfying a required level of security (LOS) from the reader; and

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 aspect 11, wherein the eID wallet application further comprises instruction to cause the processor to:

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

13. The mobile device of aspect 11 or 12, 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 the reader connected to a verifier.

14. The mobile device of aspect 11, 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.

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

Date Reçue/Date Received 2024-06-11

associating a security policy with each of a plurality of supported namespaces on a mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS);

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

selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) 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 verifier to:

determine for which of the candidate namespaces the verifier can satisfy corresponding access rules of the security policy of the namespace; and

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

if the verifier cannot satisfy the corresponding access rules of 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 corresponding access rules of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

16. The method of aspect 15, wherein selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces is performed 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.

17. The method of aspect 15, wherein selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces is performed by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

18. The method of any one of aspects 15 to 17, further comprising:

Date Reçue/Date Received 2024-06-11

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

19. The method of any one of aspects 15 to 18, 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.

20. The method of any one of aspects 15 to 19, wherein a required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

21. The method of aspect 15, 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 a verifier terminal.

Date Reçue/Date Received 2024-06-11

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 the mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS); and

operating a reader executing a reader module to communicate with the mobile device and to select a namespace satisfying a required level of security (LOS) 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 of claim 1, comprising:

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

selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces satisfying the required level of security (LOS) based on confidence the verifier assigns to the namespace, whitelisting or

Date Reçue/Date Received 2024-06-11

blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.

3. The method of claim 1, comprising:

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

selecting, by the verifier module, at least one candidate namespace satisfying the required level of security (LOS) by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

4. The method of claim 1 or 2, further comprising:

prior to transmitting the list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that a 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 of any one of claims 1 to 4, comprising:

Date Reçue/Date Received 2024-06-11

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

6. The method of any one of claims 1 to 5, 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 of any one of claims 1 to 6, wherein a 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 of claim 1, further comprising 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 a verifier associates with each namespace in the plurality of supported namespaces.

9. The method of any one of claims 1 to 8, further comprising 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

Date Reçue/Date Received 2024-06-11

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 of claim 1, 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 a 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 request for supported namespaces from a reader;

transmit a list of supported namespaces to the reader;

receive a list of selected namespaces satisfying a required level of security (LOS) from the reader; and

Date Reçue/Date Received 2024-06-11

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 11, wherein the eID wallet application further comprises instruction to cause the processor to:

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

13. The mobile device of claim 11 or 12, 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 the reader connected to a verifier.

Date Reçue/Date Received 2024-06-11

14. The mobile device of claim 11, 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.

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

associating a security policy with each of a plurality of supported namespaces on a mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS);

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

selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) 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 verifier to:

Date Reçue/Date Received 2024-06-11

determine for which of the candidate namespaces the verifier can satisfy corresponding access rules of the security policy of the namespace; and

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

if the verifier cannot satisfy the corresponding access rules of 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 corresponding access rules of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.

16. The method of claim 15, wherein selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces is performed 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.

17. The method of claim 15, wherein selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces is performed by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

18. The method of any one of claims 15 to 17, further comprising:

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

19. The method of any one of claims 15 to 18, 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.

Date Reçue/Date Received 2024-06-11

20. The method of any one of claims 15 to 19, wherein a required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

21. The method of claim 15, 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 a verifier terminal.

Date Reçue/Date Received 2024-06-11

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~~ the mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS); and

operating a reader executing a reader module to communicate with the mobile device and to select a namespace satisfying a required level of security (LOS) 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 of claim 1, comprising:

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

selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces satisfying the required level of security (LOS) based on confidence the verifier assigns to the namespace, whitelisting or

Date Reçue/Date Received 2024-06-11

blacklisting of namespaces, or overhead associated with satisfying the security policy of a namespace.

3. The method of claim 1, comprising:

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

selecting, by the verifier module, at least one candidate namespace satisfying the required level of security (LOS) by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

4. The method of claim 1 or 2, further comprising:

prior to transmitting ~~a~~ the list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that ~~the~~ a 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 of any one of claims 1 to 4, comprising:

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

6. The method of any one of claims 1 to 5, 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 of any one of claims 1 to 6, wherein a 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 of claim 1, further comprising 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 a verifier associates with each namespace in the plurality of supported namespaces.

9. The method of any one of claims 1 to 8, further comprising 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

Date Reçue/Date Received 2024-06-11

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 of claim 1, 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 a 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 request for supported namespaces from a reader;

transmit a list of supported namespaces to the reader;

receive a list of selected namespaces -satisfying a required level of security (LOS) from thea reader; and

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 11, 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.~~12. The mobile device of claim 11 ~~or 12~~, wherein the eID wallet application further comprises instruction to cause the processor to:

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

~~14.~~13. The mobile device of ~~any one of claims 11 to 13~~claim 11 or 12, 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~~ the reader connected to a verifier.

~~15.~~14. The mobile device of claim 11 ~~or 12~~, 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.~~15. A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device ~~in accordance with any one of claims 1 to 15~~, the method comprising:

associating a security policy with each of a plurality of supported namespaces on a mobile device, each of the plurality of supported namespaces either satisfying or not satisfying a level of security (LOS);

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

selecting, by the ~~reader~~verifier, at least one of the namespaces satisfying a required level of security (LOS) 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~~ verifier to:

determine for which of the candidate namespaces the ~~reader~~ verifier can satisfy corresponding access rules of the security policy of the namespace; and

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

if the verifier cannot satisfy the corresponding access rules of 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 corresponding access rules of the security policy

of the selected namespace, granting access to the data item by the mobile device to the reader.

16. The method of claim 15, wherein selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces is performed 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.

17. The method of claim 15, wherein selecting, by the verifier, at least one of the namespaces satisfying a required level of security (LOS) as candidate namespaces is performed by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.

18. The method of any one of claims 15 to 17, further comprising:

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

Date Reçue/Date Received 2024-06-11

19. The method of any one of claims 15 to 18, 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.

20. The method of any one of claims 15 to 19, wherein a required authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

21. The method of claim 15, 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 a verifier terminal.

Date Reçue/Date Received 2024-06-11

14 February 2024 (14-02-2024)

ROBIC AGENCE PI S.E.C./ROBIC IP AGENCY LP
opic.brevets@robic.com

Application No.	:	**3,154,428**
PCT No.	:	**EP2020076906**
Owner	:	THALES DIS FRANCE SAS
Title	:	**SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES**
Classification	:	G06F 21/62 (2013.01)
Your File No.	:	**014211-0023**
Examiner	:	Phoenix Bard-Cavers

YOU ARE HEREBY NOTIFIED OF A REQUISITION BY THE EXAMINER IN ACCORDANCE WITH SUBSECTION 86(2) OF THE *PATENT RULES*. IN ORDER TO AVOID ABANDONMENT UNDER PARAGRAPH 73(1)(*a*) OF THE *PATENT ACT*, A WRITTEN REPLY MUST BE RECEIVED WITHIN **FOUR (4)** MONTHS AFTER THE ABOVE DATE.

The applicant's letter of 25 August 2023 (25-08-2023) has been received and the application has been examined having regard to the applicant's arguments. However, the examiner considers that the application still does not comply with the *Patent Act* or *Patent Rules*.

The number of claims in this application is 16.

Response to Applicant's Correspondence

The applicant's remarks of 25 August 2023 (25-08-2023) have been considered, but are not persuasive. The applicant states that "the claimed subject matter defines the configuration by identification data issuers of security rules applying to data, which are determined at the mobile interface only by their names or labels", in order to support the argument that the subject matter is more that an administrative policy. The applicant also states that "the feature so-called LOS (i.e., level of security) is not just an administrative accreditation to access data, but it is in practice a specific coding of security conditions that cannot be by default bore by labels because labels are not structures or containers pre-determined by existing standards, with known (to the skilled person in the art) fields or sub-containers dedicated to host security rules with known coding language, etc. So, this one aspect is where the claimed subject matter is laid: informing about security mechanisms attached to unstructured labels or names that are not files, dedicated files, data objects, records, byte strings or so".

These arguments cannot be followed. First, the feature of "level of security (LOS)" is not found in the claims, and cannot be used be used to limit their scope. Second, the claims are given their broadest reasonable interpretation; the applicant's arguments define a scope narrower

than the wording of the claims suggests. For example, claim 1 recites 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.

Namespaces are commonly known in the art as a namespace is a set of signs (names) that are used to identify and refer to objects of various kinds. Merely "associating" security policies with each of a plurality of supported namespaces encompasses many possibilities, including the basic administration of allowing specific namespaces to allow access to data. No information regarding the relationship between the security policies (or the details of the policies), and data items stored on the mobile device is recited, and so the claims encompass the embodiment of basic administration. There is no indication of LOS or security conditions in the claims.

The feature "the configuration by identification data issuers of security rules applying to data" also appears absent in the claims.

In light of the newly identified non-compliance with subsection 27(4) of the *Patent Act* and section 60 of the *Patent Rules*, further examination of the claims with regard to novelty and obviousness has been deferred, as the applicant appears to rely on features absent from the claims to support their arguments for inventiveness.

The examiner has identified the following defects in the application:

Lack of Support

Claims 1, 11, and 16 are not fully supported by the description and do not comply with section 60 of the *Patent Rules*. The claimed subject matter is directed to the desired result rather than to the combination necessary to achieve that result as described in the description. Specifically, claim 1 recites "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"; it is unclear how the reader selects a namespace to access a data item based on the security policies associated with the plurality of supported namespaces, as the specifics of the security policies are recited in the claims, or how the security policies are assessed in order for a namespace to be selected. In claim 11, it is unclear how the reader selects namespaces (this appears to later be recited in claim 12), and in claim 16 it is unclear how the reader selects namespaces, as only security policies are transmitted to the reader before this step. Further, the steps of 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 a 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",

are unclear; is the reader or verifier responsible for satisfying the security policy? This claim also fails to recite how the security policy is satisfied: no details regarding the determination are recited.

Claim Defects

Claims 1, 11, and 16 are indefinite and do not comply with subsection 27(4) of the *Patent Act*. Given the lack of support discussed above, the claims are unclear.

Claim 16 is indefinite and does not comply with subsection 27(4) of the *Patent Act*. This claims recites "an electronic identification (eID) wallet on a mobile device in accordance with any one of claims 1 to 15" (lines 2-3); this is unclear, as claims 1-10 are directed to a method, and claims 11-15 are directed to a mobile device. When one claim refers to another, it must include all the features and elements of the claim to which it refers, not a portion thereof.

Claim 12 is indefinite and does not comply with subsection 27(4) of the *Patent Act*. The element "reader" (claim 12, line 3), is defined with an indefinite article, causing a lack of clarity as to whether it is intended to refer to the same element "reader" as was previously defined in the claims (claim 11) or an additional element thereto.

Claims 4 and 13 are indefinite and do not comply with subsection 27(4) of the *Patent Act*. The following terms have no antecedents: "user" (claims 4 and 13, lines 3 and 4 respectively) and "supported namespaces" (claim 13, line 3). It is unclear whether the "user" is intended to be the same entity as the "operator" introduced in claim 3 (which claim 4 does not depend upon). Additionally, claim 13 is dependent upon either one of claim 11 or 12 and refers to "supported namespaces", however, this term is only introduced properly in claim 12; it is unclear whether these supported namespaces in claim 13 are meant to be the same as those in claim 12. Claim 13 is further unclear, as the step of "transmitting a list of supported namespaces to a reader" is only introduced in claim 12.

Examiner Requisitions

In view of the foregoing defects, the applicant is requisitioned, under subsection 86(2) of the *Patent Rules*, to amend the application in order to comply with the *Patent Act* and the *Patent Rules* or to provide arguments as to why the application does comply.

Under section 102 of the *Patent Rules*, any amendment made in response to this requisition must be accompanied by a statement explaining the purpose of the amendment and identifying the differences between the new page and the replaced page.

Phoenix Bard-Cavers
Patent Examiner
873-354-9901

As per CIPO Client Service Standards, a response to a telephone enquiry or voice mail should be provided by the end of the next business day. In the event that attempts to reach the examiner are unsuccessful, the examiner's Section Head, Chaza Nasrallah, can be reached at 819-635-4148.

For general inquiries: 1-866-997-1936 or for more options see http://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/wr00006.html.

CIPO values your feedback and invites you to complete a short and anonymous ongoing survey on patent examination products and services. You can access the survey at the following link: https://form.simplesurvey.com/f/s.aspx?s=91e23402-ee27-4868-a230-ab5c819f9d1c.

3154428B_PBC.docm

The Examination Search Report is provided for reference only and is not part of any requisition made by the examiner in accordance with the *Patent Act* or *Rules*. The applicant is not required to respond to the information contained in the Examination Search Report.

Examination Search Report

Box I: General Information

Application No.	3,154,428	Search Report Date	2024-02-13
Title	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		
Examiner	Phoenix Bard-Cavers	Search Conducted?	No
No search was conducted for the following reasons :			
- Search deferred - see report for reasoning (lack of unity, excluded subject matter etc.)			N/A
- Relied on previous search results (CIPO and/or by Foreign Office)			Yes

Box II: Family Prosecution

Family Member	File Wrapper Reviewed	Status of Prosecution
WO2021073853A1	2024-02-13	Completed
US2022374533A1	2024-02-12	Not Started
EP3809358A1	2024-02-13	Abandoned
EP4046126A1	2024-02-12	Not Started
AU2020367942A8	2024-02-12	In Progress

Box III: Search History

No Search Conducted

CIPO Search Record - Version 10

008
mw

General Correspondence (Patent)

Date: August 25, 2023 2:49:58 PM

Application Number

3154428

Title of invention

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Applicant(s) or Inventor Name(s)

Applicant or Inventor Name

Sender

Family Name:
First Name:
Initial:
Name of Corporation or Firm: ROBIC S.E.N.C.R.L / LLP
Address Line 1: 630 Rene-Levesque West Boulevard
Address Line 2: 20th Floor
Address Line 3:
City/Town: Montreal
Province/State: Québec
Country: Canada
Postal/Zip Code: H3B 1S6
Telephone Number: (514) 987-6242
Fax Number: (514) 845-7874
Email Address: opic.brevets@robic.com
Communicate by: Electronic Mail (Non secure)

Date Reçue/Date Received 2023-08-25

Correspondence Instructions

Commissioner, please find enclosed the following documents in response to the Examination Report issued on May 16, 2023, with respect to the present patent application: response letter, pages 1 to 20 of the description, claims 1 to 16 and marked-up copy of the claims. Respectfully submitted,

Description of Fee

No fee has been entered.
Total Fee Payment: $0.00

Payment method

No Charge

Attachments

1. 2023-08-25 Response letter - 014211-0023.pdf
Other
Response to the Examination Report

2. 2023-08-25 Amended pages 1 to 20 of the description - 014211-0023.pdf
Description
Pages 1 to 20 of the description

3. 2023-08-25 Amended set of claims (16) - 014211-0023.pdf
Claim
Claims 1 to 16

4. 2023-08-25 Marked-up claims - 014211-0023.pdf
Other
Claims 1 to 16 (Marked-up)

Transmission Identifier: pgc_MarieLouissaint1_20230825144958502

Date: August 25, 2023 2:49:58 PM

Commissioner of Patents
50 Victoria Street
Place du Portage
Phase I
Gatineau, Quebec
Canada
K1A 0C9

Application Number: 3154428
Title of invention: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
Applicant(s) or Inventor(s) Name(s): THALES DIS FRANCE SAS
THALES DIS FRANCE SAS
Reference Number: 014211-0023

Instructions: Commissioner, please find enclosed the following documents in response to the Examination Report issued on May 16, 2023, with respect to the present patent application: response letter, pages 1 to 20 of the description, claims 1 to 16 and marked-up copy of the claims. Respectfully submitted,

Attached are the following documents:
1. 2023-08-25 Response letter - 014211-0023.pdf
Response to the Examination Report
Other
2. 2023-08-25 Amended pages 1 to 20 of the description - 014211-0023.pdf
Pages 1 to 20 of the description
Description
3. 2023-08-25 Amended set of claims (16) - 014211-0023.pdf
Claims 1 to 16
Claim
4. 2023-08-25 Marked-up claims - 014211-0023.pdf
Claims 1 to 16 (Marked-up)
Other

,
ROBIC S.E.N.C.R.L / LLP
630 Rene-Levesque West Boulevard
20th Floor
Montreal
Québec
Canada
H3B 1S6
Tel: (514) 987-6242

Date Reçue/Date Received 2023-08-25

Fax: (514) 845-7874
Email:opic.brevets@robic.com

Transmission Identifier: pgc_MarieLouissaint1_20230825144958502

Date Reçue/Date Received 2023-08-25

ROBIC
1892

August 25, 2023

CANADIAN INTELLECTUAL PROPERTY OFFICE

Inventors:	FAHER, Mourad et al.
Applicant:	THALES DIS FRANCE SAS
Patent application No.:	3.154.428
Title:	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
Our file:	014211-0023

COMMISSIONER OF PATENTS
GATINEAU, QUEBEC, K1A 0C9

RESPONSE TO A NOTICE UNDER SUBSECTION 86(2) OF THE *PATENT RULES*

Commissioner:

In response to the Examination Report of May 16, 2023, please amend the above-identified patent application as follows.

IN THE DESCRIPTION:

Please cancel pages 1 to 17 presently on file and substitute therefor enclosed new pages 1 to 20.

IN THE CLAIMS:

Please cancel the set of claims presently on file, and substitute therefor the enclosed new set of 16 claims.

REMARKS

Please examine the present patent application in view of the following remarks.

Modifications to the description and subsection 57(1) of the *Patent Rules*

The Applicant has taken note of the objection to the description under subsection 57(1) of the *Patent Rules*. In response, paragraph [0038] has been amended to remove a statement incorporating another document by reference. Reconsideration and withdrawal of the objection

ROBIC, LLP
www.robic.ca
info@robic.com

MONTREAL
630 René-Lévesque Boulevard West
20th Floor
Montreal, Quebec, Canada H3B 1S6
Tel.: +1 514 987-6242 Fax: +1 514 845-7874

QUEBEC
Le Delta Building
2875 Laurier Boulevard, Delta 3 - suite 700
Quebec, Quebec, Canada G1V 2M2
Tel.: +1 418 653-1888 Fax.: +1 418 653-0006

Date Reçue/Date Received 2023-08-25

under subsection 57(1) of the *Patent Rules* are respectfully requested.

The description has also been amended to insert statements reflecting the subject matter of the instant claims.

The Applicant submits a new version of all the pages of the description to ensure that all the pages are numbered consecutively in Arabic numerals beginning with the number "1".

Modifications to the claims

The Applicant submits an amended set of 16 claims for prosecution in the present application. The claim amendments can be seen in the enclosed version of the claims in tracked changes.

Subsection 27(4) of the *Patent Act*

The Applicant has taken note of the objections to former claims 2, 3, 8, 10 and 16 under subsection 27(4) of the *Patent Act*. In response, the Applicant submits that by way of the amendments made to the claims, the defects identified in the Examination Report have been addressed.

The reconsideration and withdrawal of the objections under subsection 27(4) of the *Patent Act* are respectfully requested.

Section 63 and subsection 63(3) of the *Patent Rules*

The Applicant has taken note of the objection to former claims 3-10 and 13-15 under subsection 63(3) of the *Patent Rules* and the objection to former claims 3-10 under section 63 of the *Patent Rules*. In response, the Applicant notes that the claims have been amended to ensure that the dependent claims refer to preceding claims by number and that the dependent claims that refer to more than one claim, do so in the alternative only.

Based on the foregoing, reconsideration and withdrawal of the objections under section 63 and subsection 63(3) of the *Patent Rules* are respectfully requested.

Section 28(3) of the *Patent Act*

Former claims 1-16 were rejected under section 28.3 of the *Patent Act* as allegedly being obvious. In issuing this rejection, the Examination Report followed the conclusions of the International

Preliminary Report on Patentability (IPRP), which considered that former claims 1-16 lacked inventive step in view of either D1 (US 2016/0294831 A1) or D2 (WO 2015/036957 A1).

Without conceding to the propriety of the rejection, but instead to expedite prosecution, the claims have been amended as noted above. The Applicant respectfully requests reconsideration and withdrawal of the rejection in view of the amendments and the following observations.

In section 2.2.1, the IPRP considers that claim 16 is just a description of a verifier (reader) accreditation principle that sorts out the mobile data into categories such as “acceptable” or “not-acceptable”.

Thus, with respect to the subject matter of instant claim 1 (and consequently also instant claim 16), the Applicant considers that it is more than this administrative policy and, actually, the claimed subject matter defines the configuration by identification data issuers of security rules applying to data, which are determined at the mobile interface only by their names or labels.

Namely, the feature so-called LOS (i.e., level of security) is not just an administrative accreditation to access data, but it is in practice a specific coding of security conditions that cannot be by-default bore by labels because labels are not structures or containers pre-determined by existing standards, with known (to the skilled person in the art) fields or sub-containers dedicated to host security rules with known coding language, etc. So, this one aspect is where the claimed subject matter is laid: informing about security mechanisms attached to unstructured labels or names that are not files, dedicated files, data objects, records, byte strings or so.

They are only names of data with absolutely no hint about actual data structure that can be any. The absence of structure does not allow for attachment of security rules to a part of the structure, whereby it does not offer either a pre-existing or by-default discovery mechanism, thus it requires specific design and this is what the claimed subject matter describes; and it describes as well how such design can be exploited to allow:

1. the reader / verifier to discover the security policy assigned by the issuer and

2. the reader / verifier to ask the mobile for data meeting a given LOS.

Points (1) and (2) are specified nowhere for namespaces.

Therefore, the subject matter of instant claim 1 is not defining mere data stored on a database

with index and tables and named data with their corresponding security rules but, rather, it defines a discoverability mechanism of security policies for non-structured data.

Therefore, contrary to the assertions in sections 2.2.2 and 2.2.3 of the IPRP that the only alleged features would be the mobile device communicating with the reader, the features mentioned above are not "administrative aspects", these relate with technical discoverability and coding language for security policies. Namely, they implement a (1) coding and assignment of security policies to non-structured identification data, (2) discoverability of such policies, and (3) granularity of policies to the level of a namespace.

Once an outline of the claimed subject matter of instant claim 1 is made, the Applicant wishes to address the cited documents **D1** and **D2**.

Objective analysis of document D1:

D1 is mainly intended for the case of a verification of a driving license from remote i.e., from a police car close to the vehicle being checked with its plate number. Roughly, localization of the vehicle is matched with its plate number by requesting a registry.

Hence, it does not cover the two features quoted above: allow (1) the reader / verifier to discover the security policy assigned by the issuer and (2) the reader / verifier to ask the mobile for data meeting a given LOS.

Thus, instant claim 1 is believed to be novel and non-obvious in view of D1.

Objective analysis of document D2:

D2 is not addressing the same topic as the subject-matter of instant claim 1. In fact, D2 deals with data minimization and, thus, it does not describe a discoverability protocol with specific coding embodiment to assign access rules to names data. Particularly, D2 describes a process to assess the data that can be disclosed (for data minimization purposes) to access a service. And the data filtering out and decision can be taken either on remote secure wallet server or off-line onto the mobile. This process has nothing to do with the subject matter of instant claim 1.

Finally, concerning section 3.3 of the IPRP, the selective disclosure of the user of a namespace is but the preliminary action mandated by data minimization and user consent privacy principles; filtering out namespaces is only a usual operation before the subject matter of instant claim 1

related to security policy divulgation for selected namespaces intervenes.

Thus, instant claim 1 is also believed to be novel and non-obvious in view of D2.

Final comments

In view of the foregoing, a person skilled in the art with the teachings of D1 and D2 would not have been motivated to arrive at the subject-matter of instant claim 1. Hence, instant claim 1 is believed to be novel and non-obvious over D1 and D2. Instant independent claim 11 recites similar subject matter to instant claim 1 is therefore believed to be patentable for at least similar reasons.

Regarding instant dependent claims 2-10 and 12-16, the Applicant submits that these claims are also novel and non-obvious over the cited reference, at least due to their respective dependencies from instant independent claims 1 and 11.

Reconsideration and withdrawal of the rejection under section 28.3 of the *Patent Act* are respectfully requested.

Good standing

It is believed that the present application is in good standing. If, however, it appears that the application is deemed abandoned, or if CIPO considers that this application is deemed abandoned, we request that CIPO informs us in writing immediately.

Should the amount(s) indicated in this letter be insufficient to cover all of the fee(s) for which payment(s) is(are) explicitly or implicitly requested by this letter, or if a fee payment cannot be charged to the designated credit card, CIPO is hereby **unconditionally, clearly and unequivocally authorized** to debit any amount required to pay or complete any applicable fee from our deposit account **600000233**, in order to keep the present application in good standing.

CONCLUSION

In view of the above, it is submitted that all rejections and objections raised by the Examiner have been addressed and overcome by the present response and that the application complies with the *Patent Act* and *Patent Rules*. Allowance of the claims and issuance of a Notice of Allowance are therefore respectfully solicited.

The Examiner is invited to call us if any further amendment will expedite allowance of the

application or if the Examiner has any suggestions or questions concerning this application.

Respectfully submitted,



ROBIC S.E.N.C.R.L. / LLP
Avocats, agents de brevets et de marques de commerce /
Lawyers, Patent and Trademark Agents

Agent de brevets / Patent Agent: Vincent Boucher
+1 514 987-8897

VBO/SPE/mlt

Encl. new pages 1 to 20 of the description;
new set of 16 claims; and
marked-up copy of the amended set of claims.

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 of claim 1, comprising:

transmitting a list of supported namespaces to a verifier module executing on a 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 of claim 1, comprising:

transmitting a list of supported namespaces to 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. The method of claim 1 or 2, 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 of any one of claims 1 to 4, comprising:

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

6. The method of any one of claims 1 to 5, wherein the security policy is transmitted as a sequence of bytes having bits identifying required

Date Reçue/Date Received 2023-08-25

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

7. The method of any one of claims 1 to 6, wherein a 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 of claim 1, further comprising 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 a verifier associates with each namespace in the plurality of supported namespaces.

9. The method of any one of claims 1 to 8, further comprising 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 of claim 1, 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 a 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; and

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.

Date Reçue/Date Received 2023-08-25

12. The mobile device of claim 11, 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 of claim 11 or 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 of any one of 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 of claim 11 or 12, 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 in accordance with any one of claims 1 to 15, the method 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:

Date Reçue/Date Received 2023-08-25

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 a 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.

Date Reçue/Date Received 2023-08-25

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.,

Date Reçue/Date Received 2023-08-25

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

Date Reçue/Date Received 2023-08-25

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.

Date Reçue/Date Received 2023-08-25

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

Date Reçue/Date Received 2023-08-25

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.

Date Reçue/Date Received 2023-08-25

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.

Date Reçue/Date Received 2023-08-25

[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

Date Reçue/Date Received 2023-08-25

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)

Date Reçue/Date Received 2023-08-25

[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, of 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.

Date Reçue/Date Received 2023-08-25

[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".

[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

Date Reçue/Date Received 2023-08-25

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)

Date Reçue/Date Received 2023-08-25

[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.

Date Reçue/Date Received 2023-08-25

[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

Date Reçue/Date Received 2023-08-25

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 filed 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

Date Reçue/Date Received 2023-08-25

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.

Date Reçue/Date Received 2023-08-25

[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] The following aspects are also disclosed herein:

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 of aspect 1, comprising:

transmitting a list of supported namespaces to a verifier module executing on a 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 of aspect 1, comprising:

transmitting a list of supported namespaces to 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. The method of aspect 1 or 2, 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

Date Reçue/Date Received 2023-08-25

only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

5. The method of any one of aspects 1 to 4, comprising:

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

6. The method of any one of aspects 1 to 5, 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 of any one of aspects 1 to 6, wherein a 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 of aspect 1, further comprising 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 a verifier associates with each namespace in the plurality of supported namespaces.

9. The method of any one of aspects 1 to 8, further comprising 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 of aspect 1, 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 a verifier terminal.

Date Reçue/Date Received 2023-08-25

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; and

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 aspect 11, 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 of aspect 11 or 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 of any one of aspects 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 of aspect 11 or 12, 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 in accordance with any one of aspects 1 to 15, the method comprising:

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

Date Reçue/Date Received 2023-08-25

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 a 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.

Date Reçue/Date Received 2023-08-25

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 of claim 1~~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 a~~the~~ verifier module executing on a~~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 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~~, comprising:

transmitting a list of supported namespaces to a~~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 of claim 1 or 2~~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.

Date Reçue/Date Received 2023-08-25

5. The method of any one of claims 1 to 4~~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 of any one of claims 1 to 5~~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 of any one of claims 1 to 6~~for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims~~, wherein a~~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 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 comprisinges~~s~~ 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 a~~the~~ verifier associates with each namespace in the plurality of supported namespaces.

9. The method of any one of claims 1 to 8~~for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device according to any previous claims~~, further comprisinges~~s~~ 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.

Date Reçue/Date Received 2023-08-25

10. 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 a~~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; and

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~~11, 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 of~~according to~~ claim~~s~~ 11 or~~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 of~~according to~~ any one of 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 of~~according to~~ claim~~s~~ 11 or~~to~~ 12, ~~wherein the eID wallet application~~ wherein the security policy is transmitted as a sequence of bytes

Date Reçue/Date Received 2023-08-25

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 in accordance with any one of claims 1 to 15, the method 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 a~~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.

Date Reçue/Date Received 2023-08-25

16 May 2023 (16-05-2023)

ROBIC
opic.brevets@robic.com

Application No.	:	**3,154,428**
PCT No.	:	**EP2020076906**
Owner	:	THALES DIS FRANCE SAS
Title	:	**SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES**
Classification	:	G06Q 50/26 (2012.01)
Your File No.	:	**014211-0023**
Examiner	:	Phoenix Bard-Cavers

YOU ARE HEREBY NOTIFIED OF A REQUISITION BY THE EXAMINER IN ACCORDANCE WITH SUBSECTION 86(2) OF THE *PATENT RULES*. IN ORDER TO AVOID ABANDONMENT UNDER PARAGRAPH 73(1)(*a*) OF THE *PATENT ACT*, A WRITTEN REPLY MUST BE RECEIVED WITHIN **FOUR (4)** MONTHS AFTER THE ABOVE DATE.

This application has been examined taking into account the:

Description,	pages 1-17, as originally filed;
Claims,	1-16, as originally filed; and
Drawings,	pages 1/9-9/9, as originally filed.

This application has been examined taking into account applicant's correspondence on prior art received in this office on 27 April 2022 (27-04-2022).

The number of claims in this application is 16.

Documents Cited:

D1:*	US 2016/0294831 A1	Borunda et al.	6 October 2016 (06-10-2016)
D2:*	WO 2015/036957 A1	Renard et al.	19 March 2015 (19-03-2015)

* document cited by a foreign patent office

The examiner has identified the following defects in the application:

Obviousness

Claims 1-16 do not comply with section 28.3 of the *Patent Act*. In the present case claims 1-16 are identical to the claim set that was examined in the International Preliminary Report on

Patentability (IPRP), which concluded that claims 1-16 lack an inventive step as required under PCT Article 33(3). The prior art cited in the IPRP and the detailed reasons supporting a lack of inventive step have been considered and are found to be relevant and persuasive with respect to obviousness and section 28.3 of the *Patent Act*. Claims 1-16 encompass subject-matter that, in light of the teachings of the cited prior art, does not require any degree of invention and would have been obvious. Claims 1-16 therefore do not comply with section 28.3 of the *Patent Act*.

Claim Defects

Claims 3-10 and 13-15 are dependent claims that refer to more than one claim not in the alternative and do not comply with subsection 63(3) of the *Patent Rules*. A preamble such as "according to any one of claims", would make it clear that the above claims depend upon each claim in the alternative only.

Claims 3-10 are dependent claims that do not refer to preceding claims by number and do not comply with section 63 of the *Patent Rules*.

Claims 2, 3, 8, 10, and 16 are indefinite and do not comply with subsection 27(4) of the *Patent Act*. The following terms have no antecedents:

"verifier module" (claims 2 and 3, lines 3 and 4, respectively),
"verifier" (claim 2 and 8, lines 4 and 5, respectively), and
"verifier terminal" (claims 10 and 16, lines 7 and 16-17, respectively).

Please note that some of these defects are due to the claim dependency, which should be amended.

Description Defects

The description contains a statement that incorporates by reference another document and does not comply with subsection 57(1) of the *Patent Rules*. Such a statement is found at paragraph 0038 and should be removed.

Examiner Requisitions

In view of the foregoing defects, the applicant is requisitioned, under subsection 86(2) of the *Patent Rules*, to amend the application in order to comply with the *Patent Act* and the *Patent Rules* or to provide arguments as to why the application does comply.

Under section 102 of the *Patent Rules*, any amendment made in response to this requisition must be accompanied by a statement explaining the purpose of the amendment and identifying the differences between the new page and the replaced page.

Phoenix Bard-Cavers
Patent Examiner
873-354-9901

As per CIPO Client Service Standards, a response to a telephone enquiry or voice mail should be provided by the end of the next business day. In the event that attempts to reach the examiner are unsuccessful, the examiner's Section Head, Chaza Nasrallah, can be reached at 819-635-4148.

For general inquiries: 1-866-997-1936 or for more options see http://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/wr00006.html.

CIPO values your feedback and invites you to complete a short and anonymous ongoing survey on patent examination products and services. You can access the survey at the following link: https://form.simplesurvey.com/f/s.aspx?s=91e23402-ee27-4868-a230-ab5c819f9d1c.

3154428A_PBC.docm

The Examination Search Report is provided for reference only and is not part of any requisition made by the examiner in accordance with the *Patent Act* or *Rules*. The applicant is not required to respond to the information contained in the Examination Search Report.

Examination Search Report

Box I: General Information

Application No.	3,154,428	Search Report Date	2023-04-27
Title	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES		
Examiner	Phoenix Bard-Cavers	Search Conducted?	Yes

Box II: Family Prosecution

Family Member	File Wrapper Reviewed	Status of Prosecution
WO2021073853A1	2023-04-27	Completed
US2022374533A1	2023-04-27	Not Started
EP3809358A1	2023-04-27	Abandoned
EP4046126A1	2023-04-27	Not Started
AU2020367942A8	2023-04-27	In Progress

Box III: Search History

Claims Searched	1-16	Date of Search	2023-04-27

Type of Search Conducted (select all that apply):

Canadian first to file search	■	Supplemental/top up search	□
Inventor/applicant search	■	Non laid open search	□
Comprehensive search	□	In-house searcher	□

Search History from Databases Consulted:

```
##### CANADIAN PATENT DATABASE/INTELLECT ##########

1 534 filing-date:[2015-09-25 TO 2021-12-10] AND ipc:(G06Q\ 50/26 OR G06Q\
20/32 OR G06Q\ 20/36)

2 220 (filing-date:[2015-09-25 TO 2021-12-10] AND ipc:(G06Q\ 50/26 OR G06Q\
20/32 OR G06Q\ 20/36)) AND (security AND wallet)

3 206 ((filing-date:[2015-09-25 TO 2021-12-10] AND ipc:(G06Q\ 50/26 OR G06Q\
20/32 OR G06Q\ 20/36)) AND (security AND wallet)) AND (wallet AND mobile)
```

```
4 3 (((filing-date:[2015-09-25 TO 2021-12-10] AND ipc:(G06Q\ 50/26 OR G06Q\
20/32 OR G06Q\ 20/36)) AND (security AND wallet)) AND (wallet AND mobile))
AND (namespace)

5 3 inventor:("BAYLE CAROLE"~3 OR "FAHER MOURAD"~3)  OR applicant:("THALES
DIS FRANCE SAS"~3)
```

CIPO Search Record - Version 10

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

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

REÇU LE
24 NOV. 2020
DIRECTION PROPRIÉTÉ INTELLECTUELLE

PCT

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

(PCT Rule 44.1)

Applicant's or agent's file reference GMT4110 WO/YL	Date of mailing *(day/month/year)* 20 November 2020 (20-11-2020)
	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/EP2020/076906	International filing date *(day/month/year)* 25 September 2020 (25-09-2020)
Applicant THALES DIS FRANCE SA	

1. [X] 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 46):

   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.

2. [ ] 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.

3. [ ] **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.

4. **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 90*bis*.1 and 90*bis*.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 20 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 45*bis*.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. 5818 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)

Date Reçue/Date Received 2022-04-27

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
GMT4110.WO/YL		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/EP2020/076906	25 September 2020 (25-09-2020)	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.

[X] 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:
      [X] 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 43.6*bis*(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,**
   [X] 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,**
   [X] 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
      [X] 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

Date Reçue/Date Received 2022-04-27

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)
EPO-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

[X] Further documents are listed in the continuation of Box C. [X] 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	Date of mailing of the international search report
12 November 2020	20/11/2020

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Nicoli, Félix

1

Form PCT/ISA/210 (second sheet) (April 2005)

Date Reçue/Date Received 2022-04-27

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

1

Date Reçue/Date Received 2022-04-27

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

Date Reçue/Date Received 2022-04-27

Information on Search Strategy - Pilot phase (see OJ 2015, A86)
The type of information contained in this sheet may change during the pilot for improving the usefulness of this new service.

Application Number
PCT/EP2020/076906

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:

EPO FORM P04A42

Date Reçue/Date Received 2022-04-27

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.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.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP2020/076906	25.09.2020	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 43*bis*.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 notifed 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:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Nicoli, Félix Telephone No. +31 70 340-0

Form PCT/ISA/237 (Cover Sheet) (January 2015)

Date Reçue/Date Received 2022-04-27

Box No. I 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 43*bis*.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 13*ter*.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 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.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:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-16
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-16
Industrial applicability (IA)	Yes:	Claims	1-16
	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

Date Reçue/Date Received 2022-04-27

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 2016/156386 A1 (VAN NIEUWENHUYZE OLIVIER [BE] ET AL) 2 June 2016 (2016-06-02)

D4 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]

D5 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]

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-

Date Reçue/Date Received 2022-04-27

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.

Date Reçue/Date Received 2022-04-27

Basically, a user whishes to access a service for which he/she needs to provide identification information. The user can provides 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. It 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 legitimity 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 by a mobile device with a digital wallet in communication with a reader. Any other feature is deemed to relate to a 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 a reader. Such a system was well-known in art at the priority date of the application as this 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.

Date Reçue/Date Received 2022-04-27

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.

Date Reçue/Date Received 2022-04-27

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 his feature can be found in claim 1.

Date Reçue/Date Received 2022-04-27

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.

BNSDOCID: <XS_____ Date Rescue/Date Received 2022-04-27

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 CPRTENPRDE

server date 20200106; downloaded by EPO on 20191106

EMV '96
Integrated Circuit Card Application Specification for Payment Systems

Version 3.1.1
May 31, 1998

© 1998 Europay International S.A., MasterCard International Incorporated, and Visa International Service Association. All rights reserved. Permission to copy and implement the material contained herein is granted subject to the conditions that (i) any copy or re-publication must bear this legend in full, (ii) any derivative work must bear a notice that it is not the *Integrated Circuit Card Application Specification for Payment Systems* jointly published by the copyright holders, and (iii) that none of the copyright holders shall have any responsibility or liability whatsoever to any other party arising from the use or publication of the material contained herein.

The authors of this documentation make no representation or warranty regarding whether any particular physical implementation of any part of this specification does or does not violate, infringe, or otherwise use the patents, copyrights, trademarks, trade secrets, know-how, and/or other intellectual property of third parties, and thus any person who implements any part of this specification should consult an intellectual property attorney before any such implementation. The following Specification includes public key encryption technology, which is the subject matter of patents in several countries. Any party seeking to implement this specification is solely responsible for determining whether their activities require a license to any technology including, but not limited to, patents on public key encryption technology. Europay International S. A., MasterCard International Incorporated, and Visa International Service Association shall not be liable for any party's infringement of any intellectual property right.

Date Reçue/Date Received 2022-04-27

Date Reçue/Date Received 2022-04-27

Table of Contents

1. Scope 1
2. Normative References 3
3. Definitions 4
4. Abbreviations and Notations 6
5. Files for Financial Transaction Interchange 8
5.1 Mandatory Data Objects 9
5.2 Data Retrievable by GET DATA Command 10
5.3 Data Retrievable by Get Processing Options 11
6. Transaction Flow 12
6.1 Exception Handling 12
6.2 Example Flowchart 12
6.3 Additional Functions 14
7. Functions Used in Transaction Processing 15
7.1 Initiate Application Processing 15
7.2 Read Application Data 16
7.3 Offline Data Authentication 17
7.4 Processing Restrictions 20
7.4.1 Application Version Number 20
7.4.2 Application Usage Control 20
7.4.3 Application Effective/Expiration Dates Checking 21
7.5 Cardholder Verification 22
7.5.1 Offline PIN Processing 23
7.5.2 Online PIN Processing 24
7.5.3 Signature Processing 24
7.5.4 Combination CVMs 24
7.6 Terminal Risk Management 25
7.6.1 Floor Limits 25
7.6.2 Random Transaction Selection 26
7.6.3 Velocity Checking 27
7.7 Terminal Action Analysis 28
7.8 Card Action Analysis 31
7.8.1 Terminal Messages for an AAC 32
7.8.2 Advice Messages 32
7.9 Online Processing 32
7.10 Issuer-to-Card Script Processing 33
7.11 Completion 35
8. GENERATE AC Command Coding 36
8.1 Command Parameters 39
8.2 Command Data 39
8.2.1 Card Risk Management Data 39
8.2.2 Transaction Certificate Data 39
8.3 Command Use 40

Date Reçue/Date Received 2022-04-27

8.3.1 GENERATE AC (First Issuance) 40
8.3.2 GENERATE AC (Second Issuance) 41
9. Erroneous or Missing Data in the ICC 42
Annex A - Coding of Data Elements A-1
A1. Application Interchange Profile A-2
A2. Application Usage Control A-3
A3. Cardholder Verification Rule Format A-4
A4. Issuer Code Table Index A-6
A5. Terminal Verification Results A-7
A6. Transaction Status Information A-10

Date Reçue/Date Received 2022-04-27

Tables

Table 1 - Data Objects Used by the Offline Data Authentication Algorithm 9
Table 2 - Mandatory Data Objects 9
Table 3 - Data Required for Offline Static Data Authentication 10
Table 4 - Data Required for Offline Dynamic Data Authentication 10
Table 5 - Data Objects Retrievable by GET DATA Command 11
Table 6 - Data Retrievable by GET PROCESSING OPTIONS 11
Table 7 - ICC Data Missing Indicator Setting 43
Table A-1 - Application Interchange Profile A-2
Table A-2 - Application Usage Control A-3
Table A-3 - CVM Codes A-4
Table A-4 - CVM Condition Codes A-5
Table A-5 - Issuer Code Table Index A-6
Table A-6 - Terminal Verification Results A-9
Table A-7 - Transaction Status Information A-10

Date Reçue/Date Received 2022-04-27

Figures

Figure 1 - Transaction Flow Example 13
Figure 2 - Random Selection Probability (not to scale) 27
Figure 3 - Issuer Script Format 34
Figure 4 - Issuer Script Command Format (Shown with Three Commands) 34
Figure 5 - Use of GENERATE AC Options 37
Figure 6 - Use of GENERATE AC with Referrals 38

Date Reçue/Date Received 2022-04-27

1. Scope

The *Integrated Circuit Card Application Specification for Payment Systems* (hereinafter referred to simply as 'the Application Specification') defines the terminal and integrated circuit card (ICC) procedures necessary to effect a payment system transaction in an international interchange environment.

In particular it covers:

- Mapping of data elements to files
- Transaction flow (the sequence of events and the commands issued to the card)
- Exception processing
- Coding of specific data objects described generally in the *Integrated Circuit Card Specification for Payment Systems* (hereinafter referred to simply as the 'Card Specification') (see Annex A)

The functions described are those necessary to ensure that payment system cards conforming to this specification can perform the set of common core functions in all terminals conforming to this specification. Application functions unique to individual payment systems and those functions not performed in interchange are not described, but are not precluded.

This specification does not address clearing and settlement or any transactions where the ICC is not present.

The Application Specification assumes familiarity with the Card Specification. The Card Specification describes functionality outside the application layer, including application selection. Both specifications are intended for use by payment system members, ICC and terminal manufacturers, and designers of applications using ICCs or interfacing to payment system applications that use ICCs.

1.1 EMV Specification Version Numbering

To facilitate future reference of the EMV specifications and to differentiate between technical updates and editorial clarifications, with the publication of this version of the EMV specifications, EMV has introduced the following version numbering scheme:

version X.Y.Z,

where:

X indicates the phase number of the specifications
Y indicates technical change(s) from the previous version
Z indicates editorial change(s) from the previous version

Date Reçue/Date Received 2022-04-27

Therefore, this version of the EMV specifications is version 3.1.1, since the basis for this specification is version 3 and both technical and editorial changes have been made.

Date Reçue/Date Received 2022-04-27

2. Normative References

The following standards contain provisions that are referenced in this specification:

Europay, MasterCard, and Visa (EMV):March 31, 1998	Integrated Circuit Card Specification for Payment Systems
Europay, MasterCard, and Visa (EMV):March 31, 1998	Integrated Circuit Card Terminal Specification for Payment Systems
ISO 8859:1987	Information processing - 8-bit single byte coded graphic character sets
ISO 9564:1991	Banking - Personal identification number management and security
ISO/IEC 7816-4:1995	Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange
ISO/IEC 7816-5:1994	Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers

Date Reçue/Date Received 2022-04-27

3. Definitions

The following terms are used in this specification.

Application - The protocol between the card and the terminal and its related set of data.

Byte - 8 bits.

Card - A payment card as defined by a payment system.

Command - A message sent by the terminal to the ICC that initiates an action and solicits a response from the ICC.

Concatenation - Two elements are concatenated by appending the bytes from the second element to the end of the first. Bytes from each element are represented in the resulting string in the same sequence in which they were presented to the terminal by the ICC, that is, most significant byte first. Within each byte bits are ordered from most significant bit to least significant. A list of elements or objects may be concatenated by concatenating the first pair to form a new element, using that as the first element to concatenate with the next in the list, and so on.

Cryptogram - Result of a cryptographic operation.

Financial Transaction - The act between a cardholder and a merchant or acquirer that results in the exchange of goods or services against payment.

Function - A process accomplished by one or more commands and resultant actions that are used to perform all or part of a transaction.

Integrated Circuit(s) - Electronic component(s) designed to perform processing and/or memory functions.

Integrated Circuit(s) Cards - A card into which one or more integrated circuits are inserted to perform processing and memory functions.

Message - A string of bytes sent by the terminal to the card or vice versa, excluding transmission control characters.

Online - When used in the Application Specification, online means online to the issuer or to a host system standing in for the issuer. Connections between the terminal and a merchant or acquirer host are not included in this definition.

Payment System - For the purposes of this specification, Europay International S.A., MasterCard International Incorporated, or Visa International Service Association.

PIN Pad - An arrangement of numeric and command keys to be used for PIN entry.

Date Reçue/Date Received 2022-04-27

Response - A message returned by the ICC to the terminal after the processing of a command message received by the ICC.

Script - A command or a string of commands transmitted by the issuer to the terminal for the purpose of being sent serially to the ICC as commands.

Template - Value field of a constructed data object, defined to give a logical grouping of data objects.

Terminal - The device used in conjunction with the ICC at the point of transaction to perform a financial transaction. It incorporates the interface device and may also include other components and interfaces such as host communications.

Date Reçue/Date Received 2022-04-27

4. Abbreviations and Notations

The following abbreviations and notations are used in this specification.

AAC	Application Authentication Cryptogram
AAR	Application Authorisation Referral
AC	Application Cryptogram
ADF	Application Definition File
AFL	Application File Locator
AID	Application Identifier
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
ARQC	Authorisation Request Cryptogram
ATC	Application Transaction Counter
b	Binary
BER	Basic Encoding Rules
CDOL	Card Risk Management Data Object List
CVM	Cardholder Verification Method
CVR	Cardholder Verification Rule
DDOL	Dynamic Data Authentication Data Object List
DF	Dedicated File, as defined by ISO 7816-4
FCI	File Control Information
hex.	Hexadecimal
ICC	Integrated Circuit Card
ID	Identifier
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation

Date Reçue/Date Received 2022-04-27

M	Mandatory
O	Optional
PAN	Primary Account Number
PDOL	Processing Options Data Object List
PIN	Personal Identification Number
RFU	Reserved for Future Use
RID	Registered Application Provider Identifier
SFI	Short File Identifier
SW1	Status Word 1
SW2	Status Word 2
TC	Transaction Certificate
TDOL	Transaction Certificate Data Object List
TLV	Tag Length Value
TSI	Transaction Status Information
TVR	Terminal Verification Results
var.	Variable

The following notations apply:

'0' to '9' and 'A' to 'F'	16 hexadecimal digits
#	Number
[...]	Optional part
xx	Any value

Date Reçue/Date Received 2022-04-27

5. Files for Financial Transaction Interchange

The description of the file structure and commands for accessing the files may be found in the Card Specification, as may the definition of each of the data objects. The payment system or issuer will map the appropriate data objects to files according to their needs, subject to the following restrictions:

- All files accessible using the READ RECORD command as defined in the Card Specification containing data objects defined in the Card Specification shall use short file identifiers (SFIs) in the range 1 to 10. These files:

  – Shall be linear files readable using the READ RECORD command as described in the Card Specification.

  – May contain multiple records. Each record is limited to 254 bytes, including tag and length.

  – Each record shall be coded as a constructed data object. The tag of the constructed data object shall be '70' indicating a template proprietary to this specification, and the length field shall contain the total length of the encapsulated data objects.

  – Shall contain only data objects defined in this specification and coded in accordance with the Basic Encoding Rules - Tag Length Value (BER-TLV) described in the Card Specification.

  – May have access conditions to be satisfied for updates, but must be readable unconditionally.

- Files with SFIs in the range 11 to 20 are reserved for proprietary data to be specified by the individual payment systems.

- Files with SFIs in the range 21 to 30 are reserved for proprietary data to be specified by the issuer.

- The Application File Locator (AFL) described in the Card Specification determines the files and records to be used for processing a transaction. The use of the AFL is described in section 7.2. The data objects listed in Table 1 are used by the offline data authentication algorithm and, when present, should be located in the first record referenced by the AFL.[1]

[1] This allows the terminal to optionally perform the hashing necessary for data authentication in parallel with reading and parsing of data for other purposes.

Date Reçue/Date Received 2022-04-27

Tag	Value
'8F'	Certification Authority Public Key Index
'90'	Issuer Public Key Certificate

Table 1 - Data Objects Used by the Offline Data Authentication Algorithm

Additional information may be found in complementary payment system documentation.

5.1 Mandatory Data Objects

Table 2 lists the data objects that must be present in the ICC in files read using the READ RECORD command. All other data objects defined in this specification to be resident in such files in the card are optional.

Tag	Value	Presence
'5F24'	Application Expiration Date	M
'5A'	Application Primary Account Number (PAN)	M
'8C'	Card Risk Management Data Object List 1	M
'8D'	Card Risk Management Data Object List 2	M

Table 2 - Mandatory Data Objects

Table 3 lists the data objects that must be present if the ICC supports offline static data authentication. Table 4 lists the data objects that must be present if the ICC supports offline dynamic data authentication.[2] Offline data authentication is required to support offline transactions but is optional in cards that support only online transactions.

[2] The exception may be that the Issuer Public Key Remainder or the ICC Public Key Remainder could be absent. This is because if the public key modulus can be recovered in its entirety from the public key certificate there is no need for a remainder.

Date Reçue/Date Received 2022-04-27

Tag	Value
'8F'	Certification Authority Public Key Index
'90'	Issuer Public Key Certificate
'93'	Signed Static Application Data
'92'	Issuer Public Key Remainder
'9F32'	Issuer Public Key Exponent

Table 3 - Data Required for Offline Static Data Authentication

Tag	Value
'8F'	Certification Authority Public Key Index
'90'	Issuer Public Key Certificate
'92'	Issuer Public Key Remainder
'9F32'	Issuer Public Key Exponent
'9F46'	ICC Public Key Certificate
'9F47'	ICC Public Key Exponent
'9F48'	ICC Public Key Remainder
'9F49'	Dynamic Data Authentication Data Object List (DDOL)

Table 4 - Data Required for Offline Dynamic Data Authentication

5.2 Data Retrievable by GET DATA Command

Data objects listed in Table 5 are not retrievable by the READ RECORD command but are retrieved by the terminal using the GET DATA command as described in the Card Specification.

Of the objects listed here, only the Application Transaction Counter (ATC) is a mandatory data object, and it can be retrieved by either the GET DATA command or in the response to a GENERATE APPLICATION CRYPTOGRAM (AC) command. The terminal retrieves the ATC via the GET DATA command only if the ICC contains the Lower Consecutive Offline Limit and Upper Consecutive Offline Limit

Date Reçue/Date Received 2022-04-27

data objects. If the issuer does not wish terminal velocity checking to be performed and omits these data objects, the ICC does not need to support the GET DATA command.

Tag	Value	Presence
'9F36'	Application Transaction Counter (ATC)	M
'9F17'	PIN Try Counter	O
'9F13'	Last Online ATC Register	O

Table 5 - Data Objects Retrievable by GET DATA Command

5.3 Data Retrievable by Get Processing Options

Data objects listed in Table 6 are not retrievable by the READ RECORD command but are retrieved by the terminal using the GET PROCESSING OPTIONS command as described in the Card Specification. Table 6 defines the data returned, not the format of the response; the Card Specification describes the format of the data when returned by the GET PROCESSING OPTIONS command.

Tag	Value	Presence
'82'	Application Interchange Profile	M
'94'	Application File Locator	M

Table 6 - Data Retrievable by GET PROCESSING OPTIONS

Date Reçue/Date Received 2022-04-27

6. Transaction Flow

The Application Interchange Profile specifies the application functions that are supported by the card. The terminal shall attempt to execute only those functions that the ICC supports.

6.1 Exception Handling

Exceptions to normal processing are described in the Application Specification for specific status codes returned in the status bytes (SW1, SW2) or for missing data. Unless otherwise specified in the Application Specification, any SW1 SW2 returned by the transport layer to the application layer other than '9000', '63Cx', or '6283' shall cause termination of the transaction.[3] This requirement applies to the Application Specification but does not apply to the application selection process.

6.2 Example Flowchart

The flowchart in Figure 1 gives an example of a transaction flow that may be used by a terminal for a normal purchase transaction. This flowchart is only an example, and the order of processing may differ from that given here. All restrictions on the order of processing are provided in section 7.

[3] Other actions may be taken by prior agreement but are outside the scope of this specification.

Date Reçue/Date Received 2022-04-27

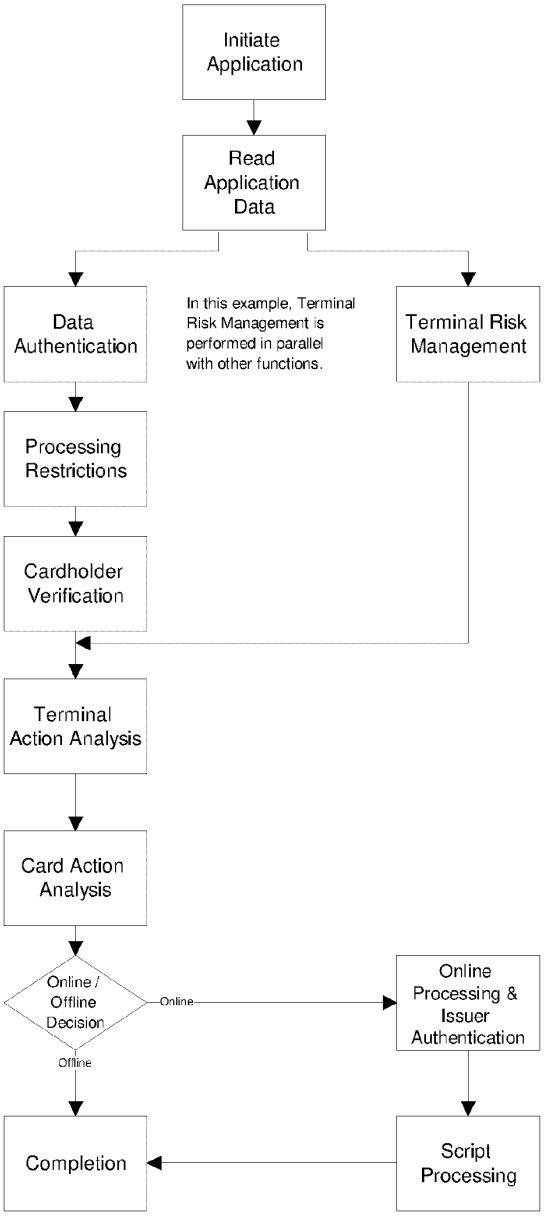


Figure 1 - Transaction Flow Example

Date Reçue/Date Received 2022-04-27

6.3 Additional Functions

Provision has been made in this specification for additional functions beyond those described here. Such additional functions may be:

- Future additions to this specification
- Proprietary functions implemented by local or national agreement or by the individual payment systems

The Application Interchange Profile indicates the functions supported in the ICC according to this specification. Most of the bits in this data object are reserved for future use (RFU). When a new function is added, a bit in the Application Interchange Profile will be allocated to indicate support for the new function, and this specification will be updated to specify the new function and where it fits into the transaction flow.

Proprietary functions may be added to the terminal and the ICC application as long as they do not interfere with processing of terminals and ICCs not implementing the function. For example, offline dynamic data authentication based on symmetric keys may be added at local option. Such proprietary functions, while not described in this specification, are not precluded, as long as the functions specified herein continue to be supported for ICCs not implementing the proprietary functions.

Date Reçue/Date Received 2022-04-27

7. Functions Used in Transaction Processing

The Card Specification describes all functionality outside the application layer, including the selection of the application. The functions described here begin after application selection has taken place.

The remainder of this section deals with the terminal-to-ICC dialogue on the level of the application logical functions.

7.1 Initiate Application Processing

Purpose: Inform the ICC that the processing of a new transaction is beginning and provide to the ICC the terminal information about the transaction. Obtain from the ICC the Application Interchange Profile and a list of files that contain the ICC data to be used in processing the transaction, and determine whether the transaction is allowed.

Conditions of Execution: This function shall always be executed by the terminal.

Sequence of Execution: This is the first function performed after application selection.

Description: The terminal sets all bits in the Transaction Status Information (TSI) and the Terminal Verification Results (TVR) to '0'.[4]

The Processing Options Data Object List (PDOL) is a list of tags and lengths of terminal-resident data elements needed by the ICC in processing the GET PROCESSING OPTIONS command. Only data elements identified in the Card Specification as having the terminal as the source of the data may be referenced in the PDOL.

If the PDOL does not exist, the GET PROCESSING OPTIONS command uses a command data field of '8300', indicating that the length of the value field in the command data is 0.

If the PDOL exists, the terminal extracts the PDOL from the FCI of the ADF and uses it to create a concatenated list of data elements without tags or lengths. The rules specified in Part II of the Card Specification (see 'Rules for Processing a Data Object List (DOL)') apply to processing of the PDOL. If an amount field (either Amount, Authorised or Amount, Other) is referenced in the PDOL and the terminal

[4] There may be some exceptions in the timing for this. For example, these bits could be set to '0' at the completion of the previous transaction or prior to application selection of this transaction. The intent here is that the processing steps as described in the Application Specification presume the bits have been initialised to '0'.

Date Reçue/Date Received 2022-04-27

is unable to provide the amount at this point in transaction processing, the amount field in the data element list shall be filled with hexadecimal zeroes.

The terminal issues the GET PROCESSING OPTIONS command using either the command data field of '8300' (if there was no PDOL in the ICC) or a data object constructed with a tag of '83' and the appropriate length according to BER-TLV encoding rules and a value field that is the concatenated list of data elements resulting from processing the PDOL. The card returns either:

- The Application Interchange Profile, the Application File Locator (identifying the files and records containing the data to be used for the transaction), and status SW1 SW2 = '9000', or
- Status SW1 SW2 = '6985' ('Conditions of use not satisfied'), indicating that the transaction cannot be performed with this application.

The format of the response message is given in the Card Specification.

If the status words '6985' are returned, the terminal shall eliminate the current application from consideration and return to the application selection function to select another application.

7.2 Read Application Data

Purpose: Data contained in files in the ICC are required by the terminal to perform the various functions used in transaction processing as described in this section. The terminal must read this data from the ICC.

Conditions of Execution: This function shall always be executed by the terminal.

Sequence of Execution: The read application data function is performed immediately following the initiate application function.

Description: The terminal shall read the files and records indicated in the Application File Locator using the READ RECORD command identifying the file by its SFI. If an error prevents the terminal from reading data from the ICC, the transaction shall be terminated (see section 6.1).

The AFL is a list identifying the files and records to be used in the processing of a transaction. The terminal is to read only the records named in the AFL. Each element of the list corresponds to a file to be read and is structured as follows:

- The first byte codes the SFI in the five most significant bits. The three least significant bits of the first byte shall be set to zero.
- The second byte codes the first (or only) record number to be read for that SFI. The second byte shall never be set to zero.

Date Reçue/Date Received 2022-04-27

- The third byte codes the last record number to be read for that SFI. Its value is either greater than or equal to the second byte. When the third byte is greater than the second byte, all the records ranging from the record number in the second byte to and including the record number in the third byte shall be read for that SFI. When the third byte is equal to the second byte, only the record number coded in the second byte shall be read for that SFI.

- The fourth byte codes the number of records involved in offline data authentication starting with the record number coded in the second byte. The fourth byte may range from zero to the value of the third byte less the value of the second byte plus 1.

The terminal shall process each entry in the AFL from left to right. A READ RECORD command as described in the Card Specification shall be issued for each record between the starting record number and the ending record number, inclusively. Any SW1 SW2 other than '9000' passed to the application layer as a result of reading any record shall cause the transaction to be terminated. Records specified in the AFL to be included in offline data authentication shall be processed as described in section 7.3.

The terminal shall store all recognised data objects read, whether mandatory or optional, for later use in the transaction processing. Data objects that are not recognised by the terminal (that is, their tags are unknown by the terminal) shall not be stored, but records containing such data objects may still participate in their entirety in offline data authentication, depending upon the coding of the AFL.

All mandatory data objects shall be present in the card. If any mandatory data objects are not present, the terminal shall terminate the transaction.

Redundant primitive data objects are not permitted. If the terminal encounters more than one occurrence of a single primitive data object while reading data from the ICC, the transaction shall be terminated.

Proprietary data files may or may not conform to this specification. Records in proprietary files may be represented in the AFL and may participate in offline data authentication provided that they are readable without conditions by the READ RECORD command coded according to the Card Specification. Otherwise, the reading and processing of proprietary files is beyond the scope of this specification.

7.3 Offline Data Authentication

Purpose: Offline data authentication is performed as specified in the Card Specification. This specification describes how it is determined whether offline data authentication will be performed, what kind of authentication will be performed, and how the success or failure of authentication affects the transaction flow and data recorded in the TVR and TSI.

Conditions of Execution: Availability of data in the ICC to support offline data authentication is optional; its presence is indicated in the Application Interchange

Date Reçue/Date Received 2022-04-27

Profile. If both the terminal and the ICC support offline data authentication, the terminal shall perform this function. Depending on the capabilities of the card and the terminal, either offline static data authentication or dynamic data authentication may be performed but not both.

If both of the following are true, the terminal shall perform offline dynamic data authentication as specified in the Card Specification:

- The Application Interchange Profile indicates that the card supports offline dynamic data authentication.
- The terminal supports offline dynamic data authentication.

If all of the following are true, the terminal shall perform offline static data authentication as specified in the Card Specification:

- The Application Interchange Profile indicates that the card supports offline static data authentication.
- The terminal supports offline static data authentication.
- Either the card or the terminal (or both) does not support offline dynamic data authentication.

If neither offline static data authentication nor offline dynamic data authentication is performed, the terminal shall set the 'Offline data authentication was not performed' bit to '1' in the TVR.

Sequence of Execution: The terminal shall perform offline data authentication in any order after application initiation but prior to completion of the terminal action analysis.

Description: Offline static data authentication authenticates static data put into the card by the issuer. Offline dynamic data authentication authenticates ICC-resident data, data from the terminal, and the card itself.

Input to the authentication process is formed from the records identified by the AFL, followed by the data elements identified by the optional Static Data Authentication Tag List (tag '9F4A').

Only those records identified in the AFL as participating in offline data authentication are to be processed. Records are processed in the same sequence in which they appear within AFL entries. The records identified by a single AFL entry are to be processed in record number sequence. The first record begins the input for the authentication process, and each succeeding record is concatenated at the end of the previous record.

The data from each record to be included in the offline data authentication input depends upon the SFI of the file from which the record was read.

Date Reçue/Date Received 2022-04-27

- For files with SFI in the range 1 to 10, the record tag ('70') and the record length are excluded from the offline data authentication process. All other data in the data field of the response to the READ RECORD command (excluding SW1 SW2) is included.

- For files with SFI 11-30, all data in the data field (excluding SW1 SW2) is included.

The bytes of the record are included in the concatenation in the order in which they appear in the command response.

After all records identified by the AFL have been processed, the Static Data Authentication Tag List is processed, if it exists. Each entry in the list is processed, from left to right. Each entry consists of a tag representing a data element whose source is the ICC; data element lengths are not included in the tag list. The following rules apply to processing of the tag list:

- Only tags defined in the Card Specification and with the ICC as the source are permitted.

- All tags must represent data elements available in the current transaction.

- Tags must not refer to a constructed data object.

- The value field of the data object identified by the tag is to be concatenated to the current end of the input string. Tags and lengths of the data objects identified in the tag list are not included in the concatenation.

Building of the input list for offline data authentication is considered the first step in the offline data authentication process. If the input cannot be built because of a violation of one of the above rules but offline data authentication should be performed according to the 'Conditions of Execution' above, offline data authentication shall be considered to have been performed and to have failed; that is, the terminal shall set to '1' the 'Offline data authentication was performed' bit in the TSI and the appropriate 'Offline static data authentication failed' or 'Offline dynamic authentication failed' bit shall be set in the TVR.

See Part IV of the Card Specification for additional steps to be performed for offline data authentication. If offline static data authentication is performed but is unsuccessful, the 'Offline static data authentication failed' bit shall be set to '1' in the TVR, otherwise it shall be set to '0'. If offline dynamic data authentication is performed but is unsuccessful, the 'Offline dynamic data authentication failed' bit shall be set to '1' in the TVR, otherwise it shall be set to '0'.

Upon completion of the offline data authentication function, the terminal shall set to '1' the 'Offline data authentication was performed' bit in the TSI.

Date Reçue/Date Received 2022-04-27

7.4 Processing Restrictions

Purpose: The purpose of the processing restrictions function is to determine the degree of compatibility of the application in the terminal with the application in the ICC and to make any necessary adjustments, including possible rejection of the transaction.

Conditions of Execution: This function shall always be executed by the terminal.

Sequence of Execution: Functions described here may be performed at any time after application selection and prior to completion of the terminal action analysis.

Description: The processing restrictions function is described as comprising the following compatibility checks:

- Application Version Number
- Application Usage Control
- Application Effective/Expiration Dates Checking

7.4.1 Application Version Number

The application within both the terminal and the ICC shall maintain an Application Version Number assigned by the payment system. The terminal shall use the version number in the ICC to ensure compatibility. If the Application Version Number is not present in the ICC, the terminal shall presume the terminal and ICC application versions are compatible, and transaction processing shall continue. If the Application Version Number is present in the ICC, it shall be compared to the Application Version Number maintained in the terminal. If they are different, the 'ICC and terminal have different application versions' bit shall be set to '1' in the TVR.

7.4.2 Application Usage Control

The Application Usage Control indicates restrictions limiting the application geographically or to certain types of transactions. If this data object is present, the terminal shall make the following checks:

- If the transaction is being conducted at an ATM, the 'Valid at ATMs' bit must be on in Application Usage Control.
- If the transaction is not being conducted at an ATM, the 'Valid at terminals other than ATMs' bit must be on in Application Usage Control.

If the Application Usage Control and Issuer Country Code are both present in the ICC, the terminal shall make the following checks:

Date Reçue/Date Received 2022-04-27

- If the Transaction Type indicates that this is a cash transaction and the Issuer Country Code matches the Terminal Country Code, the 'Valid for domestic cash transactions' bit must be on in Application Usage Control.

- If the Transaction Type indicates that this is a cash transaction and the Issuer Country Code does not match the Terminal Country Code, the 'Valid for international cash transactions' bit must be on in Application Usage Control.

- If the Transaction Type indicates a purchase of goods and the Issuer Country Code matches the Terminal Country Code, the 'Valid for domestic goods' bit must be on in Application Usage Control.

- If the Transaction Type indicates a purchase of goods and the Issuer Country Code does not match the Terminal Country Code, the 'Valid for international goods' bit must be on in Application Usage Control.

- If the Transaction Type indicates a purchase of services and the Issuer Country Code matches the Terminal Country Code, the 'Valid for domestic services' bit must be on in Application Usage Control.

- If the Transaction Type indicates a purchase of services and the Issuer Country Code does not match the Terminal Country Code, the 'Valid for international services' bit must be on in Application Usage Control.

- If the transaction has a cashback amount[5] and the Issuer Country Code matches the Terminal Country Code, the 'Domestic cashback allowed' bit must be on in Application Usage Control.

- If the transaction has a cashback amount[5] and the Issuer Country Code does not match the Terminal Country Code, the 'International cashback allowed' bit must be on in Application Usage Control.

If any of the above tests fail, the 'Requested service not allowed for card product' bit shall be set to '1' in the TVR.

7.4.3 Application Effective/Expiration Dates Checking

If the Application Effective Date is present in the ICC, the terminal shall check that the current date is greater than or equal to the Application Effective Date. If it is not, the 'Application not yet effective' bit shall be set to '1' in the TVR.

---

[5] It is preferred that if the relevant 'Domestic cashback allowed' or 'International cashback allowed' bit is set to '0' in the Application Usage Control, the cashback option should not be offered to the cardholder. However, it is possible for some terminals that the decision regarding cashback may have been made before application selection.

Date Reçue/Date Received 2022-04-27

The terminal shall check that the current date is less than or equal to the Application Expiration Date. If it is not, the 'Expired application' bit shall be set to '1' in the TVR.

7.5 Cardholder Verification

Purpose: Cardholder verification is performed to ensure that the person presenting the ICC is the person to whom the application in the card was issued.

Conditions of Execution: Ability of the ICC to support at least one cardholder verification method is indicated in the Application Interchange Profile. If this bit is set to '1', the terminal shall use the cardholder verification related data in the ICC to determine whether one of the issuer-specified cardholder verification methods (CVMs) shall be executed. This process is described below.

Sequence of Execution: This function may be performed any time after application selection and before completion of the terminal action analysis.

Description: The CVM List (tag '8E') is a composite data object consisting of the following:

1. An amount field (4 bytes, binary format), referred to as 'X' in the CVM Condition Codes (see Table A-4 in Annex A). 'X' is expressed in the Application Currency Code with implicit decimal point. For example, 123 (hexadecimal '7B') represents £1.23 when the currency code is '826'.

2. A second amount field (4 bytes, binary format), referred to as 'Y' in the CVM Condition Codes (see Table A-4 in Annex A). 'Y' is expressed in Application Currency Code with implicit decimal point. For example, 123 (hexadecimal '7B') represents £1.23 when the currency code is '826'.

3. A variable-length list of two-byte data elements called Cardholder Verification Rules (CVRs). Each CVR describes a CVM and the conditions under which that CVM should be applied (See Table A-3 and Table A-4 in Annex A).

If the CVM List is not present in the ICC, the terminal shall terminate cardholder verification without setting the 'Cardholder verification was performed' bit in the TSI. If the CVM List is present in the ICC, the terminal shall process each rule in the order in which it appears in the list according to the following specifications. Cardholder verification is completed when any one CVM is successfully performed or when the list is exhausted.

If any of the following are true:

- The conditions expressed in the second byte of a CVR are not satisfied, or

- The ICC data required by the condition (for example, the Application Currency Code) is not present, or

Date Reçue/Date Received 2022-04-27

- The CVM Condition Code is outside the range of codes understood by the terminal (which might occur if the terminal application program is at a different version level than the ICC application),

the terminal shall bypass the rule and proceed to the next. If there are no more CVRs in the list, cardholder verification has not been successful, and the terminal shall set the 'Cardholder verification was not successful' bit to '1' in the TVR.

If the conditions expressed in the second byte of a CVR are satisfied, the terminal shall attempt to perform the CVM if the CVM code is one of those listed in Annex A or is otherwise understood by the terminal. If the CVM is not among those listed and is not understood by the terminal, the terminal shall set the 'Unrecognised CVM' bit to '1' in the TVR.

If the CVM is performed successfully, cardholder verification is complete and successful. Otherwise, the terminal shall then examine b7 of byte 1 of the CVM field. If b7 is set to '1', processing continues with the next CVR, if one is present. If b7 is set to '0', or there are no more CVRs in the list, the terminal shall set the 'Cardholder verification was not successful' bit to '1' in the TVR and cardholder verification is complete.

When cardholder verification is completed, the 'Cardholder verification was performed' bit in TSI shall be set to '1'.

7.5.1 Offline PIN Processing

This section applies to the verification by the ICC of a plaintext or enciphered PIN presented by the terminal. cc>

cc>

If an offline PIN is the selected CVM as determined by the above process, offline PIN processing may not be successfully performed for any one of the following reasons:

- The terminal does not support offline PIN[6]. In this case, the terminal shall set to '1' the 'PIN entry required and PIN pad not present or not working' bit in the TVR. The terminal supports offline PIN, but the PIN pad is malfunctioning. In this case, the terminal shall set to '1' the 'PIN entry required and PIN pad not present or not working' bit in the TVR.

[6] This means that the terminal does not support either offline plaintext PIN verification or offline enciphered PIN verification. If the terminal supports at least one of these functions, it is considered to support offline PIN for the purposes of setting the TVR bits.

Date Reçue/Date Received 2022-04-27

- The terminal bypassed PIN entry at the direction of either the merchant or the cardholder. In this case, the 'PIN entry required, PIN pad present, but PIN was not entered' bit shall be set to '1' in the TVR.

- The PIN is blocked upon initial use of the VERIFY command (the ICC returns SW1 SW2 = '6983' or '6984' in response to the VERIFY command). In this case, the 'PIN Try Limit exceeded' bit shall be set to '1' in the TVR.

- The number of remaining PIN tries is reduced to zero (indicated by an SW1 SW2 of '63C0' in the response to the VERIFY command). In this case, the 'PIN Try Limit exceeded' bit shall be set to '1' in the TVR.

The only case in which offline PIN processing is considered successful is when the ICC returns an SW1 SW2 of '9000' in response to the VERIFY command.

7.5.2 Online PIN Processing

If online PIN processing is a required CVM as determined by the above process, the processing may not be successfully performed for any one of the following reasons:

- The terminal does not support online PIN. In this case, the terminal shall set to '1' the 'PIN entry required and PIN pad not present or not working' bit in the TVR.

- The terminal supports online PIN, but the PIN pad is malfunctioning. In this case, the terminal shall set to '1' the 'PIN entry required and PIN pad not present or not working' bit in the TVR.

- The terminal bypassed PIN entry at the direction of either the merchant or the cardholder. In this case, the 'PIN entry required, PIN pad present, but PIN was not entered' bit shall be set to '1' in the TVR.

If the online PIN is successfully entered, the terminal shall set to '1' the 'Online PIN entered' bit in the TVR. In this case, cardholder verification is considered successful and complete.

7.5.3 Signature Processing

If a (paper) signature is a required CVM as determined by the above process, the terminal shall determine success based upon the terminal's capability to support the signature process (see complementary payment systems documentation for additional information). If the terminal is able to support signature, the process is considered successful, and cardholder verification is complete.

7.5.4 Combination CVMs

Some CVMs require multiple verification methods (for example, offline PIN plus signature). For these CVMs, all methods in the CVM must be successful for cardholder verification to be considered successful.

Date Reçue/Date Received 2022-04-27

7.6 Terminal Risk Management

Purpose: Terminal risk management is that portion of risk management performed by the terminal to protect the acquirer, issuer, and system from fraud. It provides positive issuer authorisation for high-value transactions and ensures that transactions initiated from ICCs go online periodically to protect against threats that might be undetectable in an offline environment. The result of terminal risk management is the setting of appropriate bits in the TVR.

Conditions of Execution: Terminal risk management shall be performed if the 'Terminal risk management is supported' bit is set to '1' in the Application Interchange Profile. Random transaction selection need not be performed by a terminal with no online capability. If terminal risk management is not performed, sections 7.6.1 through 7.6.3 do not apply.

Sequence of Execution: Terminal risk management may be performed at any time prior to issuing the first GENERATE AC command.

Description: Terminal risk management consists of:

- Floor limit checking
- Random transaction selection
- Velocity checking

7.6.1 Floor Limits

To prevent split sales, the terminal may have a transaction log of approved transactions stored in the terminal consisting of at least the Application PAN and transaction amount and possibly the Application PAN Sequence Number and Transaction Date. The number of transactions to be stored and maintenance of the log is outside the scope of this specification, although to prevent split sales the number of transactions stored may be quite small.

During terminal risk management floor limit checking, the terminal checks the transaction log (if available) to determine if there is a log entry with the same Application PAN, and, optionally, the same Application PAN Sequence Number. If there are several log entries with the same PAN, the terminal selects the most recent entry. The terminal adds the Amount, Authorised for the current transaction to the amount stored in the log for that PAN to determine if the sum exceeds the Terminal Floor Limit. If the sum is greater than or equal to the Terminal Floor Limit, the terminal sets the 'Transaction exceeds floor limit' bit to '1' in the TVR.

If the terminal does not have a transaction log available or if there is no log entry with the same PAN, the Amount, Authorised is compared to the appropriate floor limit. If the amount authorised is equal to or greater than the floor limit, the 'Transaction exceeds floor limit' bit is set to '1' in the TVR.

Date Reçue/Date Received 2022-04-27

7.6.2 Random Transaction Selection

For each application the relevant payment system specifies, in addition to the floor limit:

- Target Percentage to be Used for Random Selection (in the range of 0 to 99)
- Threshold Value for Biased Random Selection (which must be zero or a positive number less than the floor limit)
- Maximum Target Percentage to be Used for Biased Random Selection (also in the range of 0 to 99 but at least as high as the previous Target Percentage for Random Selection). This is the desired percentage of transactions 'just below' the floor limit that will be selected by this algorithm.

Any transaction with a transaction amount less than the Threshold Value for Biased Random Selection will be subject to selection at random without further regard for the value of the transaction. The terminal shall generate a random number in the range of 1 to 99. If this random number is less than or equal to the Target Percentage to be Used for Random Selection, the transaction shall be selected.

Any transaction with a transaction amount equal to or greater than the Threshold Value for Biased Random Selection but less than the floor limit will be subject to selection with bias toward sending higher value transactions online more frequently (biased random selection). For these transactions, the terminal shall compare its generated random number against a Transaction Target Percent, which is a linear interpolation of the target percentages provided by the payment system (Target Percentage to be Used for Random Selection, and Maximum Target Percentage to be Used for Biased Random Selection).[7] If the random number is less than or equal to the Transaction Target Percent, the transaction shall be selected.

The probability of selection as a function of the transaction amount may be charted as shown in Figure 2:

[7] The Transaction Target Percent is calculated as follows:

$$\text{Interpolation factor} = \frac{\text{Amount, Authorised} - \text{Threshold Value}}{\text{Floor Limit} - \text{Threshold Value}}$$

$$\text{Transaction Target Percent} = \left(\left(\text{Maximum Target Percent} - \text{Target Percent}\right) \times \text{Interpolation factor}\right) + \text{Target Percent}$$

Date Reçue/Date Received 2022-04-27

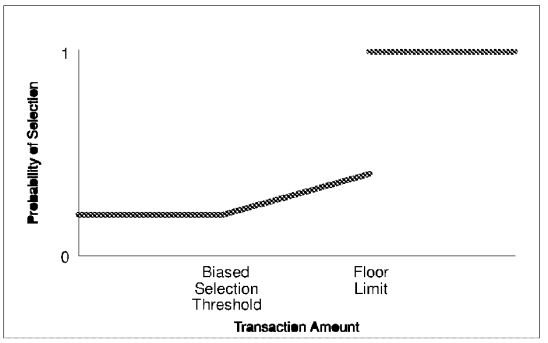


Figure 2 - Random Selection Probability (not to scale)

If the transaction is selected through the process described in this section, the 'Transaction selected randomly for online processing' bit shall be set to '1' in the TVR.

7.6.3 Velocity Checking[8]

If both the Lower Consecutive Offline Limit (tag '9F14') and Upper Consecutive Offline Limit (tag '9F23') exist, the terminal shall perform velocity checking as described in this section. If either of these data objects is not present in the ICC application, the terminal shall skip this section.

The ATC and Last Online ATC Register shall be read from the ICC using GET DATA commands. If either of the required data objects are not returned by the ICC in response to the GET DATA command, the terminal shall:

- Set both the 'Lower consecutive offline limit exceeded' and the 'Upper consecutive offline limit exceeded' bits to '1' in the TVR.
- Not set the 'New card' indicator in the TVR.
- End velocity checking for this transaction.

[8] The purpose of velocity checking is to allow an issuer to request that, after a certain number of consecutive offline transactions (the Lower Consecutive Offline Limit), transactions should be completed online. However, if the terminal is incapable of going online, transactions may still be completed offline until a second (Upper Consecutive Offline Limit) limit is reached. After the upper limit is reached, the recommendation of the issuer might be to reject any transaction that cannot be completed online. Once a transaction has been completed online with successful issuer authentication, the count begins anew, so that transactions may be processed offline until the lower limit is once again reached.

Date Reçue/Date Received 2022-04-27

If the required data objects are available, the terminal shall compare the difference between the ATC and the Last Online ATC Register with the Lower Consecutive Offline Limit to see if the limit has been exceeded. If the difference is equal to the Lower Consecutive Offline Limit, this means that the limit has not yet been exceeded. If the limit has been exceeded, the terminal shall set the 'Lower consecutive offline limit exceeded' bit to '1' in the TVR and also compare the difference with the Upper Consecutive Offline Limit to see if the upper limit has been exceeded. If it has, the terminal shall set the 'Upper consecutive offline limit exceeded' bit to '1' in the TVR.

The terminal shall also check the Last Online ATC Register for a zero value. If it is zero, the terminal shall set the 'New card' bit to '1' in the TVR.

Upon completion of terminal risk management, the terminal shall set to '1' the 'Terminal risk management was performed' bit in the TSI.

7.7 Terminal Action Analysis

Purpose: Once terminal risk management and application functions related to a normal offline transaction have been completed, the terminal makes the first decision as to whether the transaction should be approved offline, declined offline, or transmitted online. If the outcome of this decision process is to proceed offline, the terminal issues a GENERATE AC command to ask the ICC to return a TC. If the outcome of the decision is to go online, the terminal will issue a GENERATE AC command to ask the ICC for an Authorisation Request Cryptogram (ARQC). If the decision is to reject the transaction, the terminal will issue a GENERATE AC to ask for an Application Authentication Cryptogram (AAC).

An offline decision made here is not final. If the terminal asks for a TC from the ICC, the ICC, as a result of card risk management, may return an ARQC or AAC.

Conditions of Execution: The terminal action analysis function is always performed.

Sequence of Execution: The terminal action analysis function is performed after terminal risk management and cardholder- and merchant-entered transaction data has been completed. It shall be performed prior to the first use of the GENERATE AC command.

The Issuer Action Code - Default and Terminal Action Code - Default processing described below shall also be performed after online processing is attempted in the case where the terminal was unable to process the transaction online.

The terminal action analysis function may be executed at several places during a transaction to eliminate the need for unnecessary processing. If any processing results in the setting of a bit in the TVR (for example, failure of cardholder verification), it may be desirable to perform this function immediately to determine whether the transaction should be rejected offline based upon the issuer's parameters in the ICC or the acquirer's parameters in the terminal. Recognition of

Date Reçue/Date Received 2022-04-27

such a decision early in processing may allow the terminal to avoid prolonging a transaction that will ultimately be rejected. Multiple executions of this decision process is optional on the part of the terminal.

Description: The terminal shall make a preliminary decision to reject the transaction, complete it online, or complete it offline based upon the TVR, issuer action preferences, and acquirer action preferences according to the method described in this section.

The ICC contains (optionally) three data elements to reflect the issuer's selected action to be taken based upon the content of the TVR. Each of the three data elements has defaults specified here in case any of these data elements are absent from the ICC. The three data elements are:

- Issuer Action Code - Denial
- Issuer Action Code - Online
- Issuer Action Code - Default

Collectively, these three data objects are termed the Issuer Action Codes. The purpose of each is described in this section below. The format of each is identical and mirrors the TVR. Each has one bit corresponding to each bit in the TVR, and the Issuer Action Code bit specifies an action to be taken if the corresponding bit in the TVR is set to '1'. Thus, the size and format of each of the Issuer Action Codes is identical to the TVR.

Similarly, the terminal may contain three data elements to reflect the acquirer's selected action to be taken based upon the content of the TVR. These data elements are:

- Terminal Action Code - Denial
- Terminal Action Code - Online
- Terminal Action Code - Default

Collectively, these three data objects are termed the Terminal Action Codes. The purpose of each is described in this section below. The format of each is identical and mirrors the TVR. Each has one bit corresponding to each bit in the TVR, and the Terminal Action Code bit specifies an action to be taken if the corresponding bit in the TVR is set to '1'. Thus, the size and format of each of the Terminal Action Codes is identical to the TVR and to the Issuer Action Codes.

The existence of each of the Terminal Action Codes is optional. In the absence of any Terminal Action Code, a default value consisting of all bits set to '0' is to be used in its place. However, it is strongly recommended that as a minimum, the Terminal Action Code - Online and Terminal Action Code - Default should be included with the bits corresponding to 'Offline data authentication was not performed', 'Offline

Date Reçue/Date Received 2022-04-27

static data authentication failed', and 'Offline dynamic data authentication failed' set to '1'.[9]

Processing of the action codes is done in pairs, that is, the Issuer Action Code - Denial is processed together with the Terminal Action Code - Denial, the Issuer Action Code - Online is processed together with the Terminal Action Code - Online, and the Issuer Action Code - Default is processed together with the Terminal Action Code - Default. Processing of the action codes shall be performed in the order specified here.

If the Issuer Action Code - Denial does not exist, a default value with all bits set to '0' is to be used. Together, the Issuer Action Code - Denial and the Terminal Action Code - Denial specify the conditions that cause denial of a transaction without attempting to go online. If either data object exists, the terminal shall inspect each bit in the TVR. For each bit in the TVR that has a value of '1', the terminal shall check the corresponding bits in the Issuer Action Code - Denial and the Terminal Action Code - Denial. If the corresponding bit in either of the action codes is set to '1', it indicates that the issuer or the acquirer wishes the transaction to be rejected offline. In this case, the terminal shall issue a GENERATE AC command to request from the ICC an AAC. This AAC may be presented to the issuer to prove card presence during this transaction, but details of handling a rejected transaction are outside the scope of this specification.

If the Issuer Action Code - Online is not present, a default value with all bits set to '1' shall be used in its place. Together, the Issuer Action Code - Online and the Terminal Action Code - Online specify the conditions that cause a transaction to be completed online. These data objects are meaningful only for terminals capable of online processing. Offline-only terminals may skip this test and proceed to checking the Issuer Action Code - Default and Terminal Action Code - Default, described below. For a terminal capable of online processing, if the terminal has not already decided to reject the transaction as described above, the terminal shall inspect each bit in the TVR. For each bit in the TVR that has a value of '1', the terminal shall check the corresponding bits in both the Issuer Action Code - Online and the Terminal Action Code - Online. If the bit in either of the action codes is set to '1', the terminal shall complete transaction processing online and shall issue a GENERATE AC command requesting an ARQC from the ICC.

If the Issuer Action Code - Default does not exist, a default value with all bits set to '1' shall be used in its place. Together, the Issuer Action Code - Default and the Terminal Action Code - Default specify the conditions that cause the transaction to be rejected if it might have been approved online but the terminal is for any reason unable to process the transaction online. The Issuer Action Code - Default and the Terminal Action Code - Default are used only if the Issuer Action Code - Online and

[9] This protects against a fraudulent card with all the bits in the Issuer Action Code set to '0'. Without this protection, such a card could be created with no possibility of going online or declining transactions. All transactions would be approved offline.

Date Reçue/Date Received 2022-04-27

the Terminal Action Code - Online were not used (for example, in case of an offline-only terminal) or indicated a desire on the part of the issuer or the acquirer to process the transaction online but the terminal was unable to go online. If the terminal has not already rejected the transaction and the terminal is for any reason unable to process the transaction online, the terminal shall use this code to determine whether to approve or reject the transaction offline. If any bit in Issuer Action Code - Default or the Terminal Action Code - Default and the corresponding bit in the TVR are both set to '1', the transaction shall be rejected and the terminal shall request an AAC to complete processing. If no such condition appears, the transaction may be approved offline, and a GENERATE AC command shall be issued to the ICC requesting a TC.

7.8 Card Action Analysis

Purpose: An ICC may perform its own risk management to protect the issuer from fraud or excessive credit risk. Details of card risk management algorithms within the ICC are specific to the issuer and are outside the scope of this specification, but as a result of the risk management process, an ICC may decide to complete a transaction online or offline or request a referral or reject the transaction. The ICC may also decide that an advice message should be sent to the issuer to inform the issuer of an exceptional condition.

Conditions of Execution: The card online/offline decision is specified by its response to the GENERATE AC command. Therefore, this section applies to all transactions. Whether the ICC performs any risk management tests is transparent to the terminal and outside the scope of this specification.

Sequence of Execution: The card action analysis process is performed when the terminal issues the GENERATE AC command for a given transaction.

Description: The result of risk management performed by the ICC is a decision for one of the following actions to be taken by the terminal:

- Approve the transaction offline. This option is available to the ICC only if the terminal has made a preliminary decision to complete the transaction offline, as described in section 7.7.
- Complete the transaction online.
- Request a referral.
- Reject the transaction.

The decision by the ICC is made known to the terminal by returning either a TC, an ARQC, an AAR, or an AAC to the terminal in response to a GENERATE AC command, as described in section 8.

Upon the completion of the card action analysis function, the terminal shall set to '1' the 'Card risk management was performed' bit in the TSI.

Date Reçue/Date Received 2022-04-27

7.8.1 Terminal Messages for an AAC

An AAC returned by the card indicates either a rejection of the specific transaction or a restriction that disallows use of the card in the environment of the transaction (for example, the card application may be restricted only to specific merchant categories). In both cases, the card disapproves the transaction, but the terminal may choose to display different messages in the two cases. The card may optionally distinguish the cases by the use of the code returned in the Cryptogram Information Data (see the GENERATE AC command in the Card Specification). If an AAC is returned with b3-b1 = '001' in the Cryptogram Information Data, the AAC was returned due to card restrictions.

7.8.2 Advice Messages

The issuer may wish for an advice message, separate from either an authorisation request or a clearing message, to be sent in certain exception cases. (Currently, the only identified such case is 'PIN Try Limit exceeded', but allowance has been made for the addition of other cases later; see 'Coding of Cryptogram Information Data' in the GENERATE AC command in the Card Specification).

If b4 of the Cryptogram Information Data is '1', the terminal shall format and send an advice message. Further information may be found in complementary payment system documentation and in the Terminal Specification.

7.9 Online Processing

Purpose: Online processing is performed to ensure that the issuer can review and authorise or reject transactions that are outside acceptable limits of risk defined by the issuer, the payment system, or the acquirer.

Conditions of Execution: Online processing shall be performed if the ICC returns an ARQC in response to the first GENERATE AC command for the transaction.

Sequence of Execution: The online processing function is performed when the terminal receives an ARQC in response to the first GENERATE AC command.

Description: In general, online processing is the same as today's online processing of magnetic stripe transactions and is not described here. This section is limited to the additional online processing provided in an ICC environment that is not available in a magnetic stripe environment.

The ARQC may be sent in the authorisation request message.[10] The authorisation response message from the issuer may contain the Issuer Authentication Data (tag

[10] Actions performed by the acquirer or issuer systems are outside the scope of this specification. However, an explanation of what is expected to take place at the issuer may be useful for clarity. The ARQC is a cryptogram generated by the card from transaction

Date Reçue/Date Received 2022-04-27

'91'). If the Issuer Authentication Data is received in the authorisation response message and the Application Interchange Profile indicates that the ICC supports issuer authentication, the Issuer Authentication Data shall be sent to the ICC in the EXTERNAL AUTHENTICATE command. If the ICC responds with SW1 SW2 other than '9000', the 'Issuer authentication was unsuccessful' bit shall be set to '1' in the TVR.

If the Issuer Authentication Data is received but the Application Interchange Profile indicates that the ICC does not support issuer authentication, this indicates that the ICC has combined the issuer authentication function with the GENERATE AC command. In this case, or if no Issuer Authentication Data is received, the terminal shall not execute the EXTERNAL AUTHENTICATE command.

The ICC shall permit at most one EXTERNAL AUTHENTICATE command in a transaction. If the terminal issues more than one, the second and all succeeding EXTERNAL AUTHENTICATE commands shall end with SW1 SW2 = '6985'.

Upon completion of online processing, if the EXTERNAL AUTHENTICATE command was sent to the card by the terminal, the terminal shall set to '1' the 'Issuer authentication was performed' bit in the TSI.

7.10 Issuer-to-Card Script Processing

Purpose: An issuer may provide command scripts to be delivered to the ICC by the terminal to perform functions that are not necessarily relevant to the current transaction but are important for the continued functioning of the application in the ICC. Multiple scripts may be provided with an authorisation response, and each may contain any number of Issuer Script Commands. Script processing is provided to allow for functions that are outside the scope of this specification but are nonetheless necessary.[11]

---

data using an issuer key stored in the card and known at the issuer authorisation system. The issuer uses this key to authenticate the ARQC and thereby authenticate the card. This process is termed 'online card authentication' or simply 'card authentication'.

Subsequent to card authentication, the issuer may generate a cryptogram on selected data included in the authorisation response or already known to the card. This cryptogram is sent to the terminal in the authorisation response as part of the Issuer Authentication Data. The terminal provides the Issuer Authentication Data to the ICC in the EXTERNAL AUTHENTICATE command or the second GENERATE AC command, as described in the Card Specification. The ICC may use the Issuer Authentication Data to authenticate that the response message originated from the issuer.

[11] An example might be unblocking of an offline PIN, which might be done differently by various issuers or payment systems.

Date Reçue/Date Received 2022-04-27

A script may contain Issuer Script Commands not known to the terminal, but each command shall be delivered by the terminal to the ICC individually according to this specification.

Conditions of Execution: None.

Sequence of Execution: Two separate script tags are defined that are available for use by the issuer. Issuer scripts with tag '71' shall be processed prior to issuing the final GENERATE AC command. Issuer scripts using tag '72' shall be processed after issuing the final GENERATE AC command.

Description: An Issuer Script is a constructed data object (tag '71' or '72') containing (optionally) a Script Identifier and a sequence of Issuer Script Command APDUs to be delivered serially to the ICC. The Script Identifier is optional and is not interpreted by the terminal; it is meaningful only to the issuer. Figure 3 and Figure 4 illustrate an Issuer Script containing a Script Identifier and three commands.

T	L	T	L	Script ID	Commands
'71' or '72'	L(∑data, including Script ID, tags, and lengths)	'9F18'	'04'	Identifier (4 bytes)	(see Figure 4)

Figure 3 - Issuer Script Format

T_1	L_1	V_1	T_2	L_2	V_2	T_3	L_3	V_3
'86'	$L(V_1)$	Command	'86'	$L(V_2)$	Command	'86'	$L(V_3)$	Command

Figure 4 - Issuer Script Command Format (Shown with Three Commands)

It is possible for multiple Issuer Scripts to be delivered with a single authorisation response. Each Issuer Script shall be processed by the terminal in the sequence in which it appears in the authorisation response according to the following rules:

- Issuer Script Commands shall be separated using the BER-TLV coding of the data objects defining the commands (tag '86').
- Each command will be delivered to the ICC as a command APDU in the sequence in which it appeared in the Issuer Script.
- The terminal shall examine only SW1 in the response APDU and perform one of the following actions:
  - If SW1 indicates either normal processing or a 'warning' according to the conventions described in the Card Specification, the terminal shall continue with the next command from the Issuer Script (if any).

Date Reçue/Date Received 2022-04-27

- If SW1 indicates an 'error' condition, the processing of the Issuer Script shall be terminated.

If an Issuer Script is processed, the terminal shall set the 'Script processing was performed' bit in the TSI to '1'. If an error occurred in processing a script, the terminal shall set to '1' either the 'Script processing failed before final GENERATE AC' in the TVR if the identifying tag of the failing script was '71' or the 'Script processing failed after final GENERATE AC' in the TVR if the tag was '72'.

7.11 Completion

Purpose: The completion function closes processing of a transaction.

Conditions of Execution: This function is always performed by the terminal unless the transaction is terminated prematurely by error processing.

Sequence of Execution: The completion function is always the last function in the transaction processing. (Script processing may be performed after the completion function.)

Description: The ICC indicates willingness to complete transaction processing by returning either a TC or an AAC to either the first or second GENERATE AC command issued by the terminal. If the terminal decides to go online, completion shall be done when the second GENERATE AC command is issued.

See section 8 for additional information on the use of the GENERATE AC command.

Date Reçue/Date Received 2022-04-27

8. GENERATE AC Command Coding

The GENERATE AC command format and response codes are described fully in the Card Specification. This section describes how the various options and data elements are used in transaction processing. Figure 5 and Figure 6 depict the interaction between the terminal decisions, ICC decisions, issuer approval, the GENERATE AC command, and the possible ICC responses. Figure 5 describes the overall flow; Figure 6 provides the additional logic for referral transactions.

The complete transaction flow is not shown in these charts, only the GENERATE AC commands, responses, and associated decisions.

Date Reçue/Date Received 2022-04-27

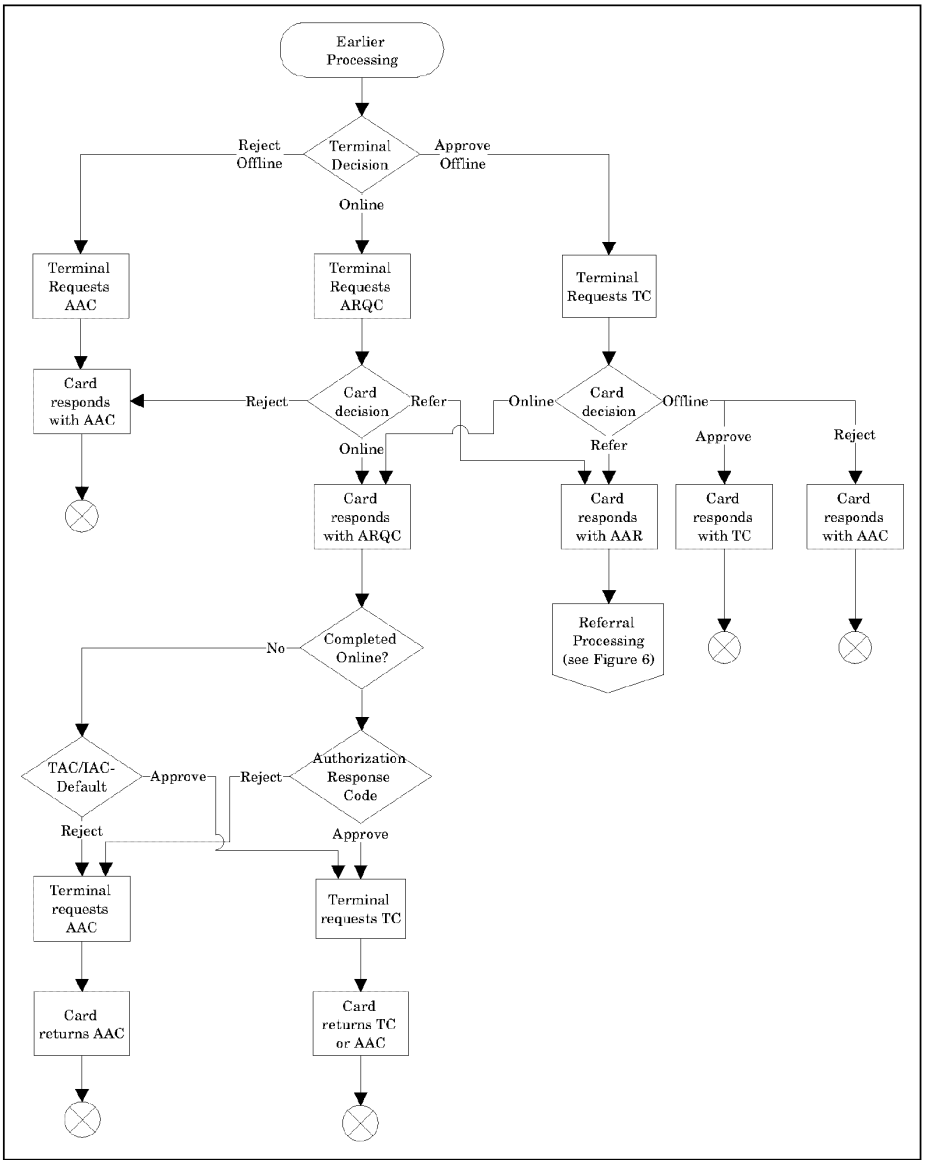


Figure 5 - Use of GENERATE AC Options cc>

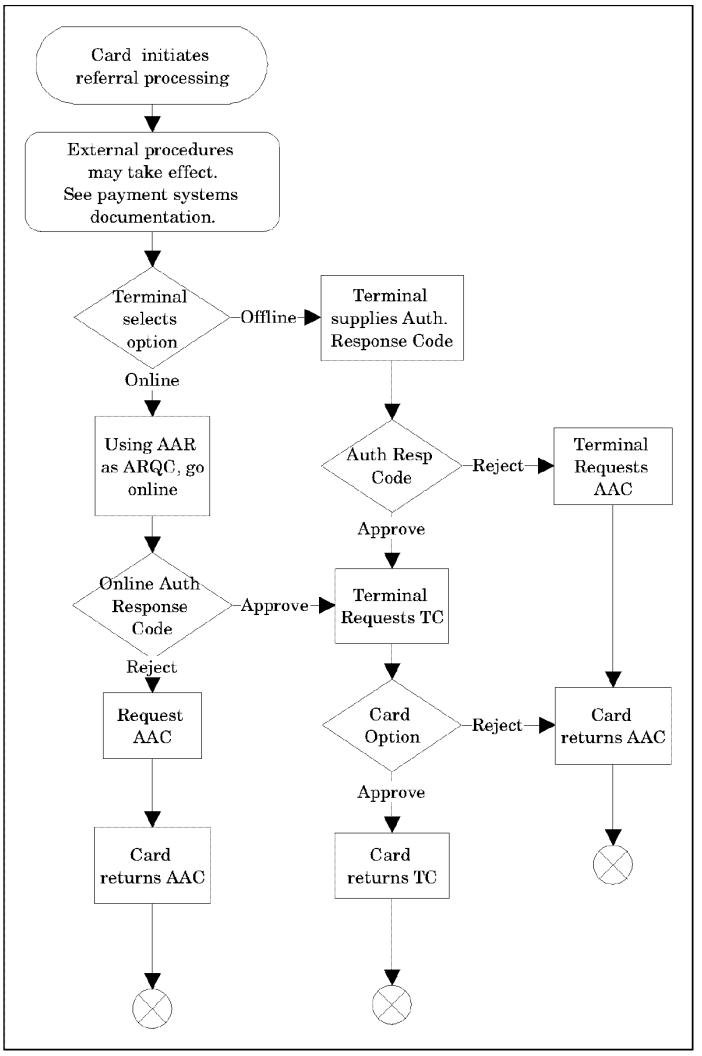


Figure 6 - Use of GENERATE AC with Referrals

Date Reçue/Date Received 2022-04-27

8.1 Command Parameters

The GENERATE AC command parameters provide three different options to the terminal:

- Request for the generation of a TC
- Request for the generation of an ARQC
- Request for the generation of an AAC

8.2 Command Data

The data field of the GENERATE AC command is not TLV encoded, so it is imperative that the ICC know the format of this data when the command is received. This is achieved by allowing the ICC to specify the format of the data to be included in the command. This section describes how the ICC makes that specification.

8.2.1 Card Risk Management Data

The Card Risk Management Data Object List (CDOL) is a data object in the ICC that provides to the terminal a list of data objects that must be passed from the terminal to the ICC in the GENERATE AC command. There shall be two CDOLs in the ICC, referred to as CDOL1 (tag '8C') and CDOL2 (tag '8D'). CDOL1 is used with the first GENERATE AC command, and CDOL2 is used with the second GENERATE AC command (if used). The terminal uses the appropriate CDOL and the rules specified in the Card Specification (see 'Rules for Processing Data Object Lists (DOLs)') to build the appropriate data field for the command. It is the responsibility of the terminal to ensure that current data is used in building the GENERATE AC command. To this end, the command data should be built immediately prior to issuing the GENERATE AC command.

8.2.2 Transaction Certificate Data

A CDOL may request a TC Hash Value to be included in the command data of a GENERATE AC command. The TDOL is a data object that provides to the terminal a list of data objects to be used in generating the TC Hash Value. The ICC may contain the TDOL, but there may be a default TDOL in the terminal, specified by the payment system, for use in case the TDOL is not present in the ICC. To create the hash value, the terminal shall use the TDOL (if present) or the default TDOL to create the appropriate value for input to the hash algorithm, applying the rules specified in the Card Specification (see 'Rules for Processing Data Object Lists (DOLs)'). If the default TDOL is used, the terminal shall set to '1' the 'Default TDOL used' bit in the TVR. If a default TDOL is required but is not present in the terminal, a default TDOL with no data objects in the list shall be assumed.

Date Reçue/Date Received 2022-04-27

If the terminal issues a second GENERATE AC command during the processing of a transaction, the terminal shall ensure that the data provided in the TC Hash Value is current at the time the command is issued.

8.3 Command Use

Either one or two GENERATE AC commands are issued during the processing of a transaction according to this specification.

The ICC shall respond to the first GENERATE AC command with any of the following:

- TC
- ARQC
- AAR
- AAC

The ICC shall respond to a second GENERATE AC command with either a TC or an AAC.

The possible responses listed above are in hierarchical order, with a TC being the highest and an AAC being the lowest. The terminal may request a TC, an ARQC, or an AAC. If the ICC responds with a cryptogram at a higher level, this indicates a logic error in the ICC. If this occurs after the first GENERATE AC command in a transaction, the transaction shall be terminated. If it occurs after the second GENERATE AC command, all processing for the transaction has been completed, and the cryptogram returned shall be treated as an AAC.

8.3.1 GENERATE AC (First Issuance)

The terminal completes its online/offline decision process with a GENERATE AC command (see Figure 5). The form of the command depends upon the decision made by the terminal:

- If the terminal decides the transaction might be completed offline, it requests a TC from the ICC. The ICC shall reply with a TC, an ARQC, an AAR, or an AAC, depending upon its own analysis of the transaction.
- If the terminal decides the transaction should go online, it requests an ARQC from the ICC. The ICC shall reply with an ARQC, an AAR, or an AAC.
- If the terminal decides to reject the transaction, it requests an AAC from the ICC. The ICC shall reply with an AAC.

If the ICC responds with a TC or an AAC, the terminal completes the transaction offline.

Date Reçue/Date Received 2022-04-27

If the ICC responds with an AAR, the terminal either provides an Authorisation Response Code and proceeds to the completion function or uses the AAR to go online. See Figure 6 for referral processing logic.

If the ICC responds with an ARQC, the terminal attempts to go online, sending an authorisation request message to the issuer. Included in the authorisation request message is the ARQC for online card authentication.

8.3.2 GENERATE AC (Second Issuance)

Whether the terminal receives an authorisation response message as a result of online processing or an approval or rejection by using the Issuer Action Code - Default, it completes the transaction by requesting either a TC (in the case an approval was obtained) or an AAC (in case the issuer's instruction is to reject the transaction) from the ICC. If a TC was requested, the ICC shall reply with either a TC or an AAC. If an AAC was requested, the card shall reply with an AAC.

The ICC shall permit at most two GENERATE AC commands in a transaction. If the terminal issues more than two, the third and all succeeding GENERATE AC commands shall end with SW1 SW2 = '6985', and no cryptogram shall be returned.

Date Reçue/Date Received 2022-04-27

9. Erroneous or Missing Data in the ICC

Data objects in the card are classified in section 5 as either mandatory or optional. However, some optional data objects must be present to support optional functions selected by the issuer or must be present to avoid inconsistencies if other related data objects are present.

When any mandatory data object is missing, the terminal terminates the transaction. When an optional data object is required because of the existence of other data objects or to support functions that must be performed due to the setting of bits in the Application Interchange Profile, the terminal sets to '1' the 'ICC data missing' indicator in the TVR.

Table 7 summarises the conditions under which this bit should be set to '1'. If none of the conditions in Table 7 apply, the bit shall be set to '0'. The setting of this bit is in addition to any other actions specified in other sections of this document.

Name	Tag	'ICC Data Missing' Shall Be Set If ...
Application Transaction Counter (ATC)	'9F36'	ATC is not returned by GET DATA command and both Lower and Upper Consecutive Offline Limit data objects are present
Cardholder Verification Method (CVM) List	'8E'	Not present and AIP indicates that cardholder verification is supported
Certification Authority Public Key Index	'8F'	Not present and AIP indicates offline static or dynamic data authentication is supported
Dynamic Data Authentication Data Object List (DDOL)	'9F49'	Not present and AIP indicates offline dynamic data authentication is supported
Issuer Public Key Certificate	'90'	Not present and AIP indicates offline static or dynamic data authentication is supported
Issuer Public Key Exponent	'9F32'	Not present and AIP indicates offline static or dynamic data authentication is supported
Issuer Public Key Remainder	'92'	Not present and AIP indicates offline static or dynamic data authentication is supported and the 'length of the Issuer Public Key', as recovered from the Issuer Public Key Certificate, indicates that there was insufficient space for the entire Issuer's Public Key in the certificate
Last Online Application Transaction Counter (ATC) Register	'9F13'	Last Online ATC Register is not returned by GET DATA command and both Lower and Upper Consecutive Offline Limits are present

Date Reçue/Date Received 2022-04-27

Signed Static Application Data	'93'	Not present and AIP indicates offline static data authentication is supported
ICC Public Key Certificate	'9F46'	Not present and AIP indicates offline dynamic data authentication is supported
ICC Public Key Exponent	'9F47'	Not present and AIP indicates offline dynamic data authentication is supported
ICC Public Key Remainder	'9F48'	Not present and AIP indicates offline dynamic data authentication is supported and the 'length of the ICC Public Key', as recovered from the ICC Public Key Certificate, indicates that there was insufficient space for the entire ICC's Public Key in the certificate

Table 7 - ICC Data Missing Indicator Setting

It is up to the issuer to ensure that data in the card is of the correct format, and no format checking is mandated on the part of the terminal. However, if in the course of normal processing the terminal recognises that data is incorrectly formatted, the terminal shall terminate processing. This rule includes (but is not limited to):

I. Constructed data objects that do not parse correctly.

II. Dates that are out of range (for example, months that are not in the range 1 to 12).

III. Other data that must be in a specific range of values but are not.

IV. CVM Lists with no CVRs.

V. Multiple occurrences of a data object that should only appear once.

VI. An AFL with no entries.

VII. An AFL entry with invalid syntax, that is, any one or more of the following:

A. An SFI of 0 or 31.

B. A starting record number of 0.

C. An ending record number less than the starting record number (byte 3 < byte 2).

D. Number of records participating in offline data authentication greater than the number of records (byte 4 > byte 3 - byte 2 + 1).

Date Reçue/Date Received 2022-04-27

THIS PAGE LEFT INTENTIONALLY BLANK

Date Reçue/Date Received 2022-04-27

Annexes

Date Reçue/Date Received 2022-04-27

Date Reçue/Date Received 2022-04-27

Annex A - Coding of Data Elements

This annex provides the coding for specific data elements used to control the transaction flow in the terminal or to record the status of processing for the transaction. In the tables, a '1' means that if that bit has the value '1', the corresponding 'Meaning' applies. An 'x' means that the bit does not apply.

Data (bytes or bits) indicated as RFU shall be set to '0'.

Date Reçue/Date Received 2022-04-27

A1. Application Interchange Profile

Byte 1 (Leftmost):

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Initiate[12]
x	1	x	x	x	x	x	x	Offline static data authentication is supported
x	x	1	x	x	x	x	x	Offline dynamic data authentication is supported
x	x	x	1	x	x	x	x	Cardholder verification is supported
x	x	x	x	1	x	x	x	Terminal risk management is to be performed
x	x	x	x	x	1	x	x	Issuer authentication is supported
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Byte 2 (Rightmost):

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	x	x	x	x	x	x	RFU
x	0	x	x	x	x	x	x	RFU
x	x	0	x	x	x	x	x	RFU
x	x	x	0	x	x	x	x	RFU
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table A-1 - Application Interchange Profile

[12] This version of this specification does not describe processing in the case where this bit is set to '1'.

Date Reçue/Date Received 2022-04-27

A2. Application Usage Control

Byte 1 (Leftmost):

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Valid for domestic cash transactions
x	1	x	x	x	x	x	x	Valid for international cash transactions
x	x	1	x	x	x	x	x	Valid for domestic goods
x	x	x	1	x	x	x	x	Valid for international goods
x	x	x	x	1	x	x	x	Valid for domestic services
x	x	x	x	x	1	x	x	Valid for international services
x	x	x	x	x	x	1	x	Valid at ATMs
x	x	x	x	x	x	x	1	Valid at terminals other than ATMs

Byte 2 (Rightmost):

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Domestic cashback allowed
x	1	x	x	x	x	x	x	International cashback allowed
x	x	0	x	x	x	x	x	RFU
x	x	x	0	x	x	x	x	RFU
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table A-2 - Application Usage Control

Date Reçue/Date Received 2022-04-27

A3. Cardholder Verification Rule Format

Byte 1 (Leftmost): Cardholder Verification Method (CVM) Codes

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0								RFU
	0							Fail cardholder verification if this CVM is unsuccessful
	1							Apply succeeding CVR if this CVM is unsuccessful
		0	0	0	0	0	0	Fail CVM processing
		0	0	0	0	0	1	Plaintext PIN verification performed by ICC
		0	0	0	0	1	0	Enciphered PIN verified online
		0	0	0	0	1	1	Plaintext PIN verification performed by ICC and signature (paper)
		0	0	0	1	0	0	Enciphered PIN verification performed by ICC
		0	0	0	1	0	1	Enciphered PIN verification performed by ICC and signature (paper)
		0	x	x	x	x	x	Values in the range 000110-011101 reserved for future use by this specification
		0	1	1	1	1	0	Signature (paper)
		0	1	1	1	1	1	No CVM required
		1	0	x	x	x	x	Values in the range 100000-101111 reserved for use by the individual payment systems
		1	1	x	x	x	x	Values in the range 110000-111110 reserved for use by the issuer
		1	1	1	1	1	1	This value is not available for use

Table A-3 - CVM Codes

Date Reçue/Date Received 2022-04-27

Value	Meaning
'00'	Always
'01'	If cash or cashback
'02'	If not cash or cashback
'03'	If terminal supports the CVM[13]
'04' - '05'	RFU
'06'	If transaction is in the application currency[14] and is under X value
'07'	If transaction is in the application currency and is over X value
'08'	If transaction is in the application currency and is under Y value
'09'	If transaction is in the application currency and is over Y value
'0A' - '7F'	RFU
'80' - 'FF'	Reserved for use by individual payment systems

Table A-4 - CVM Condition Codes

[13] In the case of offline PIN CVM, this means 'If offline PIN pad present'. In the case of online PIN CVM, this means 'If online PIN pad present'.

[14] That is, Transaction Currency Code = Application Currency Code.

Date Reçue/Date Received 2022-04-27

A4. Issuer Code Table Index

Value	Refers to
'01'	Part 1 of ISO 8859
'02'	Part 2 of ISO 8859
'03'	Part 3 of ISO 8859
'04'	Part 4 of ISO 8859
'05'	Part 5 of ISO 8859
'06'	Part 6 of ISO 8859
'07'	Part 7 of ISO 8859
'08'	Part 8 of ISO 8859
'09'	Part 9 of ISO 8859
'10'	Part 10 of ISO 8859

Table A-5 - Issuer Code Table Index

Date Reçue/Date Received 2022-04-27

A5. Terminal Verification Results

Byte 1: (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Offline data authentication was not performed
x	1	x	x	x	x	x	x	Offline static data authentication failed
x	x	1	x	x	x	x	x	ICC data missing
x	x	x	1	x	x	x	x	Card appears on terminal exception file[15]
x	x	x	x	1	x	x	x	Offline dynamic data authentication failed
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Byte 2:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	ICC and terminal have different application versions
x	1	x	x	x	x	x	x	Expired application
x	x	1	x	x	x	x	x	Application not yet effective
x	x	x	1	x	x	x	x	Requested service not allowed for card product
x	x	x	x	1	x	x	x	New card
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

[15] There is no requirement in this specification for an exception file, but it is recognised that some terminals may have this capability.

Date Reçue/Date Received 2022-04-27

Byte 3:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Cardholder verification was not successful
x	1	x	x	x	x	x	x	Unrecognised CVM
x	x	1	x	x	x	x	x	PIN Try Limit exceeded
x	x	x	1	x	x	x	x	PIN entry required and PIN pad not present or not working
x	x	x	x	1	x	x	x	PIN entry required, PIN pad present, but PIN was not entered
x	x	x	x	x	1	x	x	Online PIN entered
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Byte 4:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Transaction exceeds floor limit
x	1	x	x	x	x	x	x	Lower consecutive offline limit exceeded
x	x	1	x	x	x	x	x	Upper consecutive offline limit exceeded
x	x	x	1	x	x	x	x	Transaction selected randomly for online processing
x	x	x	x	1	x	x	x	Merchant forced transaction online
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Date Reçue/Date Received 2022-04-27

Byte 5 (Rightmost):

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Default TDOL used
x	1	x	x	x	x	x	x	Issuer authentication was unsuccessful
x	x	1	x	x	x	x	x	Script processing failed before final GENERATE AC
x	x	x	1	x	x	x	x	Script processing failed after final GENERATE AC
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table A-6 - Terminal Verification Results

Date Reçue/Date Received 2022-04-27

A6. Transaction Status Information

Byte 1 (Leftmost):

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Offline data authentication was performed
x	1	x	x	x	x	x	x	Cardholder verification was performed
x	x	1	x	x	x	x	x	Card risk management was performed
x	x	x	1	x	x	x	x	Issuer authentication was performed
x	x	x	x	1	x	x	x	Terminal risk management was performed
x	x	x	x	x	1	x	x	Script processing was performed
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Byte 2 (Rightmost):

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	x	x	x	x	x	x	RFU
x	0	x	x	x	x	x	x	RFU
x	x	0	x	x	x	x	x	RFU
x	x	x	0	x	x	x	x	RFU
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table A-7 - Transaction Status Information

Date Reçue/Date Received 2022-04-27

US 20160156386A1

(19) **United States**

(12) **Patent Application Publication**

Van Nieuwenhuyze et al.

(10) **Pub. No.: US 2016/0156386 A1**

(43) **Pub. Date: Jun. 2, 2016**

(54) **DATA ACCESS IN A MOBILE DEVICE WITH NFC**

(71) Applicants: **PROTON WORLD INTERNATIONAL N.V.**, Zaventem (BE); **STMICROELECTRONICS (ROUSSET) SAS**, Rousset (FR)

(72) Inventors: **Olivier Van Nieuwenhuyze**, Wezembeek-Oppem (BE); **Alexandre Charles**, Auriol (FR)

(21) Appl. No.: **14/871,851**

(22) Filed: **Sep. 30, 2015**

(30) **Foreign Application Priority Data**

Nov. 28, 2014 (FR) 1461631

Publication Classification

(51) **Int. Cl.**

H04B 5/00 (2006.01)

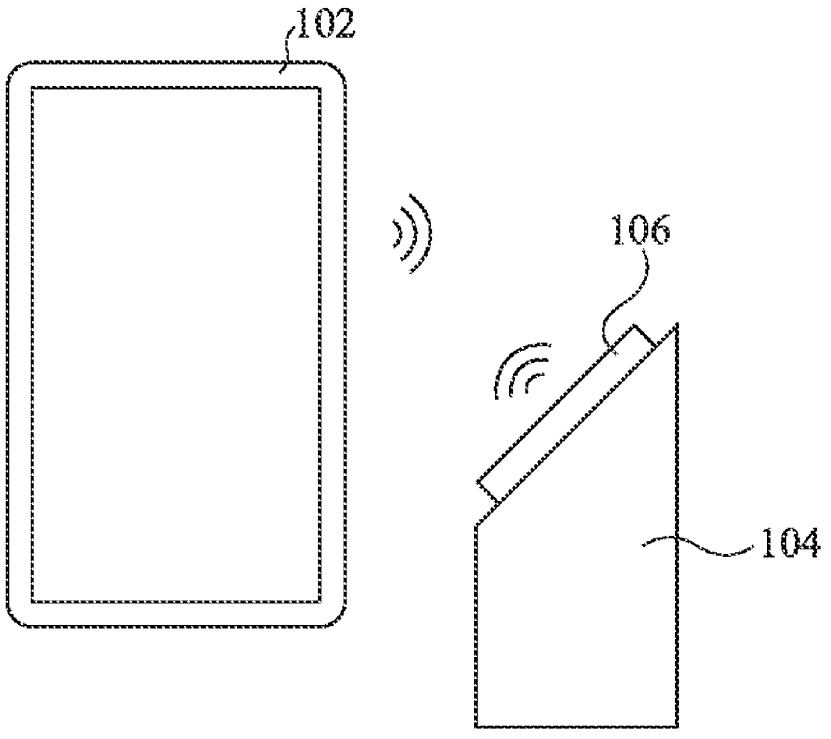
H04W 4/00 (2006.01)

(52) **U.S. Cl.**

CPC ***H04B 5/0031*** (2013.01); ***H04W 4/008*** (2013.01)

(57) **ABSTRACT**

The disclosure concerns an NFC (near field communications) device having an NFC router. The NFC router includes a memory adapted to store data to be shared with an external device and an NFC antenna circuit. The NFC router is capable of operating in a card emulation mode in which the shared data stored by the memory is accessible via the NFC antenna circuit.



Date Reçue/Date Received 2022-04-27

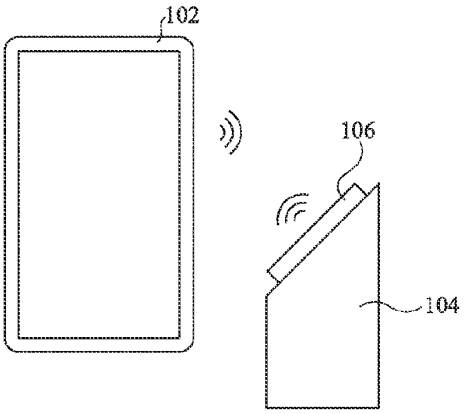


Fig 1

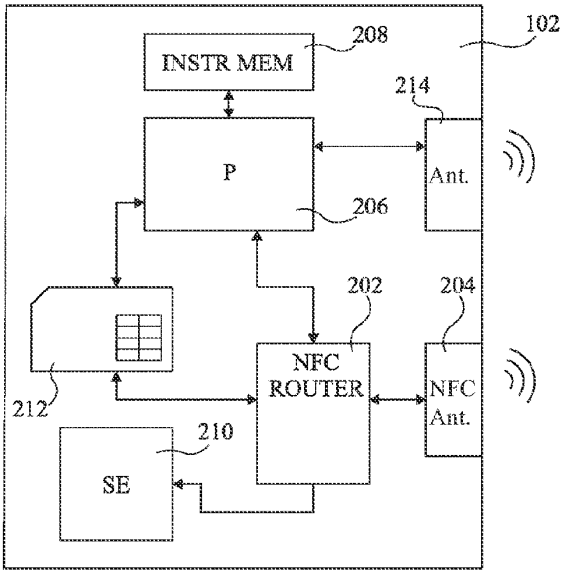


Fig 2

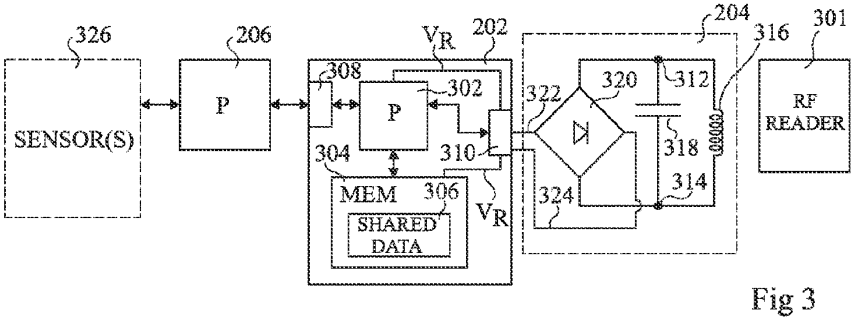


Fig 3

Date Reçue/Date Received 2022-04-27

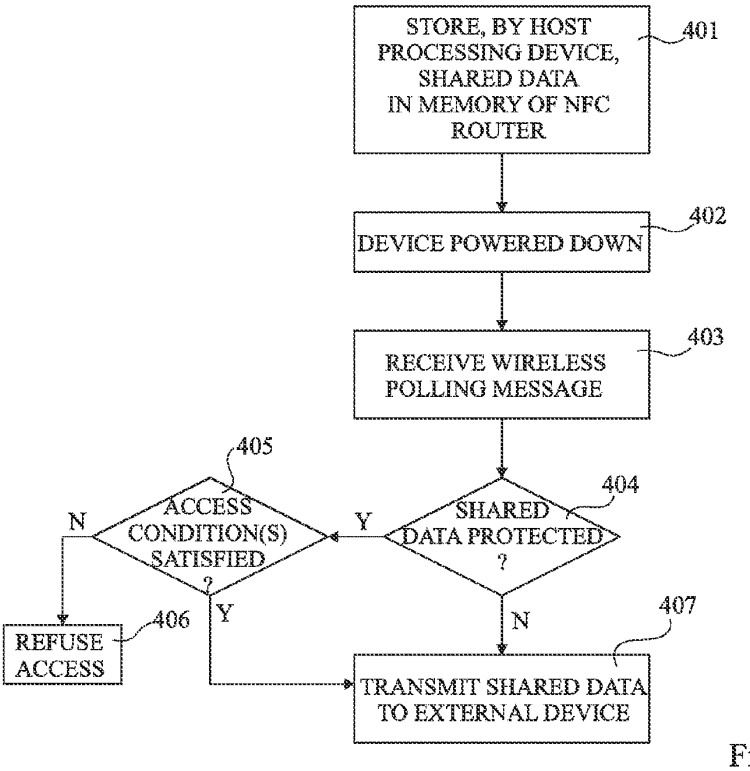


Fig 4

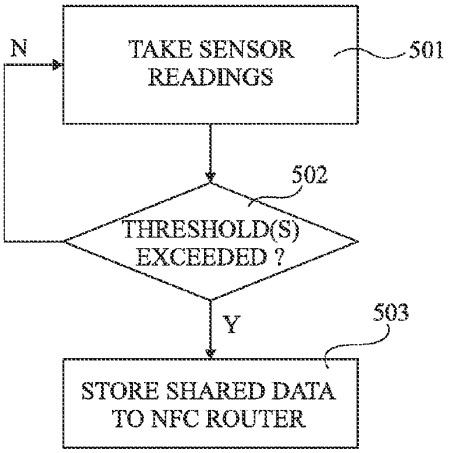


Fig 5

Date Reçue/Date Received 2022-04-27

DATA ACCESS IN A MOBILE DEVICE WITH NFC

[0001] This application claims the priority benefit of French Patent application number 14/61631, filed on Nov. 28, 2014, the contents of which is hereby incorporated by reference in its entirety to the maximum extent allowable by law.

BACKGROUND

[0002] 1. Technical Field

[0003] The present disclosure relates to the field of mobile communications devices, and in particular to a method and device for near field communications (NFC).

[0004] 2. Description of the Related Art

[0005] Mobile telephones and other types of mobile devices are increasingly being equipped with NFC (Near Field Communications) interfaces, which enable them to perform electromagnetic transponder functions over relatively short distances in addition to their other functions. In particular, such devices are able to emulate the functions of an electromagnetic transponder, which could be of the contactless card type, or the contactless reader type. Such functionality for example enhances the mobile device, by allowing it to be used for various applications, for example as an electronic wallet allowing payments to be made and/or by transport applications for accessing services such as transport networks.

[0006] To emulate the operation of a contactless card, the mobile device is generally equipped with a contactless front-end integrated circuit (CLF), also called an NFC router. This router is equipped with a radio frequency (RF) transceiver front-end coupled to a low-range antenna to match the communication capabilities of an electromagnetic transponder. In some applications, a secure element (SE) can be used to provide authentication.

[0007] In some cases it would be desirable for certain data held by the mobile device to be available even when the mobile device is no longer powered. For example, the host processor of the mobile telephone may be capable of performing card emulation, often referred to as "Host Card Emulation". However, if the mobile telephone is switched off, or if the battery is totally out of power, Host Card Emulation is not able to work. There is a technical problem permitting data held by the mobile device to be accessible irrespectively of whether or not the mobile device is powered.

BRIEF SUMMARY

[0008] It is an aim of embodiments of the present description to at least partially address one or more problems in the prior art.

[0009] According to one aspect, there is provided an NFC (near field communications) device comprising: an NFC router comprising a memory adapted to store data to be shared with an external device; and an NFC antenna circuit, wherein the NFC router is capable of operating in a card emulation mode in which the shared data stored by the memory is accessible via the NFC antenna circuit.

[0010] According to an embodiment, the NFC router is adapted to verify, in response to a request from an external device to access the shared data, one or more access conditions before transmitting the data to the external device via the NFC antenna circuit.

[0011] According to an embodiment, the NFC router is adapted to verify a first access condition by verifying a digital signature associated with the request.

[0012] According to an embodiment, the NFC router is coupled to a processor of the NFC device for receiving the shared data to be stored in said memory.

[0013] According to an embodiment, the NFC router is adapted to detect whether a device requesting to access the shared data is the processor of the NFC device or an external device, and to selectively apply one or more access conditions based on said detection.

[0014] According to an embodiment, the NFC router is adapted to apply a first access condition for access requests detected as coming from the processor of the NFC device, and a second access condition, different from the first access condition, for access requests detected as coming from an external device.

[0015] According to an embodiment, the one or more access conditions to be applied are selected based further on one or more of: the ON/OFF state of the NFC device; the charge state of a battery of the NFC device; whether the requested access to the shared data is a read or write request.

[0016] According to an embodiment, the shared data stored by the memory comprises first data accessible by an external device without any access condition and second data accessible by an external device only if one or more access conditions are satisfied.

[0017] According to an embodiment, the NFC device further comprises one or more sensors for detecting one or more environmental parameters, and the NFC router is adapted to store the data to be shared in said memory if a reading from at least one of the sensors exceeds a threshold.

[0018] According to an embodiment, the one or more sensors comprise at least one of: a humidity sensor; an accelerometer; a positioning device; and a temperature sensor.

[0019] According to a further aspect, there is provided a method comprising: storing, in a memory of a near field communications router of an NFC device, data to be shared with an external device; and during a card emulation mode, providing by the NFC router to the external device access to the shared data via an NFC antenna circuit.

[0020] According to an embodiment, the method further comprises: receiving by the NFC router a request from an external device to access the shared data; verifying, by the NFC router in response to the request, one or more access conditions; and transmitting the data to the external device if the one or more access conditions are satisfied.

[0021] According to an embodiment, verifying the one or more access conditions comprises verifying, by the NFC router, a digital signature associated with the request.

[0022] According to an embodiment, the method further comprises detecting, using one or more sensors, one or more environmental parameters, the storage of the data in the memory being triggered by a reading from at least one of the sensors exceeding a threshold.

[0023] According to an embodiment, the one or more environmental parameters comprise at least one of: a humidity level; an acceleration reading; a geographic position of the NFC device; and a temperature level.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0024] Non-limiting and non-exhaustive embodiments are described with reference to the following drawings, wherein

Date Reçue/Date Received 2022-04-27

like labels refer to like parts throughout the various views unless otherwise specified. One or more embodiments are described hereinafter with reference to the accompanying drawings.

[0025] The foregoing and other features and advantages will become apparent from the following detailed description of embodiments, given by way of illustration and not limitation with reference to the accompanying drawings, in which:

[0026] FIG. **1** schematically illustrates an NFC device capable of near field communications according to example embodiment of the present disclosure;

[0027] FIG. **2** schematically illustrates the NFC device of FIG. **1** in more detail according to example embodiment of the present disclosure;

[0028] FIG. **3** schematically illustrates a system for communications between the device of FIG. **2** and an RF reader according to example embodiment of the present disclosure;

[0029] FIG. **4** is a flow diagram illustrating operations in a method of accessing shared data using an NFC interface according to an example embodiment of the present disclosure; and

[0030] FIG. **5** is a flow diagram illustrating operations in a method of generating shared data.

DETAILED DESCRIPTION

[0031] FIG. **1** schematically illustrates an NFC device **102**, capable of NFC communications. For example, the device **102** is a mobile communications device, such as a mobile telephone, smartphone, a tablet computer, digital media player or the like, equipped with NFC circuitry.

[0032] The NFC device **102** of FIG. **1** is shown in a communication with a reader **104**, comprising an NFC transponder **106**. For example, the reader **104** is positioned at an entry barrier of a restricted area such as at the entrance to a transport network or the like. When used with such a reader, the NFC circuit of the NFC device **102** for example operates in a tag emulation mode.

[0033] FIG. **2** schematically illustrates the NFC device **102** in more detail according to example embodiment.

[0034] As illustrated, the device **102** for example comprises an NFC router (NFC ROUTER) **202**, also known in the art as a contactless front-end (CLF). The NFC router **202** is coupled to an NFC antenna circuit **204**, and together the router **202** and the antenna circuit **204** provide an NFC circuit for emulating the behavior of an NFC transponder.

[0035] The NFC router **202** is also for example coupled to a host processing device (P) **206** of the NFC device **102**. The processing device **206** for example comprises one or more processors under the control of instructions stored in an instruction memory (INSTR MEM) **208**. Memory **208** is for example a Flash memory, and stores one or more applications that have been loaded onto the device. The NFC router **202** is also for example coupled to other devices, including one or more secure elements. Each secure element may have one of several form factors, and in particular may be for example a UICC (universal integrated circuit card), an eUICC (embedded UICC), an embedded secure element (eSE) integrated in the mobile device or contained in a micro-circuit of the subscriber identification module (SIM), a universal SIM (USIM) or a μSD (micro secure digital). In the example of FIG. **2**, a secure element (SE) **210** and USIM (Universal Subscriber Identification Module) circuit **212** are illustrated. The USIM circuit **212** is for example coupled to the NFC router **202** via an SWP (single wire protocol) link, and is additionally coupled to the host processing device **206**.

[0036] The host processing device **206** is also for example coupled to one or more antenna circuits **214**, which for example permit telecommunications within a cellular network, and/or wireless communications according to other standards such as Wi-Fi, Bluetooth, etc.

[0037] FIG. **3** schematically illustrates a system for communications between the NFC device **102** of FIG. **2** and an RF reader (RF READER) **301**.

[0038] As illustrated, the NFC router **202** for example comprises a processing device (P) **302** coupled to a memory (MEM) **304** storing shared data (SHARED DATA) **306**. The memory **304** is for example a flash memory or EEPROM (electrically erasable programmable read-only memory), or other type of memory. The processing device **202** for example comprises one or more processors under the control of instructions also for example stored in the memory **304**. The processing device **302** is for example coupled via a suitable communications interface **308** to the host processing device **206** of the NFC device **102**. For example, the link between the processing device **206** and the NFC router **202** is a serial link, and the interface **308** provides serial to parallel conversion.

[0039] The processing device **302** is also coupled via a communications interface **310** to the NFC antenna circuit **204**.

[0040] The NFC antenna circuit **204** for example comprises nodes **312** and **314** coupled to an oscillating circuit formed of the parallel connection of an inductive element **316** that forms the antenna of the NFC antenna circuit **204**, and a capacitive element **318**. In alternative embodiments, the inductive element **316** could be coupled in series with the capacitive element **318**, which could be integrated in the NFC router **202**.

[0041] The nodes **312** and **314** of the NFC antenna circuit **204** are coupled to respective inputs of a rectifying bridge **320** having output lines **322** and **324** coupled to the communications interface **310**.

[0042] The communications interface **310** for example provides radio frequency coding and decoding. Additionally, the interface **310** for example generates a supply voltage V_R from the received signal when the NFC router **202** is operating in the card emulation mode in order to power the processing device **302** and the memory **304**.

[0043] In some embodiment, the processing device **206** is coupled to one or more sensors (SENSOR(S)) **326**, which for example monitor one or more environmental parameters. For example, the sensors **326** include a humidity detector, an accelerometer, a temperature sensor, and/or a positioning device such as a GPS (global positioning system) device.

[0044] In operation, when the NFC device **102** is powered, the memory **304** of the NFC router **202** is, for example, accessible by the processing device **206**. For example, the processing device **206** may write the shared data to the memory **304** and optionally be capable of reading the shared data from the memory **304**. Furthermore the memory **304** of the NFC router **202** is also for example accessible by an external device, such as the RF reader **301**, while the NFC device **102** is powered.

[0045] When the NFC device **102** is turned off or otherwise in a non-powered state, for example because its battery is discharged, the NFC router **202** for example operates in the card emulation mode in which a signal may be received from a card reader **301**. In this mode, the processor **302** and memory **304** are for example powered by the supply voltage

Date Reçue/Date Received 2022-04-27

V_R extracted from the received wireless signal. However, in some embodiments, for example if there is still power remaining in the battery, the processor **302** and memory **304** may be powered by the battery (not shown in FIG. **3**). The memory **304** is for example accessible in this mode by the external device, although one or more access conditions may be applied, as will be described in more detail below. Furthermore, in some embodiments, the memory **304** is accessible by external devices only for read operations, and not for write operations.

[0046] Thus, by transferring, by the host processing device **206** to the NFC router **202**, the data to be shared, card emulation can be used to access this data even if the NFC device **102** is switched off or if the battery is discharged.

[0047] In some embodiments, the NFC device may be capable of operating in an NFC disabled mode in which the transmission of NFC communications via the NFC antenna circuit is generally disabled. For example, a user of the NFC device may decide to disable the transmission of NFC communications to reduce power consumption or prevent RF transmissions from the device. The memory **304** or another non-volatile storage device of the NFC router for example stores one more configuration bits indicating whether or not the NFC device is operating in the NFC disabled mode. Alternatively, one or more bits indicating whether or not the NFC device is operating in the NFC disabled mode are stored in a volatile memory, such as a RAM (random access memory), of the NFC router or of the NFC device. For example, in some embodiments, the one or more bits are stored in the RAM while the NFC device is switched ON, and one or more configuration bits are set to store the NFC enabled/disabled state when the NFC device is switched OFF. The NFC router **202** for example comprises an over-ride mechanism for overriding the general restriction of NFC communications during the NFC disabled mode.

[0048] For example, the memory **304** or another non-volatile storage device of the NFC router stores one or more further configuration bits indicating that the NFC disabled mode can be over-ridden if, for example, the charge state of the battery of the NFC device is below a threshold, such as being entirely discharged or otherwise non-functional, or if, for example, the battery is removed or otherwise disconnected from the NFC device.

[0049] Thus, if the external NFC device makes a request to access to the shared data while the NFC device is in the NFC disabled mode, the NFC router is for example adapted to verify that the further configuration bits permit an over-ride of the NFC disabled mode. If so, the NFC router is for example adapted to verify a charge state of a battery of the NFC device, and to reactive NFC communications and permit access to the shared data only if the charge state of the battery is below a threshold level. In some embodiments the charge state of the battery is determined by detecting whether a supply current of the NFC router is being drawn from the battery of the NFC device or from the NFC field, and for example only in the latter case can the NFC disabled mode be over-ridden.

[0050] FIG. **4** is a flow diagram illustrating operations in a method of accessing the shared data according to an example embodiment.

[0051] Initially, it is assumed that the NFC device **102** is powered, such that the host processing device **206** is operational.

[0052] In an operation **401**, the host processing device **206** stores shared data **306** to the memory **304** of the NFC router **202**.

[0053] For example, in some embodiments, the shared data comprises a code providing access to an event, such as an airplane ticket, a train ticket, theatre ticket, hotel booking, or the like.

[0054] Alternatively, the shared data may comprises data to be kept safe, for example in the case that the NFC device **102** is on the verge of being damaged. For example, the data provided by one or more of the sensors **326** may indicate that the NFC device is at risk of damage, and the shared data for example comprises one or more readings from the sensors **326**, and/or other data such as passwords, encryption keys, etc. Data stored by the NFC router **202** generally has more chance of being successfully recovered later than data stored elsewhere in the NFC device **102** because the NFC router **202** is generally a chip having relatively high levels of protection from impacts and/or exposure to liquids when compared to other elements of the NFC device **102**.

[0055] In a subsequent operation **402**, the NFC device **102** is powered down. For example, the NFC device **102** is turned off by a user, or turns off automatically due to a discharged battery. Alternatively, the NFC device **102** may lose power due to a mechanical stress applied to it, causing for example damage to the battery and/or its wiring, or because of a short circuit caused by immersion of the NFC device **102** in a liquid.

[0056] In a subsequent operation **403**, a wireless polling message is received from an external device, such as the RF reader **301** of FIG. **3**. The polling message for example includes a request for access to the memory **304** of the NFC router **202**. It will be apparent to those skilled in the art that there are a range of protocols that could be used for the communications for accessing the memory **304**. For example, in some embodiments the protocol defined by the international standard ISO7816, based on read binary and update binary commands, could be employed.

[0057] In a subsequent operation **404**, the processing device **302** for example determines whether or not the shared data stored in the memory **304** is protected by access conditions.

[0058] The shared data **306** may be sensitive data with restricted access. For example, in some embodiments the sensitive data comprises one or more readings made by the sensors **326**, and/or other data such as passwords, encryption keys, etc. In some embodiments, the shared data may be freely accessible by the processor **206** of the NFC device, but access is restricted when any external device attempts to access the data. In other embodiments, the access conditions to be applied may be additionally or alternatively dependent on the ON/OFF state of the mobile device and/or on the charge state of the battery of the mobile device.

[0059] If it is determined in operation **404** that the shared data is protected, the next operation is **405**, in which one or more access conditions are verified.

[0060] For example, the protection mechanism may include a symmetric or asymmetric signature or the like. In the case that a symmetric signature is employed, verifying the access condition for example involves verifying a digital signature associated with the access request. For example, the digital signature is a DES-MAC (Data Encryption Standard Message Authentication Code) associated with the access request. The verification for example involves calculating, by

Date Reçue/Date Received 2022-04-27

the NFC router **202**, the signature based on the data provided in the access request or in another message received from the external device. The signature generated by the NFC router **202** is then compared with a signature provided by the external device, and if the signatures match, the access condition is considered to be met. For example, the signature forms the last 8 bytes of the access request. In one embodiment, the signature is a MAC according to the standard ISO/IEC 9797-1 Algorithm 3. The generation of such a MAC is for example discussed in more detail in the chapter A1.2.1 of Book 2, Security and Key Management, of the EMV specification version 4.3, the contents of which is hereby incorporated by reference to the extent permitted by the law. The fact that the access request contains a signature is for example mentioned in the CLA byte of the command according to the EMV specification.

[0061] In alternative embodiments, the NFC router **202** may respond to the polling request from the RF reader **301** by verifying an encryption/decryption key held by the RF reader **301** with respect to one that it holds. This may involve transmitting, by the NFC router **202**, a data value to the RF reader **301** for encryption or decryption using the key held by the reader **301**. The NFC router **202** may also encrypt or decrypt the data value based on the key it holds, and may verify that the response from the RF reader **301** matches its own calculated value.

[0062] Of course, there are many other protection mechanisms based on signatures, keys, passwords or passcodes that could be employed. Furthermore, in some embodiments, an access condition may be based on the charge state of the battery, as described above.

[0063] If one or more of the access conditions is not satisfied, the next operation is for example **406**, in which access to the shared data is refused. For example, a message is transmitted to the RF reader **301** with a failure message.

[0064] Alternatively, if all access conditions of operation **405** have been satisfied, the next operation is for example **407**, in which the shared data is transmitted to the external device.

[0065] Operation **407** is also for example performed if in operation **404** it is determined that the shared data is not protected. For example, the shared data may comprise data that is to be wirelessly accessible by an external device at any time, whether or not the NFC device **102** is powered. For example, data representing an event ticket such as a boarding pass, train ticket, etc., may be freely accessible by any RF reader, but may be encoded such that only certain authorized readers are able to decode and interpret the data.

[0066] FIG. **5** is a flow diagram illustrating a method of generating and storing the shared data **306** to the memory **304** of the NFC router **202** of FIG. **3** according to an example embodiment.

[0067] In a first operation **501**, one or more readings are taken using the one or more sensors **326** of the NFC device of FIG. **3**.

[0068] In a subsequent operation **502**, it is determined whether any of the readings from the sensors **326** exceed a given threshold. The thresholds are for example chosen as corresponding to levels of the environmental parameters captured by the sensors that are unlikely to occur during normal operating conditions of the NFC device **102**, and that indicate that damage to the NFC device **102** is likely to occur.

[0069] If in operation **502** none of the thresholds are exceeded, the method for example returns to operation **501**, in which, after a certain time delay such as a few seconds or a few minutes, one or more new sensor readings are taken.

[0070] Alternatively, if in operation **502** one or more thresholds is exceeded, the next operation is **503**, in which the shared data is stored to the memory **304** of the NFC router **202**. For example, the shared data may include one or more readings leading up to the threshold being exceeded in operation **502**. Additionally or alternatively, the shared data may consist of data that is to be conserved, such as encryption keys, passwords or the like.

[0071] An advantage of the embodiments described herein is that data in an NFC device may be accessible even when the NFC device is no longer powered. Furthermore, the data may be accessible by both a processing device of the NFC device and by an external device, and different access conditions can be applied depending on the device that wishes to access the data.

[0072] Having thus described at least one illustrative embodiment, various alterations, modifications and improvements will readily occur to those skilled in the art.

[0073] For example, while a particular example of an NFC antenna circuit has been described in FIG. **3**, it will be apparent to those skilled in the art that various alternative circuits would be possible.

[0074] The various embodiments described above can be combined to provide further embodiments. Aspects of the embodiments can be modified, if necessary to employ concepts of the various patents, applications and publications to provide yet further embodiments. These and other changes can be made to the embodiments in light of the above-detailed description. In general, in the following claims, the terms used should not be construed to limit the claims to the specific embodiments disclosed in the specification and the claims, but should be construed to include all possible embodiments along with the full scope of equivalents to which such claims are entitled. Accordingly, the claims are not limited by the disclosure.

1. A near field communications (NFC) device, comprising:
an NFC router having a memory adapted to store data to be shared with an external device;
an NFC antenna circuit, wherein the NFC router is capable of operating in a card emulation mode in which the shared data stored by the memory is accessible via the NFC antenna circuit; and
a processor coupled to the NFC router and capable of accessing the shared data in the memory, wherein the NFC router is adapted to detect whether a device requesting access to the shared data is the processor or the external device, and to selectively verify, based on whether the requesting device is detected as being the processor or the external device, one or more first access conditions prior to permitting access to the shared data.

2. The NFC device of claim **1**, wherein the NFC router is adapted to verify, in response to a request from an external device to access the shared data, the one or more first access conditions before transmitting the shared data to the external device via the NFC antenna circuit.

3. The NFC device of claim **2**, wherein the NFC router is adapted to verify a first of the one or more first access conditions by verifying a digital signature associated with the request.

4. The NFC device of claim **1**, wherein the processor is adapted to provide the shared data to be stored in said memory.

Date Reçue/Date Received 2022-04-27

5. The NFC device of claim 1, wherein the NFC router is adapted to apply the one or more first access conditions upon detecting that the device requesting access to the shared data is the external device.

6. The NFC device of claim 1, wherein the NFC device is capable of operating in an NFC-disabled mode in which transmission of NFC communications via the NFC antenna circuit are disabled, wherein if the external device requests access to the shared data while the NFC router is in the NFC-disabled mode, the NFC router is adapted to verify a first of the one or more first access conditions by verifying a charge state of a battery of the NFC device.

7. The NFC device of claim 6, wherein the NFC router is further adapted to re-enable transmission of NFC communications and permit access to the shared data by the external device only if the charge state of the battery is below a threshold level.

8. The NFC device of claim 1, wherein the NFC router is adapted to:

apply the one more first access conditions upon detecting that the device requesting access to the shared data is the external device; and

apply one or more second access conditions, at least one of which is different from the one or more first access conditions, upon detecting that the device requesting access to the shared data is the processor.

9. The NFC device of claim 1, wherein the one or more first access conditions to be applied are selected based further on one or more of:

an ON/OFF state of the NFC device;

a charge state of a battery of the NFC device; and

whether the requested access to the shared data is a read or write request.

10. The NFC device of claim 1, wherein the shared data stored by the memory includes first data and second data, and wherein the NFC router is adapted to permit access to the first data by the external device without any access condition and to prevent access to the second data by the external device until the one or more first access conditions are satisfied.

11. The NFC device of claim 1, further comprising:

one or more sensors to detect one or more environmental parameters, wherein the NFC router is adapted to store the shared data in said memory if a reading from at least one of the one or more sensors exceeds a threshold.

12. The NFC device of claim 11, wherein said one or more sensors comprise at least one of:

a humidity sensor;

an accelerometer;

a positioning device; and

a temperature sensor.

13. A method, comprising:

storing, in a memory of a near field communications (NFC) router of an NFC device, data to be shared with an external device;

during a card emulation mode, providing by the NFC router to the external device access to the shared data via an NFC antenna circuit;

detecting, by the NFC router, whether a device requesting to access the shared data is a processor of the NFC device or the external device; and

selectively verifying, based on whether the requesting device is detected as being the processor or the external device, one or more first access conditions prior to permitting access to the shared data.

14. The method of claim 13, further comprising:

transmitting the shared data to the external device if the one or more first access conditions are satisfied.

15. The method of claim 13, wherein verifying a first of the one or more first access conditions includes verifying, by the NFC router, a digital signature associated with the request.

16. The method of claim 13, comprising:

verifying, by the NFC router, the one or more first access conditions upon detecting that the device requesting access to the shared data is the external device.

17. The method of claim 13, wherein the NFC device is capable of operating in an NFC-disabled mode in which transmission of NFC communications via the NFC antenna circuit are disabled, further comprising:

if the external device requests access to the shared data while the NFC router is in the NFC-disabled mode, applying a first of the one or more first access conditions, wherein the applying includes verifying, by the NFC router, a charge state of a battery of the NFC device.

18. The method of claim 17, further comprising:

re-enabling transmission of NFC communications; and

permitting access to the shared data by the external device only if the charge state of the battery is below a threshold level.

19. The method of claim 13, further comprising:

detecting, via one or more sensors, one or more environmental parameters, wherein the storing of the data in the memory is triggered by a reading from at least one of the sensors exceeding a threshold.

20. The method of claim 19, wherein said one or more environmental parameters comprise at least one of:

a humidity level;

an acceleration reading;

a geographic position of the NFC device; and

a temperature level.

21. A mobile device, comprising:

a processor arranged to direct operations of the mobile device;

a near field communications (NFC) router, the NFC router coupled to the processor and configured to operate in a card emulation mode;

an NFC antenna circuit coupled to the NFC router; and

a memory integrated with the NFC router, the memory arranged to store shared data, wherein the shared data stored in the memory is accessible by the mobile device and wherein the shared data stored in the memory is accessible to the external device via the NFC antenna circuit when the NFC router is operating in the card emulation mode.

22. The mobile device of claim 21, further comprising:

a sensor input coupled to the processor and coupled to at least one of a humidity sensor, an accelerometer, a positioning device, and a temperature sensor, wherein the processor is configured to direct the NFC router to store the shared data in the memory when a reading passed via the sensor input exceeds a threshold.

23. The mobile device of claim 21, wherein the NFC router comprises:

an NFC processing device, the NFC processing device arranged to prevent access to the shared data via the NFC antenna circuit until at least one access condition is verified, the at least one access condition including verification of an ON/OFF state of the mobile device, verification of a charge state of a battery coupled to the

Date Reçue/Date Received 2022-04-27

mobile device, verification of a request to read from the memory, and verification of a request to write to the memory.

24. The mobile device of claim **21**, wherein the at least one access condition includes a first access condition associated with a request to access the shared data from the processor and a second access condition associated with a request to access the shared data from the external device.

25. The mobile device of claim **21**, further comprising:

a secure element, the secure element arranged to store a digital signature, wherein access to the shared data is granted to the external device via the NFC antenna circuit after the NFC router verifies that data in an access request from the external device corresponds to the digital signature.

* * * * *

Date Reçue/Date Received 2022-04-27

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 March 2015 (19.03.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/036957 A1

(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). **PUENTE-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

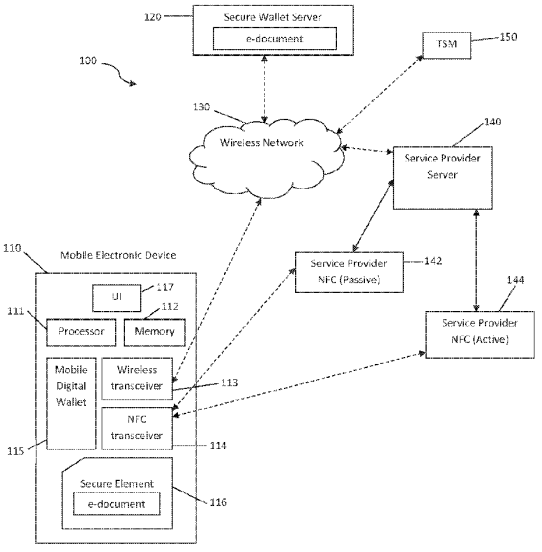


Fig. 1

(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 5 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.

WO 2015/036957 A1

Date Reçue/Date Received 2022-04-27

SYSTEMS AND METHODS FOR PROVIDING SECURE DIGITAL IDENTIFICATION

FIELD OF THE INVENTION

The present invention relates to a secure digital identification system and 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

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 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.

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

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

Date Reçue/Date Received 2022-04-27

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

Date Reçue/Date Received 2022-04-27

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

Date Reçue/Date Received 2022-04-27

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,

Date Reçue/Date Received 2022-04-27

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.

Date Reçue/Date Received 2022-04-27

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.

Date Reçue/Date Received 2022-04-27

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.

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.

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.

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.

Date Reçue/Date Received 2022-04-27

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

Date Reçue/Date Received 2022-04-27

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

Date Reçue/Date Received 2022-04-27

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.

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, 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 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 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 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 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.

Date Reçue/Date Received 2022-04-27

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

Date Reçue/Date Received 2022-04-27

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.

Date Reçue/Date Received 2022-04-27

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

Date Reçue/Date Received 2022-04-27

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

Date Reçue/Date Received 2022-04-27

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 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 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 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 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 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 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

Date Reçue/Date Received 2022-04-27

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,

Date Reçue/Date Received 2022-04-27

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,

Date Reçue/Date Received 2022-04-27

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.

Date Reçue/Date Received 2022-04-27

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.

Date Reçue/Date Received 2022-04-27

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

Date Reçue/Date Received 2022-04-27

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.

Date Reçue/Date Received 2022-04-27

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;

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;

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;

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.

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

Date Reçue/Date Received 2022-04-27

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

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.

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. 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.

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.

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.

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.

Date Reçue/Date Received 2022-04-27

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.

Date Reçue/Date Received 2022-04-27

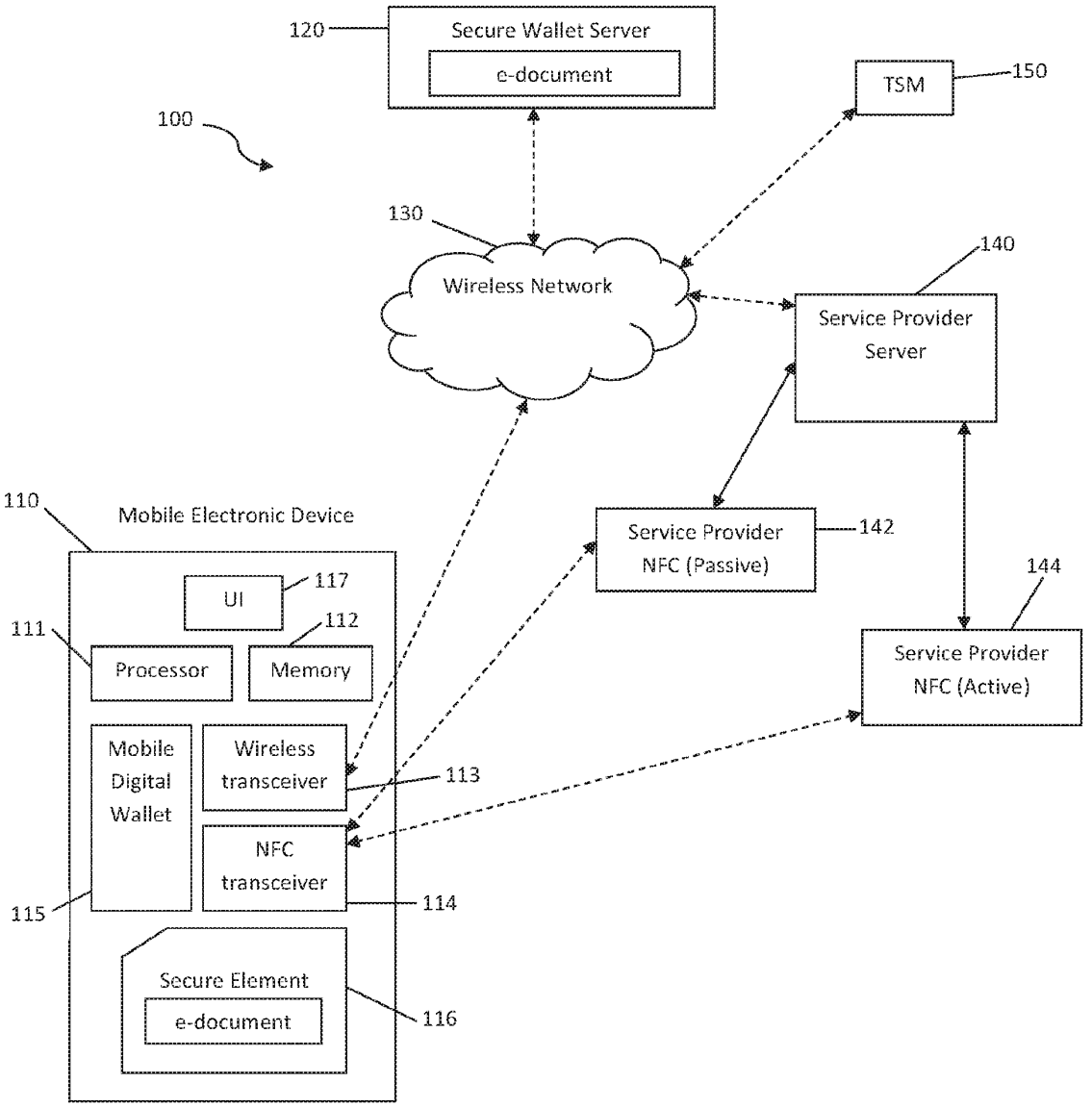
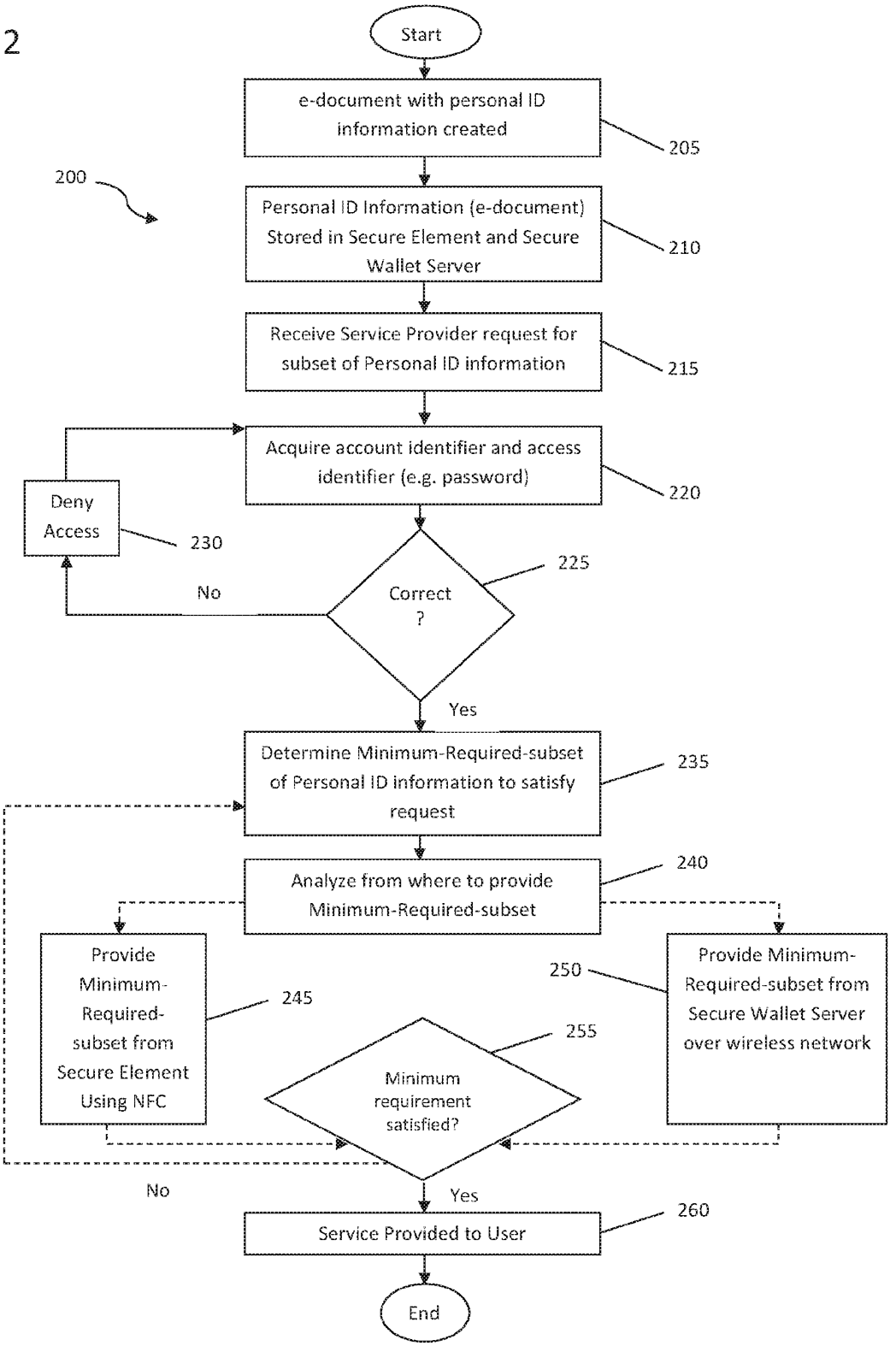


Fig. 1

Date Reçue/Date Received 2022-04-27

Fig. 2



Date Reçue/Date Received 2022-04-27

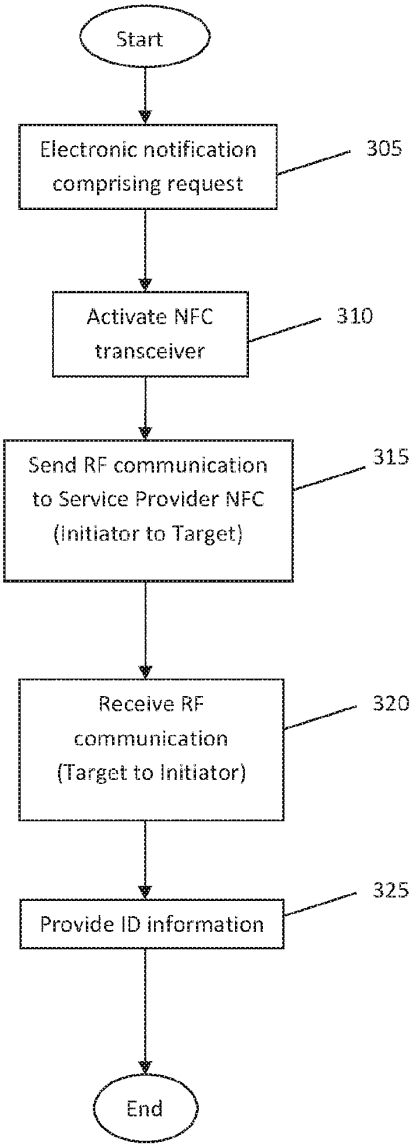


Fig. 3A

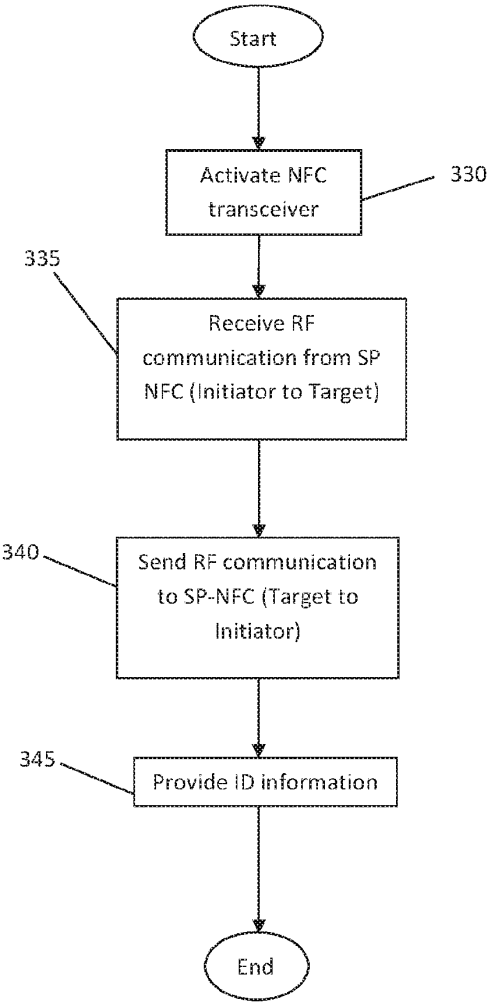


Fig. 3B

Date Reçue/Date Received 2022-04-27

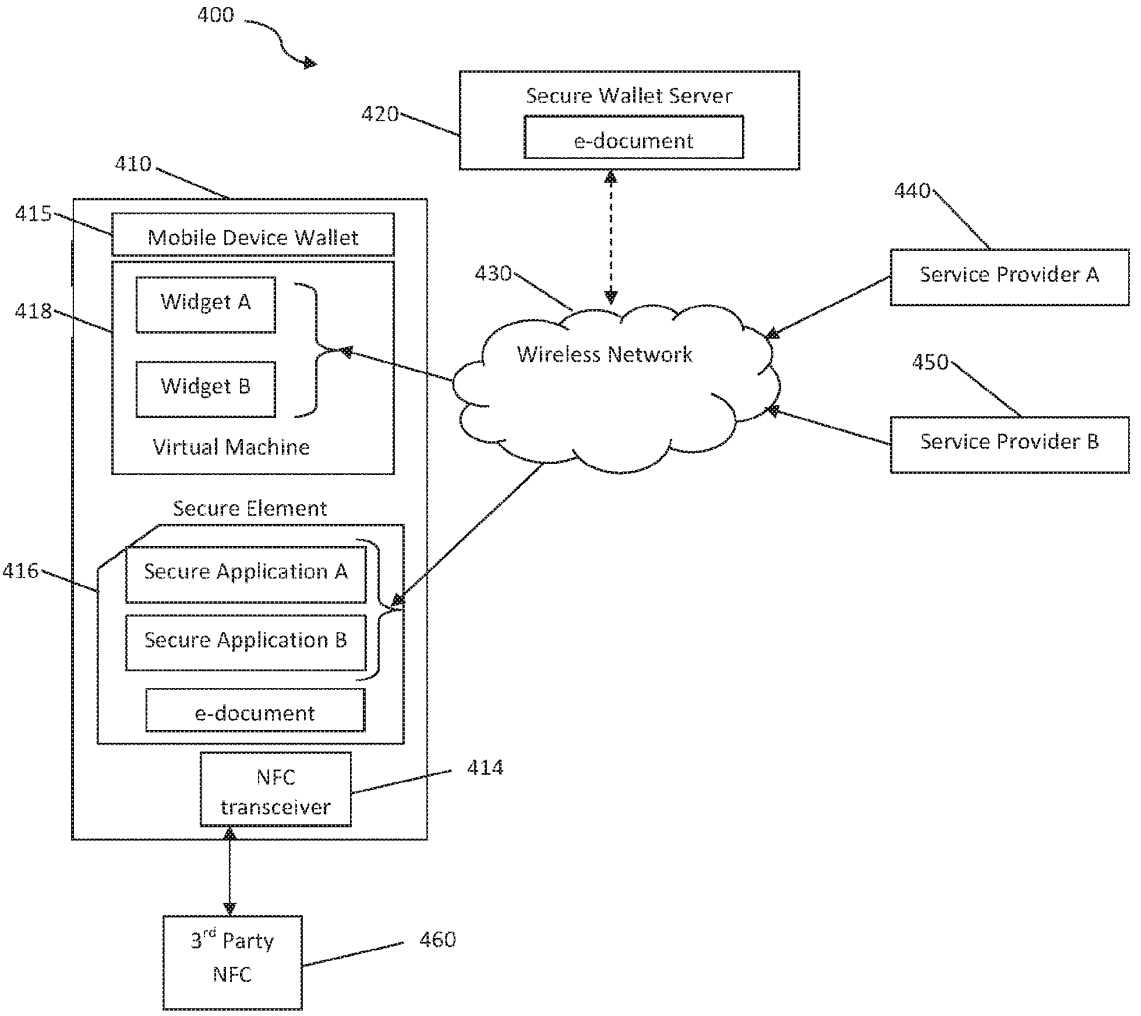


Fig. 4

Date Reçue/Date Received 2022-04-27

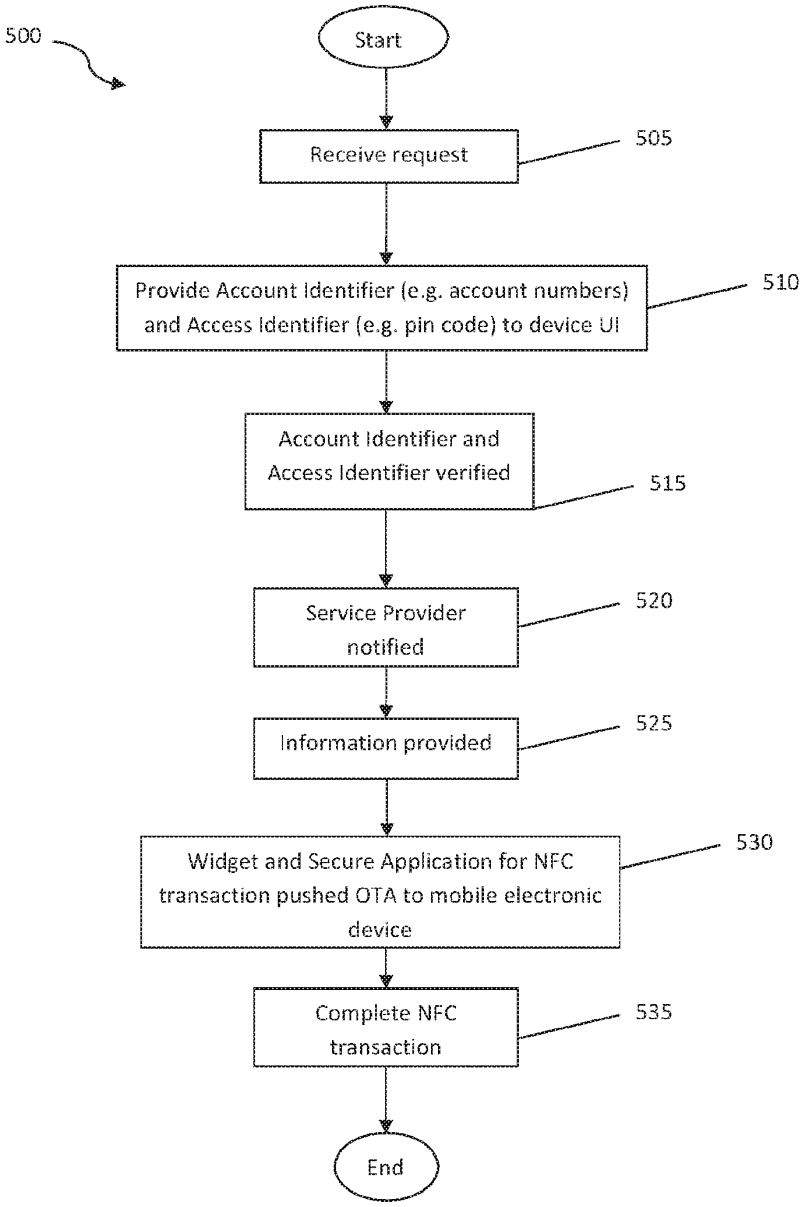


Fig. 5

Date Reçue/Date Received 2022-04-27

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

"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	Date of mailing of the international search report
21 January 2015	**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**

Form PCT/ISA/210 (second sheet) (July 2009)

Date Reçue/Date Received 2022-04-27

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	Non e	
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

Form PCT/ISA/210 (patent family annex) (July 2009)

Date Reçue/Date Received 2022-04-27

THALES LANCE SON NOUVEAU PORTEFEUILLE D'IDENTITÉ NUMÉRIQUE – VOS DOCUMENTS D'IDENTITÉ ACCESSIBLES OÙ QUE VOUS SOYEZ

| 29/07/2019 |

IDENTITÉ DIGITALE ET SÉCURITÉ

PORTEFEUILLE D'IDENTITÉ NUMÉRIQUE

PLATEFORME DIGITALE SÉCURISÉE SOLUTIONS MOBILES

SHARE

- Il est désormais facile aux citoyens de prouver leur identité, faire valoir leurs droits en accédant à tout moment à leurs documents officiels sur leur smartphone, grâce à la plate-forme hautement sécurisée Gemalto « Digital ID Wallet ».
- Les gouvernements pourront renforcer leurs liens avec les citoyens grâce aux divers services d'identification hébergés par « Gemalto Digital ID Wallet », tout

Date Reçue/Date Received 2022-04-27

THALES

• Grâce à des solutions de chiffrement sophistiquées, les données personnelles des citoyens sont totalement sécurisées, garantissant la confidentialité et le respect de la vie privée.

Avec le nouveau Gemalto « Digital ID Wallet » de Thales, les gouvernements peuvent délivrer à tous les citoyens une version mobile sécurisée de leurs documents officiels tels que leurs cartes d'identité, cartes de santé ou permis de conduire. Un simple clic suffira désormais pour accéder à ces documents dématérialisés, et ainsi faire valoir ses droits ou bénéficier de services plus facilement et rapidement. La solution repose sur plusieurs niveaux de sécurité et un chiffrement sophistiqué qui assurent une protection optimale des données personnelles, tout en offrant à l'utilisateur un contrôle total sur le choix des informations qu'il partage, les destinataires et le moment où il les envoie.

Les gouvernements étant de plus en plus nombreux à opter pour la dématérialisation des documents officiels, ce nouveau portefeuille numérique permet aux citoyens de conserver toutes leurs données vitales d'identification en un seul endroit, sécurisé et pratique. Conçu pour couvrir les cas d'usage propres aux documents physiques classiques, comme par exemple présenter sa carte d'électeur digitalisée dans un bureau de vote, le « Digital ID Wallet » facilite également l'authentification en ligne. L'utilisateur peut accéder à tout moment et de façon sécurisée à ses papiers officiels mais aussi à un grand nombre de services publics en ligne, et ainsi remplir sa déclaration d'impôt ou faire une demande d'aide sociale en ligne.

Respectueux de la vie privée, le « Digital ID Wallet » permet à l'utilisateur de décider quelles informations il partage avec des tiers. Ainsi, pour pénétrer dans un endroit dont l'accès est soumis à des conditions d'âge, par exemple un casino, il peut simplement prouver grâce à son portefeuille numérique qu'il a l'âge requis, sans avoir à donner son âge exact ou toutes autres données personnelles qui ne sont pas indispensables au bon déroulement de la vérification d'âge.

Le « Digital ID Wallet » offre aux gouvernements la possibilité de rationnaliser considérablement la gestion et la vérification de tous leurs documents officiels : le travail administratif s'en trouve optimisé et les administrations disposent d'une arme efficace contre l'usurpation d'identité et la fraude. En créant un mode de communication dynamique entre l'agence gouvernementale émettrice du document et l'utilisateur, le « Digital ID Wallet » permet également de

THALES

vaccination ou les prévenir que leur nouveau passeport électronique est arrivé.

Thales a par ailleurs conçu une application mobile extrêmement performante, Mobile Security Core, qui protège le Digital ID Wallet contre les menaces et les logiciels malveillants, et répond aux plus hautes exigences des gouvernements en matière de sécurité.

« Partout dans le monde, les gouvernements et les citoyens prennent conscience des avantages multiples de la dématérialisation des documents officiels, en complément des documents papier. Le « Digital ID Wallet » crée un écosystème évolutif et centré sur le citoyen, où cette révolution peut se déployer et répondre aux besoins de contrôle et d'authentification du monde physique et de l'univers dématérialisé, en utilisant le seul objet que nous avons le plus de chances d'avoir toujours à portée de main : nos smartphones. » Frédéric Trojani, SVP Solution identitaires et biométriques, Thales

THALES

Digital ID Wallet is a secure gateway to next-generation digital identity services, credentials, privacy and Government-to-Citizens (G2C) engagement



Note aux rédacteurs

Les solutions Gemalto sont au cœur de la vie moderne, du paiement à l'internet des objets, en passant par la sécurité des entreprises. Conçus pour authentifier les personnes, les transactions et les objets, chiffrer les données et conférer de la valeur ajoutée aux logiciels, les technologies et les services Gemalto permettent aux entreprises et aux gouvernements de fournir des services numériques sécurisés pour des milliards d'individus et d'objets.

À propos de Thales

Ceux qui font avancer le monde s'appuient sur Thales. Nous sommes aux côtés de ceux qui ont de grandes ambitions : rendre le monde meilleur et plus sûr. Riches de la diversité de leurs expertises, de leurs talents, de leurs cultures, nos équipes d'architectes conçoivent un éventail unique de solutions technologiques d'exception, qui rendent demain possible dès aujourd'hui. Du fond des océans aux profondeurs du cosmos ou du cyberespace, nous aidons nos clients à maîtriser des environnements

THALES

a réalisé en 2018 un chiffre d'affaires de 19 milliards d'euros.

Documents

Thales launches its new Gemalto Digital ID Wallet – an identity revolution in your smartphone
Thales launches its new Gemalto Digital ID Wallet – Infographics
Thales lance son nouveau portefeuille d'identité numérique – vos documents d'identité accessibles o…

Contact

Constance Arnoux- Media Relations, Security
+33 (0) 1 57 77 91 58 constance.arnoux@thalesgroup.com

20/04/2020

La technologie Thales au cœur de la sécurité du nouveau smartphone exclusivement eSIM de Motorola

THALES

Omnispace choisit Thales Alenia Space pour développer une infrastructure satellitaire reflétant sa vision d'un réseau hybride mondial

07/04/2020

Thales renforce sa résilience pour atténuer l'impact de la crise du Covid-19

SHARE THIS ARTICLE

All articles

DEFENSE ET SECURITÉ

IDENTITE ET SÉCURITÉ NUMÉRIQUES

AÉRONAUTIQUE

ESPACE

TRANSPORT

SOLUTIONS POUR MARCHÉS SPÉCIFIQUES

Social networks

THALES

Contact us

Siège social
+33 (0) 1 57 77 80 00

Envoyer un message *Carnet d'adresses*

GLOBAL

MARCHÉS

CANDIDAT

INVESTISSEUR

JOURNALISTE

CUSTOMER ONLINE

2019 Thales Group

Date Reçue/Date Received 2022-04-27

US 20160294831A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2016/0294831 A1**

Borunda et al. (43) **Pub. Date: Oct. 6, 2016**

(54) **DIGITAL IDENTIFICATION SYSTEM**

(71) Applicant: **United Services Automobile Association (USAA)**, San Antonio, TX (US)

(72) Inventors: **Adrian Borunda**, San Antonio, TX (US); **Andrew L. Anaruk**, San Antonio, TX (US); **Heather Hernandez**, San Antonio, TX (US); **Melissa Trevino**, San Antonio, TX (US); **Gunjan Vijayvergia**, San Antonio, TX (US); **William H. Wright, III**, San Antonio, TX (US); **John Shelton**, San Antonio, TX (US); **Susan Wright**, San Antonio, TX (US); **Cory S. Pickrel**, Austin, TX (US); **Christopher Bess**, San Antonio, TX (US); **Minya Liang**, Redmond, WA (US)

(21) Appl. No.: **15/088,630**

(22) Filed: **Apr. 1, 2016**

Related U.S. Application Data

(60) Provisional application No. 62/142,792, filed on Apr. 3, 2015, provisional application No. 62/188,356, filed on Jul. 2, 2015, provisional application No. 62/244,029, filed on Oct. 20, 2015.

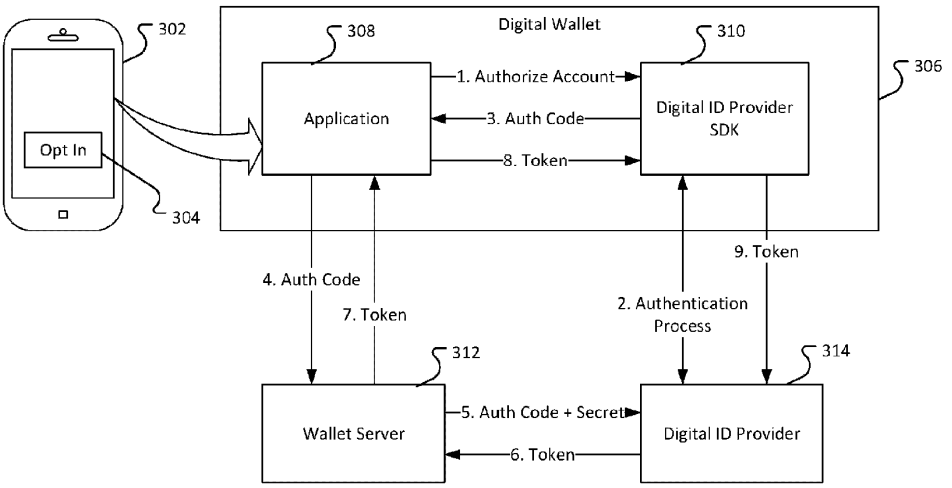
Publication Classification

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/10*** (2013.01); ***H04L 63/08*** (2013.01)

(57) **ABSTRACT**

Methods, systems, and apparatus, including computer programs encoded on computer storage media, to provide digital identification. One of these methods includes comparing the location of a requester of a digital identification to the location of an owner of the digital identification. The method also includes providing information about the digital identification to the requester based at least in part on determining that the requester and the owner are within a predetermined distance.



Date Reçue/Date Received 2022-04-27

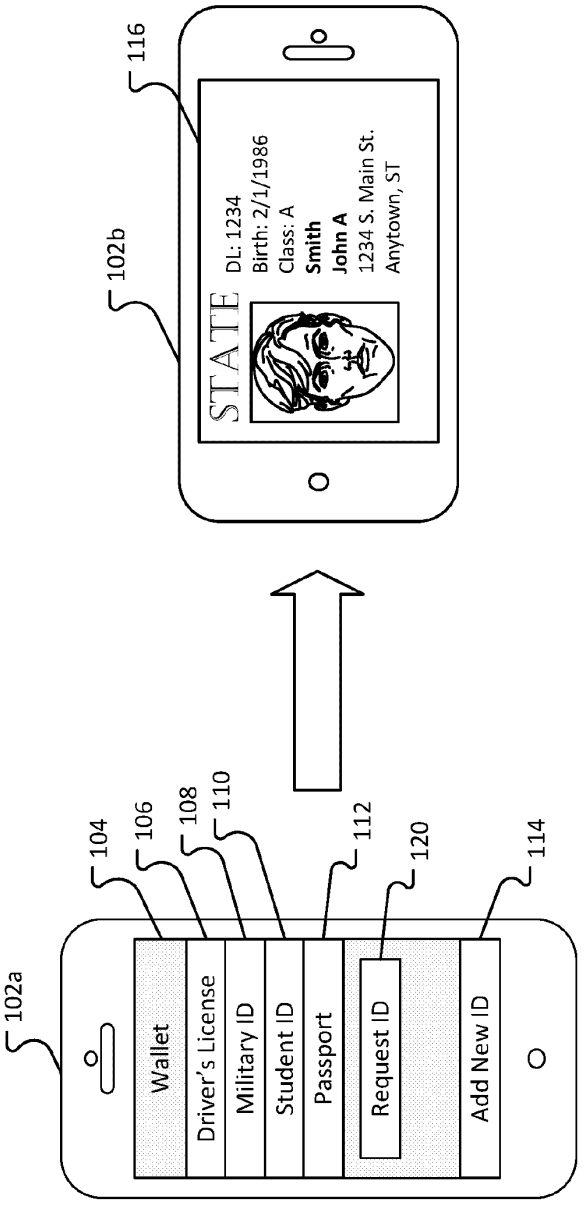


FIG. 1

Date Reçue/Date Received 2022-04-27

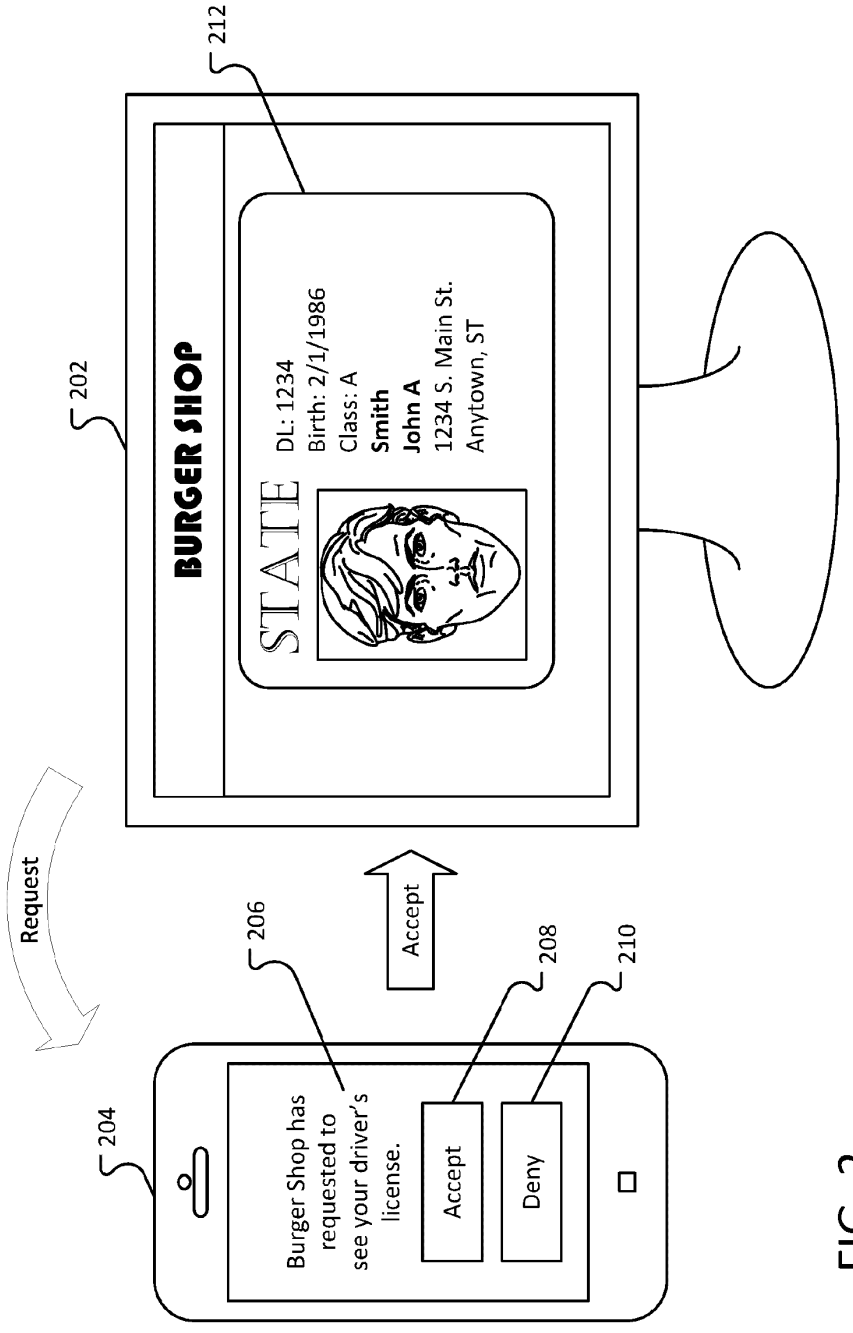


FIG. 2

Date Reçue/Date Received 2022-04-27

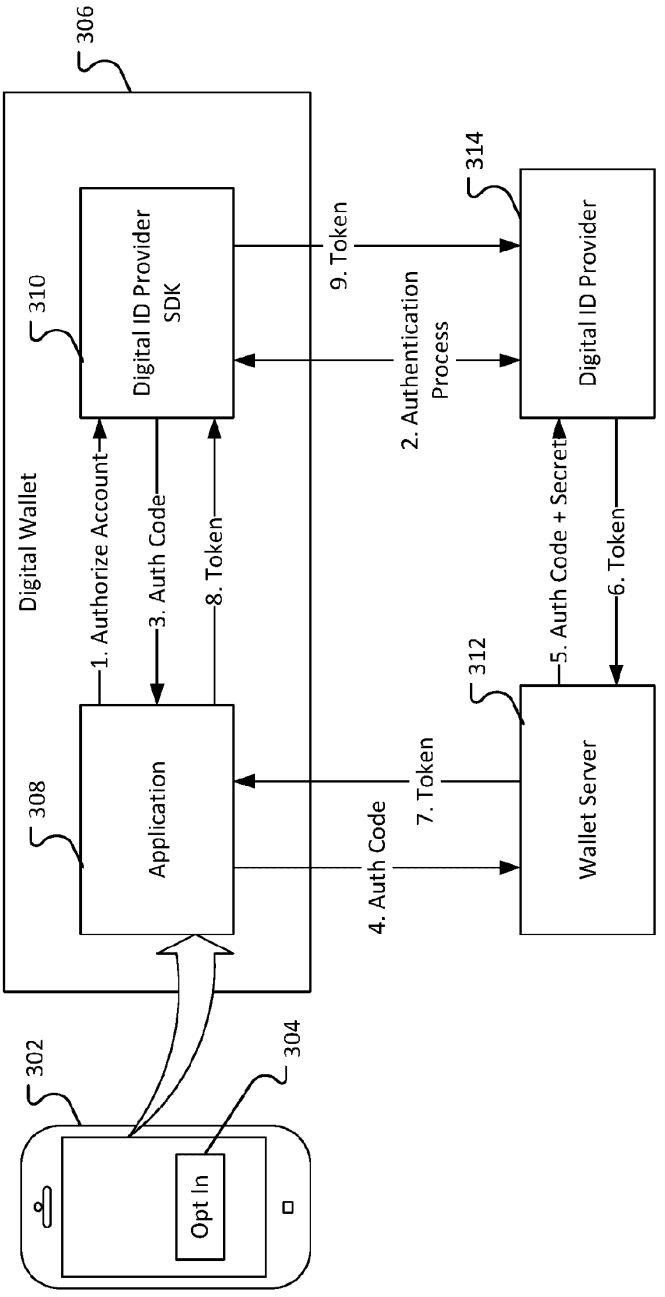


FIG. 3

Date Reçue/Date Received 2022-04-27

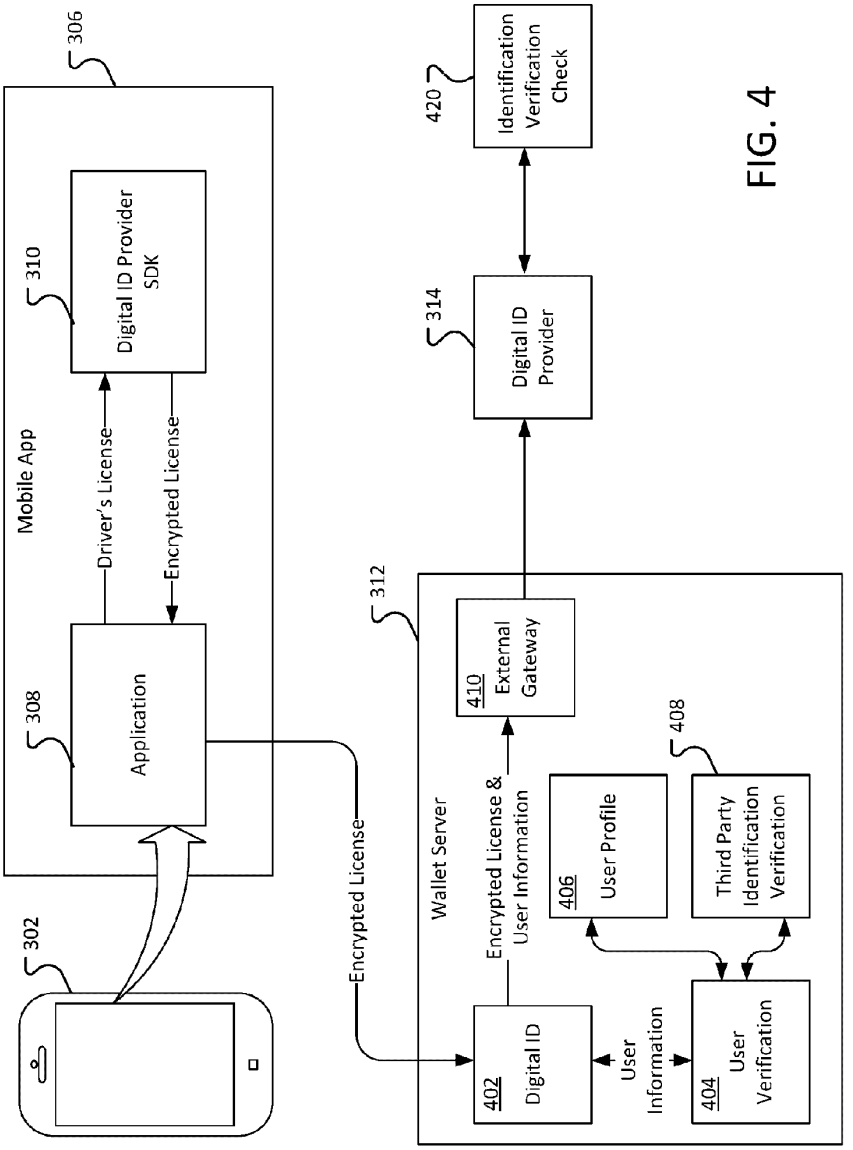

306
Mobile App
310
Digital ID Provider SDK
Driver's License
Encrypted License
308
Application
302
Encrypted License
312
Wallet Server
Encrypted License & User Information
410
External Gateway
420
Identification Verification Check
314
Digital ID Provider
408
406
User Profile
Third Party Identification Verification
402
Digital ID
User Information
404
User Verification

FIG. 4

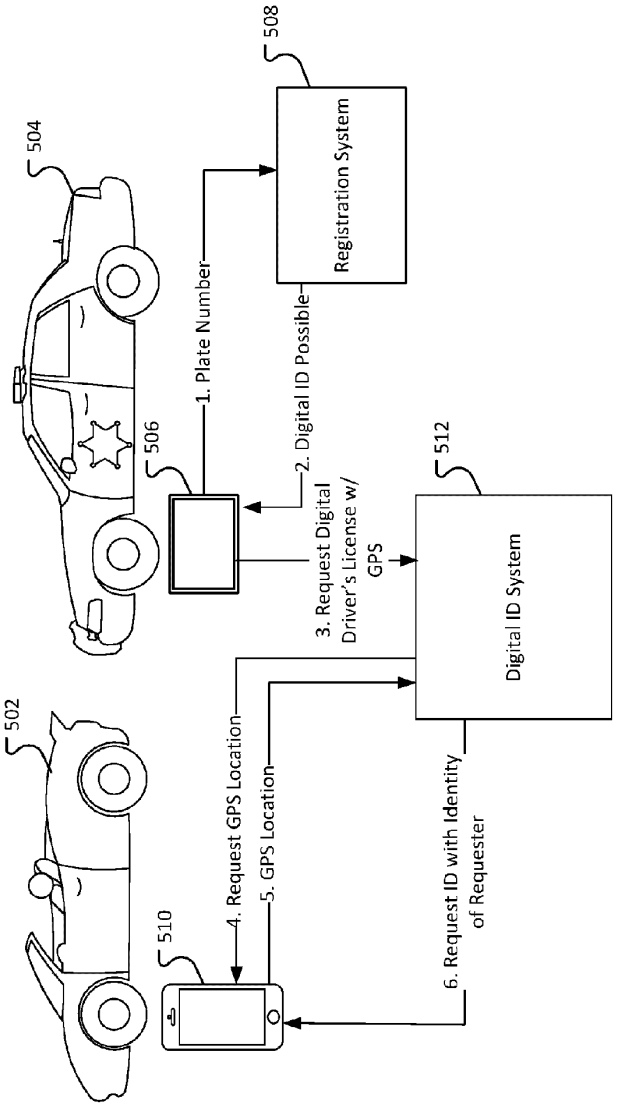
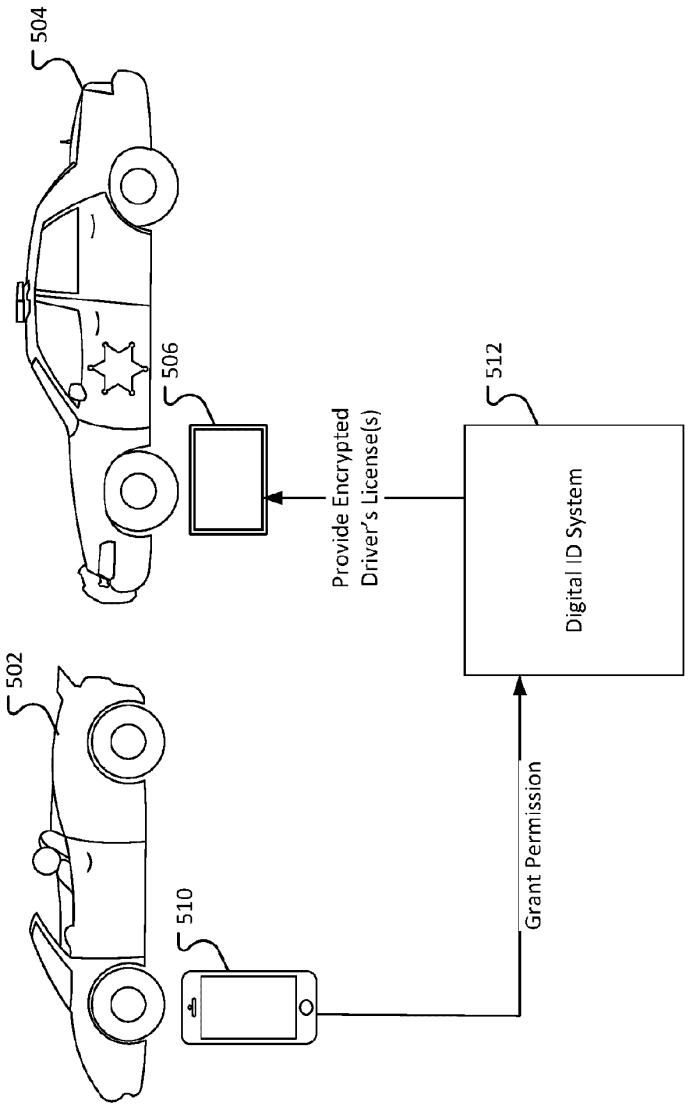

504
508
Registration System
1. Plate Number
2. Digital ID Possible
506
512
3. Request Digital Driver's License w/ GPS
Digital ID System
502
4. Request GPS Location
5. GPS Location
510
6. Request ID with Identity of Requester

FIG. 5A

FIG. 5B


504
506
512
Provide Encrypted
Driver's License(s)
Digital ID System
502
510
Grant Permission

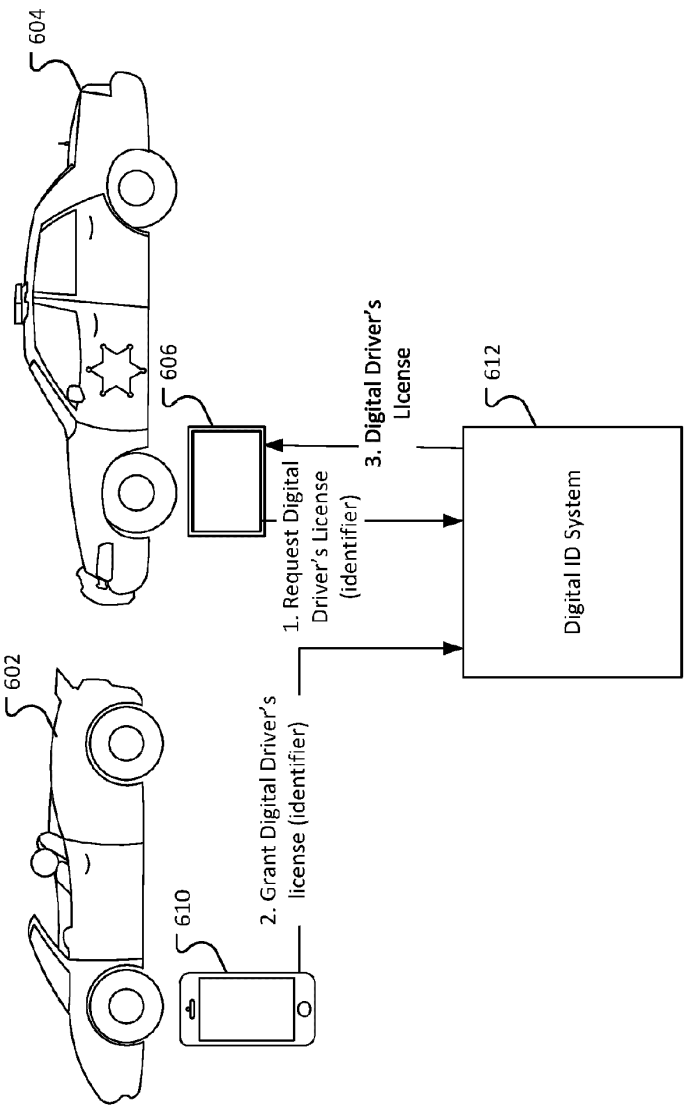

604
606
612
602
610
1. Request Digital Driver's License (identifier)
2. Grant Digital Driver's license (identifier)
3. Digital Driver's License
Digital ID System

FIG. 6

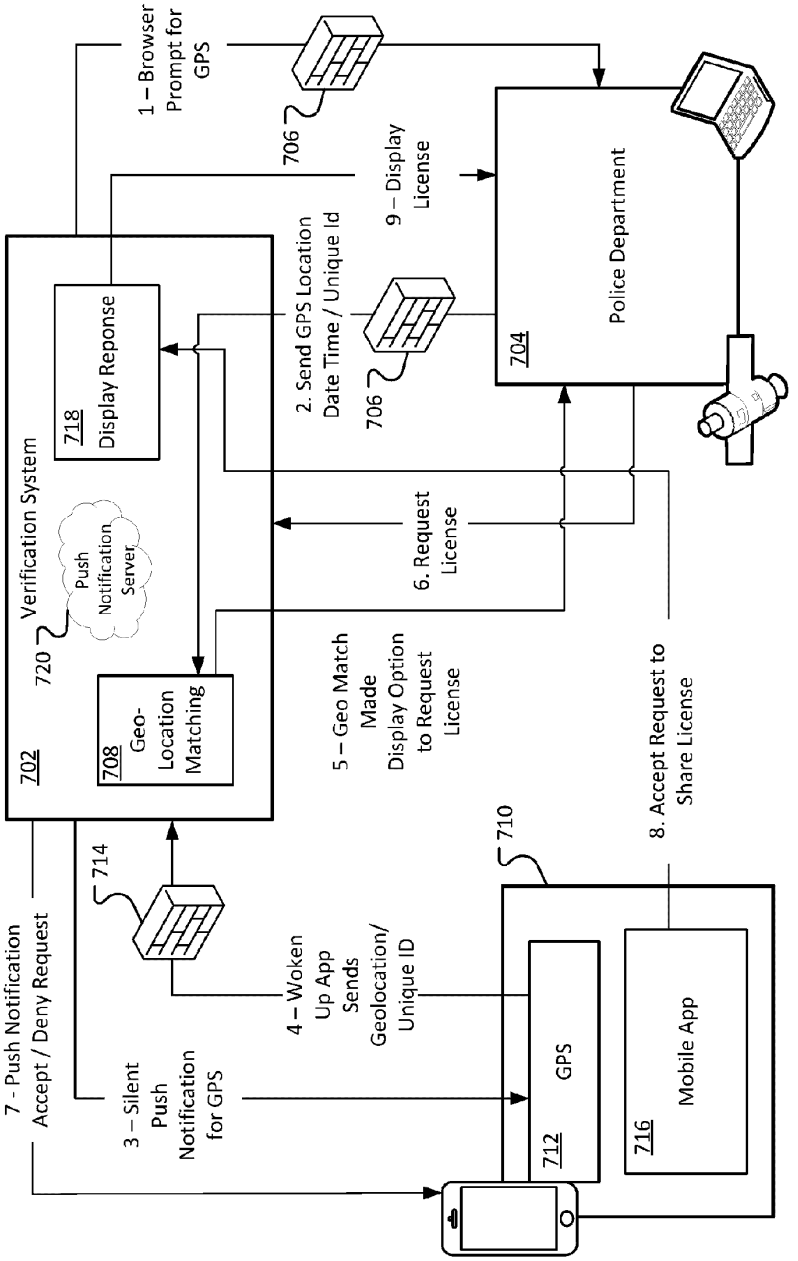

1 – Browser Prompt for GPS
706
9 – Display License
Police Department
704
2. Send GPS Location Date Time / Unique Id
706
718 Display Reponse
Verification System
720
Push Notification Server
6. Request License
702
708 Geo-Location Matching
5 – Geo Match Made Display Option to Request License
8. Accept Request to Share License
710
714
7 - Push Notification Accept / Deny Request
4 – Woken Up App Sends Geolocation/ Unique ID
3 – Silent Push Notification for GPS
712 GPS
716 Mobile App

FIG. 7

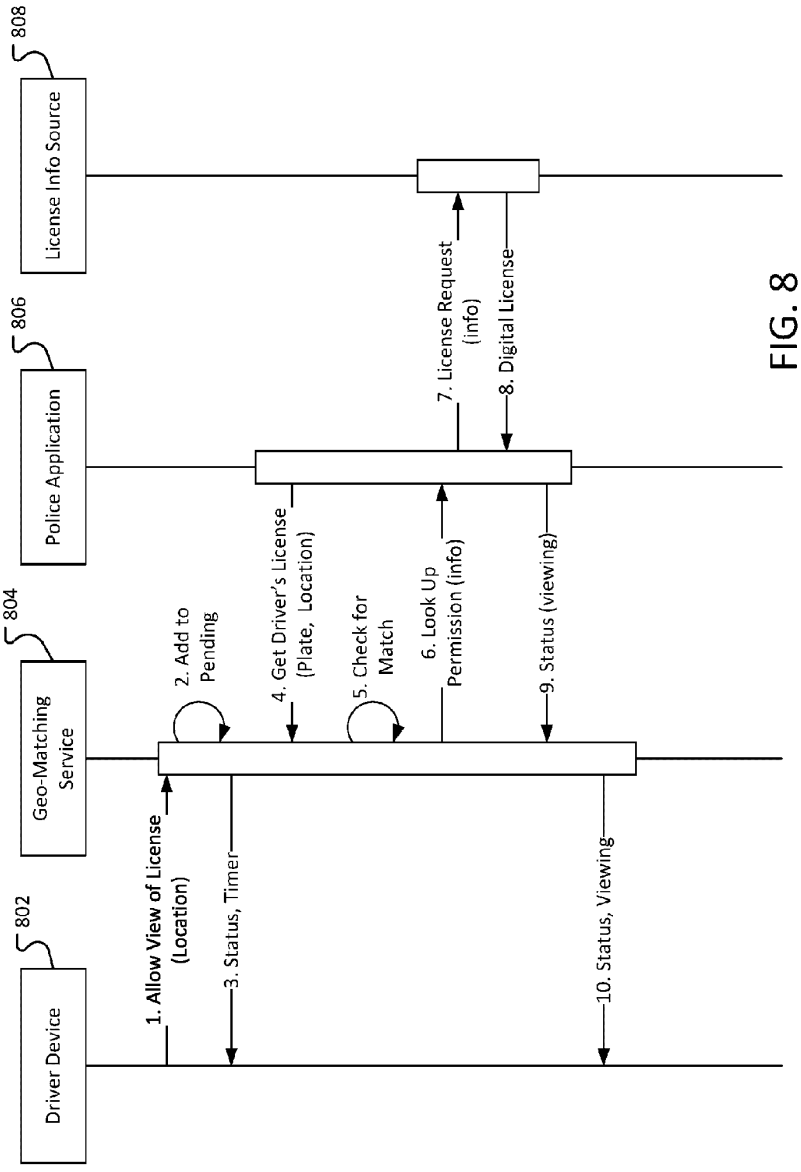

808
License Info Source
806
Police Application
804
Geo-Matching Service
802
Driver Device
1. Allow View of License (Location)
2. Add to Pending
3. Status, Timer
4. Get Driver's License (Plate, Location)
5. Check for Match
6. Look Up Permission (info)
7. License Request (info)
8. Digital License
9. Status (viewing)
10. Status, Viewing

FIG. 8

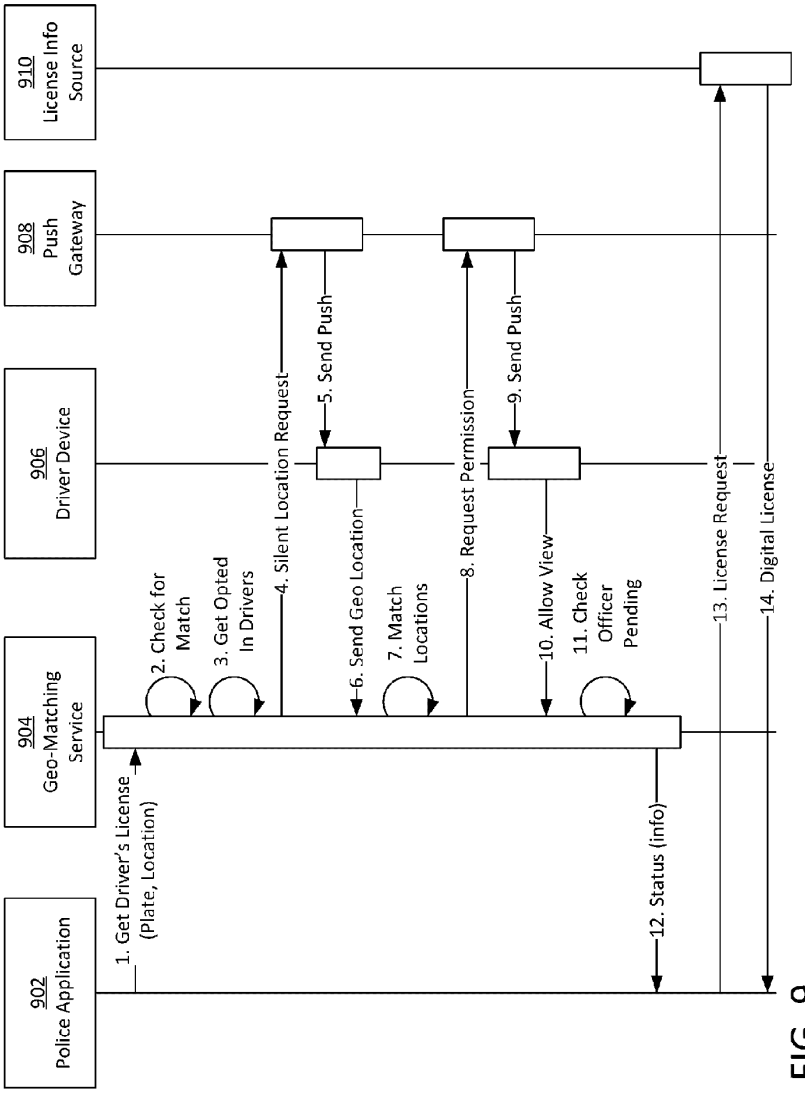

902 Police Application
904 Geo-Matching Service
906 Driver Device
908 Push Gateway
910 License Info Source
1. Get Driver's License (Plate, Location)
2. Check for Match
3. Get Opted In Drivers
4. Silent Location Request
5. Send Push
6. Send Geo Location
7. Match Locations
8. Request Permission
9. Send Push
10. Allow View
11. Check Officer Pending
12. Status (info)
13. License Request
14. Digital License

FIG. 9

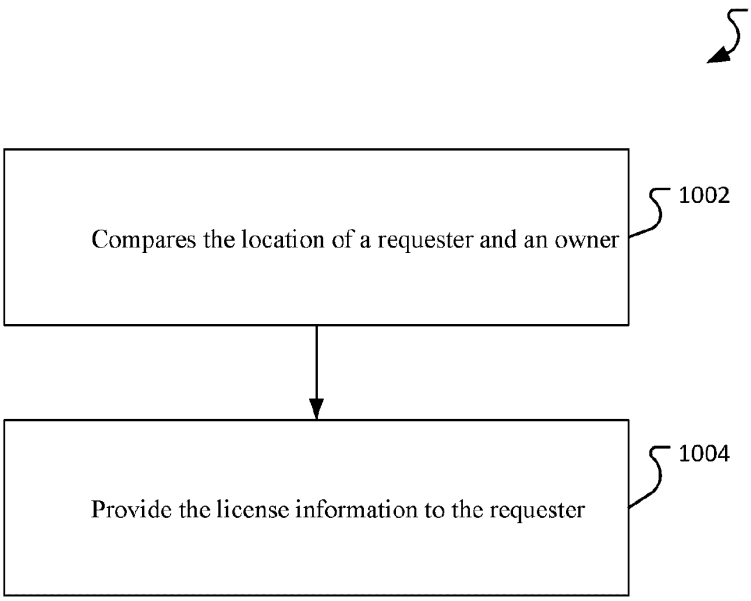


FIG. 10

Date Reçue/Date Received 2022-04-27

DIGITAL IDENTIFICATION SYSTEM

CLAIM OF PRIORITY

[0001] This application claims priority under 35 USC §119(e) to U.S. Patent Application Ser. No. 62/142,792, filed on Apr. 3, 2015, the entire contents of which are hereby incorporated by reference; U.S. Patent Application Ser. No. 62/188,356, filed on Jul. 2, 2015, the entire contents of which are hereby incorporated by reference; and U.S. Patent Application Ser. No. 62/244,029, filed on Oct. 20, 2015, the entire contents of which are hereby incorporated by reference.

BACKGROUND

[0002] Identification documents may be used to verify aspects of a person's personal identity. If issued in the form of a small, mostly standard-sized card, it is usually called an identity card (ID or ID card). Countries which do not have formal identity documents may require identity verification using informal documents.

[0003] In the absence of a formal identity document, driving licenses may be accepted in many countries for identity verification. Some countries do not accept driving licenses for identification, often because in those countries they do not expire as documents and can be old or easily forged. Most countries accept passports as a form of identification.

[0004] Identification documents may also be used to verify an individual's membership in a group. For example, student identification cards are used as proof that the individual is a student, faculty, or staff at a school. Military identification cards are used as proof that the individual is a member of the armed services.

SUMMARY

[0005] This specification describes technologies relating to digital identification.

[0006] In general, one innovative aspect of the subject matter described in this specification can be embodied in methods that include the actions of comparing the location of a requester of a digital identification to the location of an owner of the digital identification. The methods also include the actions of providing information about the digital identification to the requester based at least in part on determining that the requester and the owner are within a predetermined distance.

[0007] Other embodiments of this aspect include corresponding computer systems, apparatus, and computer programs recorded on one or more computer storage devices, each configured to perform the actions of the methods. A system of one or more computers can be configured to perform particular actions by virtue of having software, firmware, hardware, or a combination of them installed on the system that in operation causes or cause the system to perform the actions. One or more computer programs can be configured to perform particular actions by virtue of including instructions that, when executed by data processing apparatus, cause the apparatus to perform the actions.

[0008] The foregoing and other embodiments can each optionally include one or more of the following features, alone or in combination. Providing information about the digital identification may be further based on receiving authorization to share the information from the owner. The methods may include the actions of receiving a pre-authorization to share the digital identification, and storing the pre-authorization. The pre-authorization may expire after a predetermined period of time. The location of the owner of the digital identification may be obtained without notifying the owner. The methods may include the actions of receiving a license plate number associated with a vehicle of the owner, identifying the owner based on the license plate number, and contacting a user device of the owner requesting the digital driver's license. The methods may identify owner based on media or technology within the car.

[0009] The details of one or more embodiments of the subject matter described in this specification are set forth in the accompanying drawings and the description below. Other features, aspects, and advantages of the subject matter will become apparent from the description, the drawings, and the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. **1** is an example of a digital wallet application executing on a client device.

[0011] FIG. **2** illustrates providing a digital identification **212** to a computing device **202**.

[0012] FIG. **3** illustrates an example of integrating a digital wallet with a digital ID provider.

[0013] FIG. **4** illustrates an example of adding an identification document to a digital wallet.

[0014] FIGS. **5**A-**5**B illustrate an example of providing a digital identification document to a third party.

[0015] FIG. **6** illustrates another example of providing a digital identification document to a third party.

[0016] FIG. **7** illustrates an example of presenting a digital driver's license.

[0017] FIG. **8** is a sequence diagram illustrating an example presenting a digital driver's license to a law enforcement office.

[0018] FIG. **9** is a sequence diagram illustrating an example presenting a digital driver's license to a law enforcement office.

[0019] FIG. **10** is a flowchart of an example process for providing a digital driver's license to a requester.

[0020] Like reference numbers and designations in the various drawings indicate like elements.

DETAILED DESCRIPTION

[0021] Identification documents service an important role. They are used to verify that an individual is who they purport to be. Identification documents are also used to verify that an individual is a member of class of individuals entitled to certain privileges. For example, a driver's license demonstrates that a user is entitled to drive. A student identification card demonstrates that an individual is affiliated with a particular school. A military identification card demonstrates that an individual is a member of the armed services.

[0022] Physical cards have short comings. They can be lost, stolen, or forged. An individual may need to carry multiple identification cards, which may be unwieldy. Identification documents can be stored or accessed using a client device. In some implementations, identification document access can be integrated into a digital wallet or similar application. digital identification has the advantage of being able to be provided electronically, rather than physically,

Date Reçue/Date Received 2022-04-27

which in turn reduces the likelihood that the identification will be lost or stolen. digital identification also allows for real-term validation that the ID is still active (for example, that the ID has not been revoked) unlike a physical ID which can only show if the ID is expired.

[0023] FIG. **1** is an example of a digital wallet application executing on a client device. The client device can be, for example, a mobile device (such as a smart phone, a tablet, a notebook, personal digital assistant, a dedicated wallet device, a wearable computing device, or any other portable device capable of sending and receiving messages over a network). The client device can also be devices integrated into the Internet of Things, such as a smart home or devices within the home. The client device **102***a* includes a digital wallet application **104**. Within the digital wallet is information about different available digital identification documents. In this example, the digital wallet has a driver's license **106**, a military id **108**, a student id **110**, and a passport **112**. Other types of identification and permits can also be stored in the digital wallet, including but not limited to firearm permits, hunting licenses, medical licenses, bar admission cards, and a Naturalization and Immigration Services (NIS) Cards. In some implementations, the digital wallet only displays information about digital identification documents to which the application has access.

[0024] Information in the digital wallet may also establish relationships between individuals, such as legal guardianship and spousal relationships.

[0025] In some implementations, the digital wallet application **104** includes a selectable item **114** (for example, a button or a link) that enables the user to add a new form of identification to the system. In some implementations, the driver's license may be requested, for example, by selecting the appropriate identification and selecting the Request ID button **120**. In some implementations, the driver's license may be requested, for example, by voice activation and/or double tapping the driver's license item **106**.

[0026] The user can select a form of digital identification to present on the client device **102***a*. In this example, the user selects the driver's license **106**. The user interface of the client device **102***b* can update the display the user's driver's license **116**.

[0027] FIG. **2** illustrates providing a digital identification **212** to a computing device **202**. A computing device **208** may request identification from the client device **204**. In some implementations, the computing device **202** can be executing an application that is capable of sending a request to the client device **204**. For example, the application executing on the computing device **202** and the app executing on the client device **204** may be in communication through a separate system such as a server (not shown).

[0028] The client device **204** receives the request for the driver's license and displays a message **206** on the screen. The request may include the identity of the individual, company, or system requesting the identification. In this example, Burger Shop has requested to see a driver's license. In some implementations, the computing device **206** can request a particular form of identification, such as a driver's license or a passport. In some implementations, the computing device **206** may request any form of identification sufficient to demonstrate some fact about the user, such as age or citizenship.

[0029] In some implementations, the client device **204** may proactively offer the driver's license. The driver's license may be offered to particular entity (for example, the Burger Shop, a law enforcement officer, etc.) or may be generally presented to whomever requests it. In some implementations, the driver's license may be offered to a particular type of entity (for example, any bar or restaurant, any law enforcement officer, an immigration agent, etc.).

[0030] The user of the client device **204** may accept **208** or deny **210** the request. If the user accepts the request, the user's driver's license **212** is displayed on the computing device **202** of the requesting party. The computing device **202** may display the user's digital identification, but in some instances it may only display a decision or determination that is relevant to the person requesting the identification. For example, an age verification requested by a retail store may only need to know that digital identification holder is old enough to purchase alcohol. Therefore the computing device may display a YES or NO depending on whether the identification holder is old enough to purchase alcohol or not. Other examples include authorization to enter a venue or event (for example, if the client device **202** contains a ticket to the venue or event), authorization to board a transport (for example, a plane, ship, bus, or train), and authorization to vote (for example, the client device **202** is used to access a voter registration).

[0031] In some implementations, business rules may determine whether or not a request is legitimate. For example, the GPS location of the requester and the GPS location of the client device may be compared, the system may compare items purchased by the user to determine if any purchased item requires proof of age, etc.

[0032] Communication between the client device **204** and the computing device **202** may be performed using point to point communication technologies (for example, near field communication (NFC), Blue Tooth, etc.) or may be performed using communication with an application service, described further below).

[0033] In some implementations, the driver's license may be offered only for a limited amount of time. For example, the recipient of the driver's license may only have a predetermined period of time (for example, 20 seconds, 30 seconds, 1 minute) to view the driver's license. In some implementations, the recipient of the driver's license may only have a limited period of time to accept an offer to view a driver's license (for example, 15 seconds, 30 seconds, 1 minute), but once viewed, may view it for a longer period of time (for example, 5 minutes, 10 minutes, an hour, indefinitely).

[0034] In some implementations, the application executing on the computing device **202** and or the digital wallet/client device can detect when a picture, snap shot, or screen shot of the digital driver's license (or other digital license or identification stored in the digital wallet) is made. The system may generate an alert that potential identify theft and unlicensed capturing of sensitive information has occurred.

[0035] FIG. **3** illustrates an example of integrating a digital wallet with a digital ID provider **314**. The digital wallet **306** executes on the client device **302**. The user of the client device **302** indicates that he wishes to store and retrieve digital identification using a digital wallet **306**. The user can be presented with a screen that explains the legal issues surrounding the use of the digital identification service, including but not limited to an end user license agreement. The user is given the option of opting in **304** to the use of the digital identification service.

Date Reçue/Date Received 2022-04-27

[0036] In some implementations, the digital wallet may integrate with a digital ID provider **314**. The digital ID provider **314** may require that certain communication with the digital ID provider **314** be secured using a secret (for example, a client key and client secret). For example, the digital identification service may require, for example, that the communication or part of the communication be encrypted or digitally signed. The communication can be encrypted, for example, using a public key-private key or using a symmetric key. A digital signature can be applied using the public key/private key infrastructure.

[0037] The digital identification service may provide a software development kit (SDK) to enable external applications to integrate with the digital identification service. In this example, the digital wallet **306** includes an application **308** that provides functionality to the digital wallet **306** and also includes a digital ID provider SDK **310** that enables the digital wallet to access the digital ID providers **314**. To enhance security, in some implementations, the secret (for example, client key and client secret) is not stored on the client device **302**, but is instead stored on a wallet server **312**. Therefore, communications requiring the use of a secret occur from the wallet server **312** to the digital ID provider **314**. The wallet server can serve as a proxy server to transport information to and from the digital ID provider SDK **310** and the digital ID provider **314**.

[0038] When the user opts into using the digital wallet to store identification documents, the application **308** requests that the digital ID provider SDK **310** authorize the user and the to client device **302** to use the digital ID provider **314**.

[0039] The digital ID provider SDK **310** can prompt the digital ID provider **314** to create and authorize an account. The digital ID provider **314** can generate an authentication code and provides the authentication code to the digital ID provider SDK **310**, which, in turn, can provide the authentication code to the application **308**. The application can provide the authentication code to the wallet server **312** using a secure connection.

[0040] The wallet server **312** can send the authentication code and the secret to the digital ID provider **314**.

[0041] The digital ID provider **314** compares the provided authentication code to a stored authentication code. If the provided authentication code matches the stored authentication code, the digital ID provider **314** registers the user.

[0042] The digital ID provider **314** provides an access token with a refresh token to the wallet server **312**. The wallet server **312** provides the access token with the refresh token to the application **308**. The application provides the access token with the refresh token to the digital ID provider SDK **310**. The digital ID provider SDK **310** provides the access token with the refresh token to the digital ID provider **314**.

[0043] In response to receiving the token, digital ID provider **314** associates the client device **302** and/or the digital wallet **306** with the user.

[0044] FIG. **4** illustrates an example of adding an identification document to a digital wallet. While this example refers to a driver's license, the process described herein may be used to store other forms of identification, including but not limited to Military ID, Student ID, and Passports.

[0045] The user can use the mobile app **306** to obtain a digital image of his driver's license. For example, the user may use a camera associated with the client device **302** to take a picture of the driver's license. Alternatively, or additionally, the user may scan their driver's license using a conventional scanner and transfer the scanned driver's license to the client device **302**. In some implementations, the user is asked to scan a bar code, QR code, or other data bearing code that is shown on driver's license.

[0046] The image of the driver's license or bar code is provided to the digital ID provider SDK **310**. The digital ID provider SDK encrypts the image of the driver's license or scanned code using a public key associated with the digital ID provider **312**. In some implementations, the public key is stored on the client device **302** and is accessible by the digital ID provider SDK **310**. In some implementations, the digital ID provider SDK **310** may obtain the public key from the digital ID provider **312**, for example, through a network request.

[0047] The digital ID provider SDK sends the encrypted payload to the application **308**. The Application **308** sends the encrypted payload to a digital ID module **402** on the wallet server **312**. As the wallet server **312** does not possess the private key of the digital ID provider **312** the wallet server **312** cannot decrypt the encrypted payload.

[0048] The wallet server **312** can obtain additional information about the user. For example, the wallet server may use a user verification module **404** to determine whether the user is a verified user. In some implementations, determining whether a user is verified includes obtaining a user profile **406** of the user. The user profile **406** may include information that can be used to determine whether the user has accounts with a financial institution. For example, the user may have bank account, insurance, or an investment account with the financial institution. Some accounts may include sufficient information to verify the user (for example, a bank account or life insurance account). Other accounts may not include sufficient information to verify the user (for example, a property and casualty insurance account).

[0049] The wallet server also may provide additional information about the user to the digital ID provider Server. This additional information is owned by the wallet server **314** and can be used by the digital ID provider **314** for further verification of the request. The additional information may include identification information about the use stored in the wallet server **314** (such as a customer number). The additional information can also be user specific data such as first name, last name, social security number, etc.

[0050] If the user can be verified, the wallet server **312** collects information about the user.

[0051] If the user cannot be verified, information about the user may be obtained through a third party identification verification system **408**.

[0052] The information about the user (if available) and the encrypted payload is provided to an external gateway **410** that manages communications with the digital ID provider **314**. The External Gateway may send the encrypted payload and the user data (secured by the secret, as described above) to the digital ID provider **314**.

[0053] The digital ID provider **314** can decrypt the image of the driver's license or scanned code using the digital ID provider's private key.

[0054] If the user has been verified the digital ID provider **314** may store the decrypted driver's license for later retrieval. In some implementations, the image of the driver's license or scanned code may be stored in encrypted form. In some implementations, the digital ID provider **314** may use information derived from the scanned code to obtain addi-

Date Reçue/Date Received 2022-04-27

tional driver's licenses details from a third party (such as the issuer of the driver's license).

[0055] If the user has not been verified, the digital ID provider **314** can use the image of the driver's license or scanned code and any provided user data to verify the driver's license with an Identification Verification Check **420**. For example, with the appropriate governmental agency (such as the Department of Motor Vehicles, Department of State, a Military Branch, or similar institution). In some implementations, the digital ID provider may contract with a third party (such as EXPERIAN) to verify the ID. In some implementations, the digital ID provider **312** may verify the user even if the user has been verified by the wallet server.

[0056] Other information about the user may also be stored. For example, the license plate number of a registered vehicle may be stored in association with the digital driver's license. Similarly, a rental car agency may associate a digital driver's license with a rented automobile for the duration of the rental. In some implementations, a digital driver's license may be associated with a financial payment instrument (such as a credit card). The digital driver's license may be associated with a rental automobile based on the use of the credit card to rent the automobile. The digital driver's license may be associated with other appropriate transactions or object based on similar activity.

[0057] FIGS. **5**A-**5**B illustrate an example of providing a digital identification document to a third party. While this example refers to a digital driver's license and a law enforcement officer, a similar process can be used to provide other forms of digital identification to other parties. For example, the process may be used to present a passport to an immigration or customs officer.

[0058] In this example, a car **502** is pulled over by a law enforcement officer **504**. The law enforcement officer obtains an identifier for the car **502** in his computer **506** (in this example, a license plate number but other identifier such as an identifier on a decal may also be used). For example the license plate number may be manually entered, may be scanned using a camera or scanning device. The license plate number could be obtained using NFC, RFID, or another communication mechanism to obtain the information from the license plate or from the car **502**. The computer sends the license plate number to a registration system **508**. The registration system may be, for example, a law enforcement database, an insurance database, a governmental database, or a digital identification database.

[0059] Other methods may be used to determine that the driver possesses a digital driver's license. For example, a sticker or decal may be placed on the car to notify the law enforcement officer that the driver is likely to have a digital driver's license. In some implementations, the other method may also include an identifier (for example, number, bar code, QR code, etc.) that notifies that enables the law enforcement officer to look up the digital driver's licenses associated with the identifier. In some implementations, computers or media included in the dash board of the car may be able to identify that the driver has a digital driver's license. In some implementations, the system may use biometrics such as a fingerprint, retina scan, voice recognition, or other biometric to identify the driver. The identity of the driver can be cross referenced to determine that the driver has a digital driver's license.

[0060] The registration system **508** identifies that the driver of the car **502** may possess a digital driver's license.

[0061] In some implementations, the law enforcement officer may be informed by the individual that he has a digital driver's license.

[0062] The law enforcement officer may use his computer **506** to request the digital driver's license of the potential drivers from a digital ID system **512**. The digital ID system **512** may include one or more disparate systems coordinating together. For example, the digital ID system **512** may include a digital ID provider (for example, the digital ID provider **314** of FIG. **3**) and a Wallet Server (for example, the Wallet Server **312** of FIG. **3**). In some implementations, secure communication between the client device **510** and a digital ID provider may be sent through a Wallet Server. Communications between the client device and the wallet server may be secured by the wallet server. Communications between the Wallet Server and the digital ID provider may be secured using a secret provided to the Wallet Server by the digital ID provider, as described above.

[0063] The law enforcement officer may also send the GPS location. In some implementations, the GPS device may be integrated into the computer **506**, the GPS may be integrated into the law enforcement officer's vehicle **504**, alternatively or additionally the GPS location may be integrated into the GPS device may be into a hand held device, scanner, or other device that is indicative of the location of the law enforcement officer. Communication with the digital ID system **512** may include a verification of the identity of the law enforcement officer. In some implementations, other information may be included, such as a code or comment describing the reason the identification is requested (for example, "traffic stop").

[0064] The digital ID system **512** may compare the location of the law enforcement officer (as determined by the GPS location) to the location of the registered devices of the potential drivers of the car **502**. For example, the car may be insured to John Smith and Jane Smith. John Smith and Jane Smith may have each registered a smart phone (or other client device) with the digital ID system **512**. In some scenarios, the GPS location of one or more devices may be available. For example, the driver of the car **502**, may have enabled the GPS location using his digital wallet when he was pulled over. In other scenarios, the GPS location of the one or more devices may not be available. The digital ID system **512** may send a message or notification to the one or more devices asking them to enable their GPS location. In some implementations a wallet server (not shown) may act as an intermediary between the digital ID system **512** and the client device **510**.

[0065] In some implementations, GPS location information for the requester (in this example, the law enforcement officer) and the holder of the digital driver's license may be maintained for only as long as necessary to provide the digital driver's license. The GPS information may be deleted once the digital driver's license is provided to the requester. In some implementations, GPS location information may be deleted after a predetermined period of time (for example, 10 minutes). Removal of GPS information can facility improved privacy for the sender and the recipient of the driver's license. Other measures to protect the privacy of the participants may be adopted, for example, records may by cryptographically stored, requesting and granting access to a digital ID may require close proximity, etc.

Date Reçue/Date Received 2022-04-27

[0066] In some implementations, the request for the digital ID may be sent through another communication channel. For example, the user may receive an SMS text, push notification, email, etc. . . . . The user may grant or deny permission to share the requested ID using the same mechanism. For example, the user may response to the SMS text, push notification, or email. In some implementations, the user may also receive a telephone call describing the request for ID. The user may be able to respond during the telephone call. For example, using an interactive voice response (IVR) system.

[0067] The user may accept or deny this request. For example, if John Smith is driving the car and Jane Smith is at work, then Jane may decide to deny the request. Similarly, if John Smith is driving the car and Jane Smith is a passenger, Jane may deny the request to facilitate providing accurate information about the driver to the law enforcement officer.

[0068] In some implementations, the law enforcement officer or other authorized individual may be able to request identity of the identity of the driver or individuals in a vehicle without notifying the individual of the request. For example, a signal can be send to a device in the car (such as a receiver, a mobile phone, an NFC device, etc.) which may provide the law enforcement officer with information sufficient to obtain digital driver's licenses or other ID's associated with the device.

[0069] The digital ID provider determines that the GPS location of the individual driving the car is close to the GPS location of the law enforcement officer requesting the digital driver's license. In some implementations, the GPS location of the law enforcement officer and the GPS location of the driver may be considered close if the reported distance between the two locations is within the margin of error of the GPS device. In some implementations, the location of the GPS location of the law enforcement officer and the GPS location of the driver may be considered close if the locations are within a predetermined distance (e.g., 10 feet, 20 feet, 30 feet, 40 feet) as reported by each GPS.

[0070] In this example, the digital ID system **512** identifies the driver as the probable individual from whom the driver's license is requested. The digital ID system **512** ask the driver to allow his driver's license to be shared with the law enforcement officer. As described above, the request may include the identity of the law enforcement officer along with verification that the law enforcement officer is authorized to request the driver's license.

[0071] If multiple devices are determined to be close to the law enforcement officer, the digital ID system **512** may send a request to each device. For example, John Smith may be driving the car **502** and Jane Smith may be a passenger. In this scenario, Jane Smith may elect not to share her driver's license with the law enforcement officer.

[0072] Referring to FIG. **5**B, the driver of the car **502**, provides permission for the law enforcement officer to receive his digital driver's license.

[0073] The digital ID system **512** can encrypt each driver's license, which was shared with the law enforcement officer, using a public key associated with the law enforcement officer. The law enforcement officer's computer decrypts the driver license(s) using the private key associate with the law enforcement officer. The law enforcement officer's computer **506** then display's the driver's licenses that have been shared with the officer.

[0074] FIG. **6** illustrates another example of providing a digital identification document to a third party. While this example refers to a digital driver's license and a law enforcement officer, a similar process can be used to provide other forms of digital identification to other parties. For example, the process may be used to present a passport to an immigration or customs officer.

[0075] In this example, a car **602** is pulled over by a law enforcement officer **604**. The law enforcement officer **604** obtains an identifier to request the digital driver's license of the driver of the car **602**. The identifier may be an identifier associated with the car **602** (for example, a driver's license, an identifier provided on a decal, an NFC signal provided by a transponder, etc.) alternatively the identifier may be associated with the law enforcement officer (for example, the license plate of the law enforcement officer's vehicle, the law enforcement officer's badge number, etc.). The identifier can be added to the computer of the law enforcement office.

[0076] In this example, the computer **606** sends the identifier to the digital ID system **612** requesting the digital driver's license). The driver of the car **602** sends his digital driver's license to the digital id system **612** using the same identifier. The digital ID system **612** matches the request with the grant of permissions (for example, using the identifier) and provides the digital driver's license to the computer **606** of the law enforcement officer.

[0077] In some implementations, when the digital driver's license is provided to the law enforcement officer, records of the transaction are removed from the digital ID system. In this example, the exchange of identifiers occurs between the driver and the law enforcement office. The exchange increases the likelihood that the sender of the driver's license and the recipient of the driver's license are in proximity without relying on GPS tracking technology.

[0078] Other methods may be used to determine that the driver possesses a digital driver's license. For example, a sticker or decal may be placed on the car to notify the law enforcement officer that the driver is likely to have a digital driver's license. In some implementations, the other method may also include an identifier (for example, number, bar code, QR code, etc.) that notifies that enables the law enforcement officer to look up the digital driver's licenses associated with the identifier.

[0079] FIG. **7** illustrates an example of presenting a digital driver's license. In response to a request to view a digital driver's license (not shown for simplicity), a verification system **702** obtains a GPS location of the requesting law enforcement officer (step **1**). The GPS location can be obtained from the police department **704** by querying a server it controls that manages locations of law enforcement officers. Alternatively, the GPS location can be obtained directly from the law enforcement officer who requested to view the digital driver's license using either their browser location function or an on-vehicle GPS device.

[0080] The request may be transmitted through a firewall **706** of the police department. The request may be distributed by the police department to a particular police vehicle or officer who wishes to view the digital driver's license material. The police department **704** (or law enforcement officer) sends a GPS location through the firewall **706** to the to a geolocation matching service **708** (step **2**).

[0081] Generally, both the police department system **704** and the verification system **702** may maintain network security features such as firewalls (for example, firewall **706**

Date Reçue/Date Received 2022-04-27

and firewall **714**). Communication to and from these systems may pass through these network security features.

[0082] Using the information provided by the police department **704**, the verification system **702** sends a silent push request to the client device **710** of the individual for whom the driver's license is requested (step **3**). If the individual has opted in to providing a digital driver's license, the client device **710** can send the GPS location (provided by a GPS device **712**) to the geo-location matching service **708** (step **4**). The information may be provided through the firewall **714** of the verification system **702**.

[0083] The geo-location matching service **708** matches the GPS location provided by the client device **710** with the GPS location provided by the police department **704**. When a match is identified, the police department **704** is notified of the match (step **5**).

[0084] The police department **704** may request the driver's license from the verification system **702** (step **6**). The verification system may include or work with a push notification server **720**. The verification server **702** causes a push notification to be send to the mobile app **716** on the client device **710** (step **7**). The individual may be presented with the option to provide their digital driver's license to the police department. If the individual agrees to present their digital driver's license, a message may be sent to the display response **718** on the verification system **702** (step **8**). The indication of acceptance is transmitted to the police department **704** (step **9**) thereby enabling the police department **704** to obtain and display the driver's license.

[0085] FIG. **8** is a sequence diagram illustrating an example of presenting a digital driver's license to a law enforcement officer. In this example, the driver proactively shares his digital driver's license before it is requested by the law enforcement officer.

[0086] The driver device **802** informs the geo-matching service **804** that the individual is authorizing the sharing of his digital driver's license with authorized parties (such as a law enforcement officer) (step **1**). The driver device **802** provides the location of the driver device **802** (for example, a GPS location).

[0087] The geo-matching service **804** adds the location and permission to a list of pre-authorizations (step **2**). While described as a list for simplicity, other data structures may be used, for example, a dictionary, a hash table, a lookup table, etc.

[0088] The geo-matching service **804** informs the driver device **802** that the request is pending and provides a timer, indicating for how long the pending request is valid (step **3**). In some implementations, the preauthorization to view a digital driver's license may be limited in time, for example, for 1 minute, for 5 minutes, for 10 minutes, etc.

[0089] Before the timer expires (that is, while the pre-authorization to view the digital driver's license is valid), a police application **806** requests the driver's license from the geo-matching service **804** (step **4**). The request may include information that can be used to identify the individual (for example, a license plate number). The request may also include the location of the law enforcement officer making the request.

[0090] The geo-matching service compares the information in the request from the law enforcement officer with entries in the list of pre-authorizations (step **5**). The geo-location service can use the location provided by the driver device **402**, the location provided by the police application **806**, and/or the identifying information (e.g. a license plate number) provided by the police application **806** to identify the individual for whom the law enforcement officer is requesting the license.

[0091] In this example, the geo-location service **804** identifies that the individual has pre-authorized sharing of the digital driver's license. The geo-location service **804** sends information about the license to the police application **806** (step **6**).

[0092] Using the information about the license, the police application **806** requests the digital driver's license from a license information source **808** (step **7**). The license information source can be, for example, a registry of motor vehicles or other governmental or private institution.

[0093] The license information source **808** provides the digital driver's license to the police application **806** (step **8**).

[0094] The police application **806** informs the geo-matching service **804** that the law enforcement officer is viewing the digital driver's license (step **8**).

[0095] The geo-matching service **804** informs the driver device **802** that the law enforcement officer is viewing the digital driver's license (step **10**).

[0096] FIG. **9** is a sequence diagram illustrating an example of presenting a digital driver's license to a law enforcement officer. In this example, the individual reacts to a request for his driver's license by a law enforcement officer.

[0097] A police application **902** requests the driver's license from the geo-matching service **904** (step **1**). The request may include information that can be used to identify the individual (for example, a license plate number). The request may also include the location of the law enforcement officer making the request.

[0098] The geo-matching service **904** compares the information in the request from the law enforcement officer with the list of pre-authorizations (step **2**). In this example, the geo-matching service **904** does not find a pre-authorization. The geo-matching service **904**, determines whether an individual associated with the license plate number (or other identifying information provided by the police application **902**) has opted-in to the digital driver's license (step **3**).

[0099] In this example, the geo-matching service **904** identifies a driver device **906** associated with the information provided by the police application **902**. The geo-matching service **904** sends a silent location request to a push gateway **908** (step **4**).

[0100] The push gateway **908** pushes the silent location request to a driver device **906** (step **5**).

[0101] The driver device **906** sends its location to the geo-matching service **904** (step **6**).

[0102] The geo-matching service **904** compares the information in the request from the law enforcement officer and the information from the driver device **906** (step **7**). Once the geo-matching service **904** matches the request from the police application **902** with the information provided by the driver device **906**, the geo-matching service **904** sends a request for permission to share the digital driver's license to the push gateway **906** (step **8**).

[0103] The push gateway **908** pushes the request to the driver device **906** (step **9**). The request for permission may be displayed on the user interface of the driver device. The user of the driver device may elect to share the digital driver's license. In some implementations, the user may be

Date Reçue/Date Received 2022-04-27

required to authenticate with the device and/or the geo-marching service prior to sharing the driver's license.

[0104] Once the user elects to share the digital driver's license, the driver device **906** informs the geo-matching service **904** that the request has been authorized by the user (step **10**).

[0105] The geo-matching service identifies the law enforcement officer request for the driver's license (step **11**). Pending law enforcement officer requests may be stored in a data structure such as a list, collection, hash table, lookup table, dictionary, or other similar mechanism.

[0106] The geo-matching service **904** provides information about the license to the police application **902** (step **12**.) The information may be information sufficient of obtain the digital driver's license (for example, a driver's license number, a token, or other mechanism).

[0107] Using the information about the license, the police application **902** requests the digital driver's license from a license information source **910** (step **13**). The license information source can be, for example, a registry of motor vehicles or other governmental or private institution.

[0108] The license information source **910** provides the digital driver's license to the police application **902** (step **14**).

[0109] FIG. **10** is a flowchart of an example process for providing a digital driver's license to a requester.

[0110] The process **1000** compares **1002** the location of a requester of a digital identification and an owner of the digital identification. The location of the owner may be obtained without notifying the owner.

[0111] The process **1000** may receive authorization to share the information from the owner. The authorization may be made before or after the requester requests the driver's license. An authorization that is made before the requester requests the driver's license may only be valid for a predetermined period of time.

[0112] The process **1000** provides **1004** the license information to the requester.

[0113] Embodiments of the subject matter and the operations described in this specification can be implemented in digital electronic circuitry, or in computer software, firmware, or hardware, including the structures disclosed in this specification and their structural equivalents, or in combinations of one or more of them. Embodiments of the subject matter described in this specification can be implemented as one or more computer programs (i.e., one or more modules of computer program instructions, encoded on computer storage mediums for execution by, or to control the operation of, data processing apparatus). A computer storage medium can be, or be included in, a computer-readable storage device, a computer-readable storage substrate, a random or serial access memory array or device, or a combination of one or more of them. The computer storage medium can also be, or be included in, one or more separate physical components or media (e.g., multiple CDs, disks, or other storage devices). The computer storage medium can be non-transitory.

[0114] The operations described in this specification can be implemented as operations performed by a data processing apparatus on data stored on one or more computer-readable storage devices or received from other sources.

[0115] The term "data processing apparatus" encompasses all kinds of apparatus, devices, and machines for processing data, including by way of example, a programmable processor, a computer, a system on a chip, or multiple ones, or combinations, of the foregoing The apparatus can include special purpose logic circuitry (e.g., an FPGA (field programmable gate array) or an ASIC (application-specific integrated circuit)). The apparatus can also include, in addition to hardware, code that creates an execution environment for the computer program in question (e.g., code that constitutes processor firmware, a protocol stack, a database management system, an operating system, a cross-platform runtime environment, a virtual machine, or a combination of one or more of them). The apparatus and execution environment can realize various different computing model infrastructures, such as web services, distributed computing and grid computing infrastructures.

[0116] A computer program (also known as a program, software, software application, script, or code) can be written in any form of programming language, including compiled or interpreted languages, declarative or procedural languages, and it can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, object, or other unit suitable for use in a computing environment. A computer program may, but need not, correspond to a file in a file system. A program can be stored in a portion of a file that holds other programs or data (e.g., one or more scripts stored in a markup language document), in a single file dedicated to the program in question, or in multiple coordinated files (e.g., files that store one or more modules, sub-programs, or portions of code). A computer program can be deployed to be executed on one computer or on multiple computers that are located at one site or distributed across multiple sites and interconnected by a communication network.

[0117] The processes and logic flows described in this specification can be performed by one or more programmable processors executing one or more computer programs to perform actions by operating on input data and generating output. The processes and logic flows can also be performed by, and apparatus can also be implemented as, special purpose logic circuitry (e.g., an FPGA (field programmable gate array) or an ASIC (application-specific integrated circuit)).

[0118] Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any kind of digital computer. Generally, a processor will receive instructions and data from a read-only memory or a random access memory or both. The essential elements of a computer are a processor for performing actions in accordance with instructions and one or more memory devices for storing instructions and data. Generally, a computer will also include, or be operatively coupled to receive, data from or transfer data to, or both, one or more mass storage devices for storing data (e.g., magnetic, magneto-optical disks, or optical disks), however, a computer need not have such devices. Moreover, a computer can be embedded in another device (e.g., a mobile telephone, a personal digital assistant (PDA), a mobile audio or video player, a game console, a Global Positioning system (GPS) receiver, or a portable storage device (e.g., a universal serial bus (USB) flash drive)), to name just a few. Devices suitable for storing computer program instructions and data include all forms of non-volatile memory, media and memory devices, including by way of example semiconductor memory devices (e.g., EPROM, EEPROM, and flash

Date Reçue/Date Received 2022-04-27

memory devices), magnetic disks (e.g., internal hard disks or removable disks), magneto-optical disks, and CD-ROM and DVD-ROM disks. The processor and the memory can be supplemented by, or incorporated in, special purpose logic circuitry.

[0119] To provide for interaction with a user, embodiments of the subject matter described in this specification can be implemented on a computer having a display device (e.g., a CRT (cathode ray tube) or LCD (liquid crystal display) monitor) for displaying information to the user and a keyboard and a pointing device (e.g., a mouse or a trackball) by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback (e.g., visual feedback, auditory feedback, or tactile feedback) and input from the user can be received in any form, including acoustic, speech, or tactile input. In addition, a computer can interact with a user by sending documents to and receiving documents from a device that is used by the user (for example, by sending web pages to a web browser on a user's user device in response to requests received from the web browser).

[0120] Embodiments of the subject matter described in this specification can be implemented in a computing system that includes a back-end component (e.g., as a data server), a middleware component (e.g., an application server), or a front-end component (e.g., a user computer having a graphical user interface or a Web browser through which a user can interact with an implementation of the subject matter described in this specification), or any combination of one or more 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") and a wide area network ("WAN"), an inter-network (e.g., the Internet), and peer-to-peer networks (e.g., ad hoc peer-to-peer networks).

[0121] The computing system can include users and servers. A user and server are generally remote from each other and typically interact through a communication network. The relationship of user and server arises by virtue of computer programs running on the respective computers and having a user-server relationship to each other. In some embodiments, a server transmits data (e.g., an HTML page) to a user device (e.g., for purposes of displaying data to and receiving user input from a user interacting with the user device). Data generated at the user device (e.g., a result of the user interaction) can be received from the user device at the server.

[0122] While this specification contains many specific implementation details, these should not be construed as limitations on the scope of any inventions or of what may be claimed, but rather as descriptions of features specific to particular embodiments of particular inventions. 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.

[0123] 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.

[0124] Thus, particular embodiments of the subject matter have been described. Other embodiments are within the scope of the following claims. In some cases, the actions recited in the claims can be performed in a different order and still achieve desirable results. In addition, 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:

1. A computer-implemented method comprising:

comparing the location of a requester of a digital identification to the location of an owner of the digital identification; and

providing information about the digital identification to the requester based at least in part on determining that the requester and the owner are within a predetermined distance.

2. The computer-implemented method of claim **1**, wherein providing information about the digital identification is further based on receiving authorization to share the information from the owner.

3. The computer-implemented method of claim **1**, further comprising:

receiving a pre-authorization to share the digital identification; and

storing the pre-authorization.

4. The computer-implemented method of claim **3**, wherein the pre-authorization expires after a predetermined period of time.

5. The computer-implemented method of claim **1**, wherein the location of the owner of the digital identification is obtained without notifying the owner.

6. The computer-implemented method of claim **1**, further comprising:

receiving an license plate number associated with a vehicle of the owner;

identifying the owner based on the license plate number; and

contacting a user device of the owner requesting the digital driver's license.

7. A non-transitory computer storage medium encoded with computer program instructions that when executed by one or more computers cause the one or more computers to perform operations comprising:

comparing the location of a requester of a digital identification to the location of an owner of the digital identification; and

Date Reçue/Date Received 2022-04-27

providing information about the digital identification to the requester based at least in part on determining that the requester and the owner are within a predetermined distance

8. The non-transitory computer storage medium of claim **7**, wherein providing information about the digital identification is further based on receiving authorization to share the information from the owner.

9. The non-transitory computer storage medium of claim **7**, further comprising:

receiving a pre-authorization to share the digital identification; and

storing the pre-authorization.

10. The non-transitory computer storage medium of claim **9**, wherein the pre-authorization expires after a predetermined period of time.

11. The non-transitory computer storage medium of claim **7**, wherein the location of the owner of the digital identification is obtained without notifying the owner.

12. The non-transitory computer storage medium of claim **7**, further comprising:

receiving an license plate number associated with a vehicle of the owner;

identifying the owner based on the license plate number; and

contacting a user device of the owner requesting the digital driver's license.

13. A system comprising:

one or more computers and one or more storage devices storing instructions that are operable, when executed by the one or more computers, to cause the one or more computers to perform operations comprising:

comparing the location of a requester of a digital identification to the location of an owner of the digital identification; and

providing information about the digital identification to the requester based at least in part on determining that the requester and the owner are within a predetermined distance

14. The system of claim **13**, wherein providing information about the digital identification is further based on receiving authorization to share the information from the owner.

15. The system of claim **13**, further comprising:

receiving a pre-authorization to share the digital identification; and

storing the pre-authorization.

16. The system of claim **15**, wherein the pre-authorization expires after a predetermined period of time.

17. The system of claim **13**, wherein the location of the owner of the digital identification is obtained without notifying the owner.

18. The system of claim **13**, further comprising:

receiving an license plate number associated with a vehicle of the owner;

identifying the owner based on the license plate number; and

contacting a user device of the owner requesting the digital driver's license.

* * * * *

Date Reçue/Date Received 2022-04-27

General Correspondence (Patent)

Date: April 27, 2022 10:23:34 AM

008
067
CAP
MH

Application Number

3154428

Title of invention

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Applicant(s) or Inventor Name(s)

Applicant or Inventor Name

Sender

Family Name:
First Name:
Initial:
Name of Corporation or Firm: ROBIC
Address Line 1: 20-630 Boul Ren&#65533;-L&#65533;vesque O
Address Line 2:
Address Line 3:
City/Town: Montr&#65533;al
Province/State: Qu&#65533;bec
Country: Canada
Postal/Zip Code: H3B 1S6
Telephone Number: 514-987-6242
Fax Number: 514-845-7874
Email Address: opic.brevets@robic.com
Communicate by: Electronic Mail (Non secure)

Correspondence Instructions

Commissioner, please find enclosed the following documents: Voluntary Submission of Information Letter and other documents (6). Respectfully submitted.

Description of Fee

No fee has been entered.
Total Fee Payment: $0.00

Payment method

No Charge

Attachments

1. 2022-04-27 Voluntary submission of information - 014211-0023.pdf
Other
Voluntary submission of information

2. 1_1_GMT4110 WO_ISR - Nov 20 2020.pdf
Other
Document

3. 1_2_D1_US2016294831A1.pdf
Other
Document

4. 1_2_D2_WO2015036957A1.pdf
Other
Document

5. 1_2_D3_US2016156386A1.pdf
Other
Document

6. 1_2_D4_XP061034511.pdf
Other
Document

7. 1_2_D5_XP055689283.pdf
Other
Document

Transmission Identifier: pgc_sophiacoutu_20220427102334276

Date: April 27, 2022 10:23:34 AM

Commissioner of Patents
50 Victoria Street
Place du Portage
Phase I
Gatineau, Quebec
Canada
K1A 0C9

Application Number: 3154428
Title of invention: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
Applicant(s) or Inventor(s) Name(s): THALES DIS FRANCE SAS
THALES DIS FRANCE SAS
Reference Number: 014211-0023

Instructions: Commissioner, please find enclosed the following documents: Voluntary Submission of Information Letter and other documents (6). Respectfully submitted.

Attached are the following documents:
1. 2022-04-27 Voluntary submission of information - 014211-0023.pdf
Voluntary submission of information
Other
2. 1_1_GMT4110 WO_ISR - Nov 20 2020.pdf
Document
Other
3. 1_2_D1_US2016294831A1.pdf
Document
Other
4. 1_2_D2_WO2015036957A1.pdf
Document
Other
5. 1_2_D3_US2016156386A1.pdf
Document
Other
6. 1_2_D4_XP061034511.pdf
Document
Other
7. 1_2_D5_XP055689283.pdf
Document
Other

,
ROBIC
20-630 Boul Ren-L-vesque O
Montr-al
Qu-bec
Canada
H3B 1S6
Tel: 514-987-6242
Fax: 514-845-7874
Email:opic.brevets@robic.com

Transmission Identifier: pgc_sophiacoutu_20220427102334276

ROBIC | 892

April 27, 2022

CANADIAN INTELLECTUAL PROPERTY OFFICE

Inventor(s):	FAHER, Mourad et al.
Applicant(s):	THALES DIS FRANCE SAS
Patent application N° :	3.154.428
Title:	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
Our file.:	014211-0023

COMMISSIONER OF PATENTS
GATINEAU, QUEBEC, K1A 0C9

VOLUNTARY SUBMISSION OF INFORMATION

Commissioner:

We bring the following information to the attention of CIPO:

- International Search Report for EP Patent Application No. 2020/076906, issued on November 12, 2020;
- D1: US 2016/0294831 A1;
- D2: WO 2015/036957 A1;
- D3: US 2016/0156386 A1;
- D4: EMVCO, "EMV '96 Integrated Circuit Card Application Specification for Payment Systems", EMV, EMVCO, vol. 3.1.1; Contact, 31 May 1998 (1998-05-31), pages 1-62, XP061034511;
- D5: 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.

It is respectfully requested that this information be made of record and be considered for examination purpose.

Copies of the above-mentioned documents are enclosed.

Instructions

It is believed that the present application is in good standing. If, however, it appears that the application is deemed abandoned, or if CIPO considers that this application is deemed abandoned, we request CIPO to inform us in writing immediately.

CONCLUSION

In view of the above, it is submitted that the present patent application is in compliance with the *Patent Act* and *Patent Rules*. Allowance of the claims and issuance of a Notice of Allowance is therefore respectfully solicited.

The Examiner is invited to call us if any further amendment will expedite allowance of the present patent application or if the Examiner has any suggestions or questions concerning this

ROBIC, L.L.P.
www.robic.ca
info@robic.com

MONTREAL
630 René-Lévesque Boulevard West
20th Floor
Montreal, Quebec, Canada H3B 1S6
Tel.: +1 514 987-6242 Fax: +1 514 845-7874

QUEBEC
Le Delta Building
2875 Laurier Boulevard, Delta 3 - suite 700
Quebec, Quebec, Canada G1V 2M2
Tel.: +1 418 653-1888 Fax.: +1 418 653-0006

Date Reçue/Date Received 2022-04-27

patent application.

Respectfully submitted,



ROBIC S.E.N.C.R.L / LLP
Avocats, agents de brevets et de marques de commerce /
Lawyers, Patent and Trademark Agents

Agent(e) de brevets / Patent Agent: Gabrielle Moisan (+1 514-987-2717)

GMO/sac

Encl. As mentioned above

Date Reçue/Date Received 2022-04-27

General Correspondence (Patent)

Date: April 27, 2022 10:23:34 AM

008
067
CAP
MH

Application Number

3154428

Title of invention

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Applicant(s) or Inventor Name(s)

Applicant or Inventor Name

Sender

Family Name:
First Name:
Initial:
Name of Corporation or Firm: ROBIC
Address Line 1: 20-630 Boul Ren&#65533;-L&#65533;vesque O
Address Line 2:
Address Line 3:
City/Town: Montr&#65533;al
Province/State: Qu&#65533;bec
Country: Canada
Postal/Zip Code: H3B 1S6
Telephone Number: 514-987-6242
Fax Number: 514-845-7874
Email Address: opic.brevets@robic.com
Communicate by: Electronic Mail (Non secure)

Correspondence Instructions

Commissioner, please find enclosed the following documents: Voluntary Submission of Information Letter and other documents (6). Respectfully submitted.

Description of Fee

No fee has been entered.
Total Fee Payment: $0.00

Payment method

No Charge

Attachments

1. 2022-04-27 Voluntary submission of information - 014211-0023.pdf
Other
Voluntary submission of information

2. 1_1_GMT4110 WO_ISR - Nov 20 2020.pdf
Other
Document

3. 1_2_D1_US2016294831A1.pdf
Other
Document

4. 1_2_D2_WO2015036957A1.pdf
Other
Document

5. 1_2_D3_US2016156386A1.pdf
Other
Document

6. 1_2_D4_XP061034511.pdf
Other
Document

7. 1_2_D5_XP055689283.pdf
Other
Document

Transmission Identifier: pgc_sophiacoutu_20220427102334276

Date: April 27, 2022 10:23:34 AM

Commissioner of Patents
50 Victoria Street
Place du Portage
Phase I
Gatineau, Quebec
Canada
K1A 0C9

Application Number: 3154428
Title of invention: SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
Applicant(s) or Inventor(s) Name(s): THALES DIS FRANCE SAS
THALES DIS FRANCE SAS
Reference Number: 014211-0023

Instructions: Commissioner, please find enclosed the following documents: Voluntary Submission of Information Letter and other documents (6). Respectfully submitted.

Attached are the following documents:
1. 2022-04-27 Voluntary submission of information - 014211-0023.pdf
Voluntary submission of information
Other
2. 1_1_GMT4110 WO_ISR - Nov 20 2020.pdf
Document
Other
3. 1_2_D1_US2016294831A1.pdf
Document
Other
4. 1_2_D2_WO2015036957A1.pdf
Document
Other
5. 1_2_D3_US2016156386A1.pdf
Document
Other
6. 1_2_D4_XP061034511.pdf
Document
Other
7. 1_2_D5_XP055689283.pdf
Document
Other

,
ROBIC
20-630 Boul Ren-L-vesque O
Montr-al
Qu-bec
Canada
H3B 1S6
Tel: 514-987-6242
Fax: 514-845-7874
Email:opic.brevets@robic.com

Transmission Identifier: pgc_sophiacoutu_20220427102334276

Courtoisie – Lettre confirmant l'entrée en phase nationale en vertu du PCT
Courtesy – Letter Acknowledging PCT National Phase Entry

Détails de la lettre Letter Details	
Date de la lettre: Letter Date:	2022/04/11
No de la demande: Application No.:	3154428
Votre no de référence: Your Reference No.:	014211-0023
Date de dépôt: Filing Date:	2020/09/25

Date d'entrée en phase nationale: National Phase Entry Date:	2022/04/11
No de la demande PCT: PCT Application No.:	EP2020076906
Demandeur(s)/Applicant(s):	THALES DIS FRANCE SAS
Inventeur(s)/Inventor(s):	FAHER, Mourad; BAYLE, Carole
Titre de l'invention:	MÉCANISME DE SÉCURITÉ POUR ESPACES DE NOMMAGE UTILISÉS DANS L'IDENTIFICATION ÉLECTRONIQUE SUR DES DISPOSITIFS MOBILES
Title of invention:	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
Données de priorité/Priority Data:	EP (19306357.5) 2019/10/18

Vous devez payer une taxe annuelle pour maintenir en état votre demande de brevet pour chaque période d'une année à compter du deuxième anniversaire de la date de dépôt de votre demande. Le montant de la taxe de maintien en état et le délai de paiement sont indiqués à l'annexe 2 des Règles sur les brevets.

Annual fees to maintain your patent application are required for each one-year period from the second anniversary of the filing date of the application. The amount and time limits for paying maintenance fees can be found in Schedule 2 of the Patent Rules.

CITM_AppAckLetterPdf 18Jun2021

Une demande de brevet ne sera examinée que sur demande.

Pour de plus amples renseignements concernant cette lettre, veuillez consulter le Recueil des pratiques du Bureau des brevets (RPBB) sur le site canada.ca/brevets ou téléphoner au 1-819-953-7683.

A patent application will only be examined on request.

For more information regarding this letter, please refer t the Manual of Patent Office Practice (MOPOP) at canada.ca/patents or phone 1-819-953-7683.

CITM_AppAckLetterPdf 18Jun2021

Confirmation de soumission / Confirmation of submission
Demande d'entrée en phase nationale d'une demande PCT / Request for national phase entry of a PCT application

Présenté par
Submitted By

Nom: **Name:**	Anne Verreault
Adresse courriel: **Email:**	verreault@robic.com

Résumé de la demande
Application Summary

Numéro PCT: **PCT Number:**	EP2020076906
Titre:	MÉCANISME DE SÉCURITÉ POUR ESPACES DE NOMMAGE UTILISÉS DANS L'IDENTIFICATION ÉLECTRONIQUE SUR DES DISPOSITIFS MOBILES
Title:	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
No. de la demande CA.: **CA App. No.:**	3154428
Date d'entrée en phase nationale: **National Entry Date:**	2022/04/11
Numéro de référence: **Reference Number:**	014211-0023

Renseignements détaillés – Renseignements bibliographiques
Details – Bibliographic Information

CITM_Confirmation_of_submission 8Dec2021

Date de dépôt PCT: **PCT Filing Date:**	2020/09/25
Date de publication PCT: **PCT Publication Date:**	2021/04/22
Numéro de publication PCT: **PCT Publication Number:**	WO 2021/073853 A1
Langue de publication PCT: **PCT Publication Language:**	Anglais English
Abrégé:	L'invention concerne un système, un dispositif mobile et un procédé de gestion de politiques de sécurité pour des éléments de données stockés dans un portefeuille d'identification électronique (eID) sur le dispositif mobile. Des politiques de sécurité sont associées à chaque espace de nommage d'une pluralité d'espaces de nommage supportés sur un dispositif mobile et un terminal vérificateur sert à sélectionner un espace de nommage pour accéder à un élément de données stocké sur le dispositif mobile sur la base des politiques de sécurité associées à la pluralité d'espaces de nommage supportés sur le dispositif mobile.
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.
Classification: **Classification:**	G06Q 50/26 (2012.01) G06Q 20/32 (2012.01) G06Q 20/36 (2012.01)
Administration chargée de la recherche internationale (ISA): **International Searching Authority (ISA):**	EP - Office européen des brevets (OEB) EP - European Patent Office (EPO)
Chapitre: **Chapter:**	Chapitre I Chapter I
Langue de la demande en phase nationale: **Language of national entry application:**	Anglais English

Renseignements détaillés – Attestation de langue
Details – Language Attestation

CITM_Confirmation_of_submission 8Dec2021

Vous avez fourni les éléments suivants dans la Langue de la demande en phase nationale indiquée ci-dessus : la demande, tous les renseignements et documents justificatifs exigés, autres qu'une demande initialement déposée dans une langue autre que le français ou l'anglais: Oui

The application, all required information and supporting documents, other than an application originally filed in a language other than English or French, have been provided in the language of the application indicated above: Yes

Renseignements détaillés – Entrée tardive
Details – Late Entry

Cette demande d'entrer en phase nationale au Canada est soumise plus de trente (30) mois après la première date de priorité: Non

This request to enter national phase in Canada is submitted later than 30 months after the earliest priority date: No

Renseignements détaillés – Rétablissement des droits
Details - Reinstatement of Rights

Le demandeur demande que les droits du demandeur soient rétablis en ce qui concerne la demande internationale et le demandeur déclare que le non-respect des exigences liées à l'entrée en phase nationale dans les 30 mois suivant la date de priorité n'était pas intentionnel: Non

The applicant requests that the rights of the applicant be reinstated with respect to the international application and the applicant states the failure to comply with the requirements to enter national phase within 30 months from the priority date was unintentional: No

Renseignements détaillés – Correspondance
Details – Correspondence

Méthode de correspondance: **Method of Correspondence:**	Courriel Email

Renseignements détaillés – Renseignements relatifs à la priorité
Details – Priority Information

Numéro de demande Application Number	Pays/Territoire Country/Territory	Source Source	Code d'accès du SAN DAS Access Code	Date de dépôt Filing Date	Requête en restauration Request Restoration

CITM_Confirmation_of_submission 8Dec2021

Numéro de demande Application Number	Pays/Territoire Country/Territory	Source Source	Code d'accès du SAN DAS Access Code	Date de dépôt Filing Date	Requête en restauration Request Restoration
19306357.5		OMPI WIPO		2019-10-18	Non No

Parties – Consentement à la nomination
Parties – Consent to Appointment

La demande est-elle soumise par un agent de brevets nommé à l'égard de cette demande de brevet ou une personne travaillant pour l'entreprise d'un agent de brevets nommé à l'égard de cette demande de brevet: Oui

Is the application being submitted by a patent agent appointed in respect of this patent application or someone working for the firm of a patent agent appointed in respect of this patent application: Yes

Parties – Toutes les parties
Parties – All Parties

Nom Name	Type Type	Rôle Role	Ordre Order	Adresse Address	#de téléphone Phone #	#d'entreprise Business #	# de fax Fax #	Adresse courriel Email	Représentant commun Common Rep.	Source Source
THALES DIS FRANCE SAS	Entreprise Firm	Demandeur Applicant	1	6, rue de la Verrerie 92190 MEUDON FR - France					Non No	OMPI WIPO

CITM_Confirmation_of_submission 8Dec2021

Nom Name	Type Type	Rôle Role	Ordre Order	Adresse Address	#de téléphone Phone #	#d'entreprise Business #	# de fax Fax #	Adresse courriel Email	Représentant commun Common Rep.	Source Source
Mourad FAHER	Personne Person	Inventeur Inventor	1	THALES DIS FRANCE SA Intellectual Property Department 6 Rue de la Verrerie 92190 MEUDON FR - France					Non No	OMPI WIPO
Carole BAYLE	Personne Person	Inventeur Inventor	2	THALES DIS FRANCE SA Intellectual Property Department 6 Rue de la Verrerie 92190 MEUDON FR - France					Non No	OMPI WIPO
ROBIC S.E.N.C.R.L / LLP	Entreprise Firm	Agent		630, René-Lévesque W. Boulevard, 20th Fl Montreal Quebec H3B 1S6 CA - Canada	5149876242	865601371	5148457874	opic.brevets@robic.com	Non No	Anne Verreault

Options – Petite entité
Options – Small Entity

Le(s) demandeur(s) estime(nt) que la condition relative au statut de petite entité visée au paragraphe 44(2) des Règles sur les brevets est remplie: Non

CITM_Confirmation_of_submission 8Dec2021

The applicant(s) believes that the small entity status condition set out in subsection 44(2) of the Patent Rules is met: No

Signature / Signature:

Le signataire est un professionnel étranger autorisé: Non

The signatory is an authorized foreign practitioner: No

Options – l'examen avancé et accéléré
Options – Advanced and Accelerated Examination

Technologies vertes / Green Technologies: Non / No

Ordonnance spéciale / Special Order: Non / No

Autoroute du traitement des demandes de brevet (PPH) / Patent Prosecution Highway (PPH): Non / No

COVID-19 (petites entités seulement) / COVID-19 (small entities only): Non / No

Options – options additionelles
Options – Additional Options

Faire une requête d'examen / Request Examination: Oui / Yes

Demander l'accessibilité au public anticipée / Request for early public inspection: Non / No

Options – paiement des taxes de maintien
Options – Payment of maintenance fees

Ajouter le paiement de la prochaine taxe de maintien due / Add payment of the next maintenance fee due: Non / No

Paiements – détails de paiement
Payments – Payment Details

Numéro de transaction: **Transaction Number:**	10144197
Numéro de demande: **Application Order Number:**	00004922
Mode: **Method:**	Carte de crédit Credit Card
Numéro du compte de dépôt: **Deposit Account Number:**	
Date du paiement: **Date Paid:**	2022/04/11
Montant (CAD): **Amount (CAD):**	$1,221.55

Paiements – taxes
Payments – Fees

Type de taxe **Fee Type**	**Montant de taxes (CAD)** **Fee Amount (CAD)**
Taxe d'examen Examination fee	$814.37
Taxe nationale de base Basic national fee	$407.18

Documents - OMPI
Documents - WIPO

Nom du fichier **File Name**	**Type** **Type**	**Nombre de pages** **No. of Pages**	**Source** **Source**
PCT_abstract-figure_en_id00000059544104.pdf	Figure de l'abrégé (OMPI) WIPO Abstract-Figure	1	WIPO

CITM_Confirmation_of_submission 8Dec2021

Nom du fichier File Name	Type Type	Nombre de pages No. of Pages	Source Source
PCT_front-page_id00000059544104.pdf	Page de couverture (OMPI) WIPO Cover Page	1	WIPO
PCT_description_id00000059544104.pdf	Description (OMPI) WIPO Description	17	WIPO
PCT_claims_id00000059544104.pdf	Revendications (OMPI) WIPO Claims	4	WIPO
PCT_drawings_id00000059544104.pdf	Dessins (OMPI) WIPO Drawings	9	WIPO
PCT_wo-search-report_id00000059544104.pdf	Rapport de recherche internationale International Search Report	3	WIPO
PCT_IB306_id00000062809566.pdf	Notification de l'enregistrement d'un changement (IB306) Notification of Recording a Change (IB306)	1	WIPO
PCT_IB304_id00000059555701.pdf	Notification relative à la présentation ou à la transmission du document de priorité Notification Concerning Submission or Transmittal of Priority Document	1	WIPO
PCT_PDOC_id00000059503524.pdf	Document de priorité Priority Document	35	WIPO
PCT_WOSA_id00000059538030.pdf	Opinion écrite Written Opinion	8	WIPO

Documents - documents de la demande
Documents - Application Documents

CITM_Confirmation_of_submission 8Dec2021

Nom du fichier File Name	Type Type	Nombre de pages No. of Pages	Taxe Fee	Commentaires Comments	Source Source
014211-0023 Request.pdf	Lettre de présentation Cover Letter	2		Request for entry form	Anne Verreault
014211-0023 Statement.pdf	Déclaration du droit du demandeur Statement of Entitlement	1		Declaration	Anne Verreault

Commentaires
Comments

The country of the priority document is EP. Should the amount(s) indicated in this letter be insufficient to cover all of the fee(s) for which payment(s) is(are) explicitly or implicitly requested by this letter, or should a fee payment cannot be charged to the designated credit card, CIPO is hereby unconditionally, clearly and unequivocally authorized to debit any amount required to pay or complete any applicable fee from our deposit account 600000233.

50, rue Victoria • Place du Portage 1 • Gatineau (Québec) K1A 0C9 • www.opic.ic.gc.ca
50 Victoria Street • Place du Portage 1 • Gatineau, Québec K1A 0C9 • www.opic.ic.gc.ca

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:	PCT
see form PCT/ISA/220	WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY (PCT Rule 43*bis*.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.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP2020/076906	25.09.2020	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 43*bis*.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 notifed 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:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Nicoli, Félix Telephone No. +31 70 340-0

Form PCT/ISA/237 (Cover Sheet) (January 2015)
CA 03154428 2022-4-11

Box No. I 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 43*bis*.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 13*ter*.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 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.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:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-16
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-16
Industrial applicability (IA)	Yes:	Claims	1-16
	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 2016/156386 A1 (VAN NIEUWENHUYZE OLIVIER [BE] ET AL) 2 June 2016 (2016-06-02)
D4	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]
D5	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]

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 whishes to access a service for which he/she needs to provide identification information. The user can provides 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. It 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 legitimity 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 by a mobile device with a digital wallet in communication with a reader. Any other feature is deemed to relate to a 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 a reader. Such a system was well-known in art at the priority date of the application as this 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 his feature can be found in claim 1.

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

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*)**

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int

CA 03154428 2022-4-11

Digital Access Service
(DAS)

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

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)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int

CA 03154428 2022-4-11

Europäisches Patentamt
European Patent Office
Office européen des brevets

Bescheinigung	Certificate	Attestation
Die angehefteten Unterlagen stimmen mit der als ursprünglich eingereicht geltenden Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.	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.	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 President de l'Office européen des brevets
p.o.



V. Joseph

Anmeldung Nr:
Application no.: 19306357.5
Demande no :

Anmeldetag:
Date of filing: 18.10.19
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 Vertragstaaten / 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, of 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 filed 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

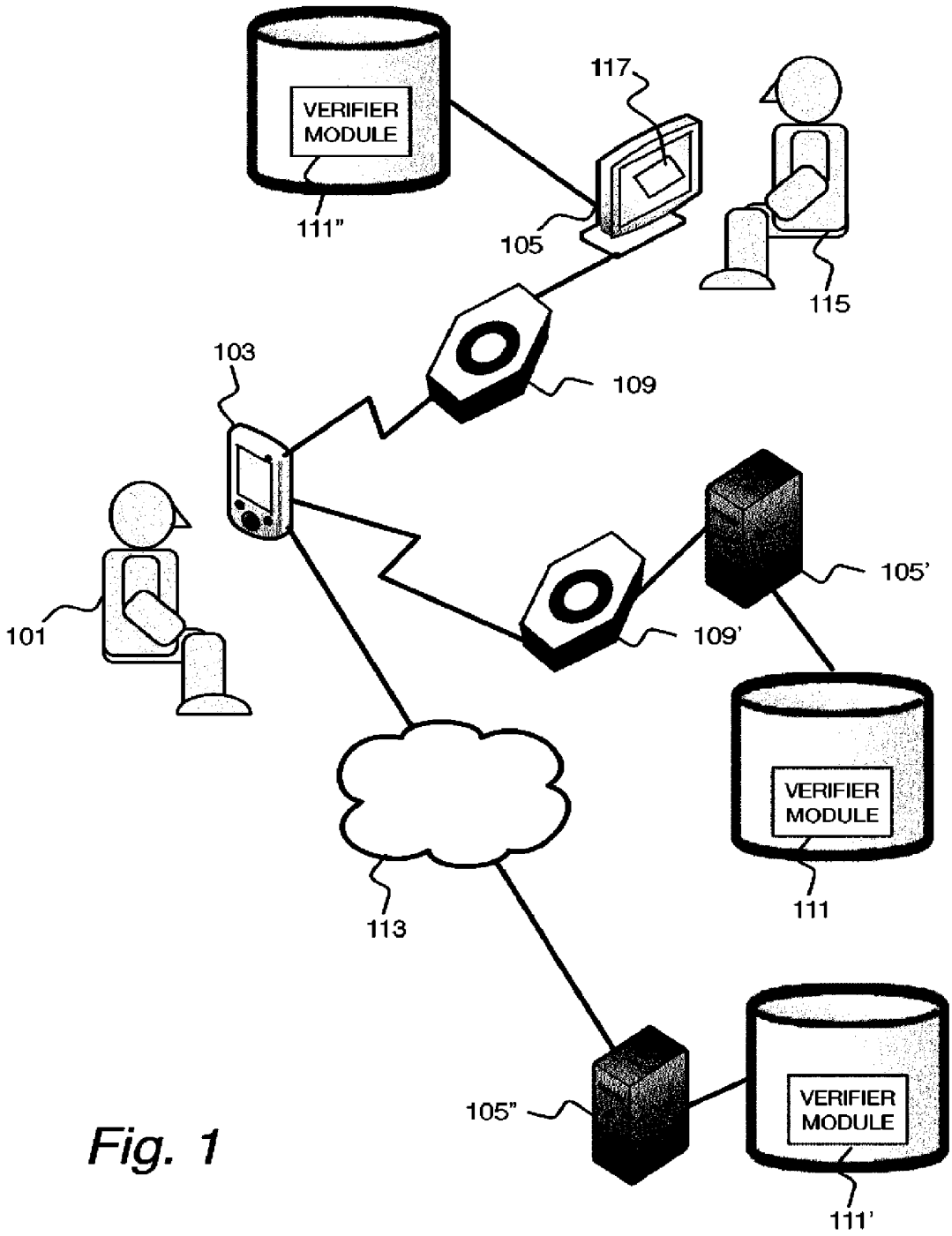

VERIFIER MODULE
111"
117
105
115
103
109
101
105'
109'
VERIFIER MODULE
111
113
105"
VERIFIER MODULE
111'

Fig. 1

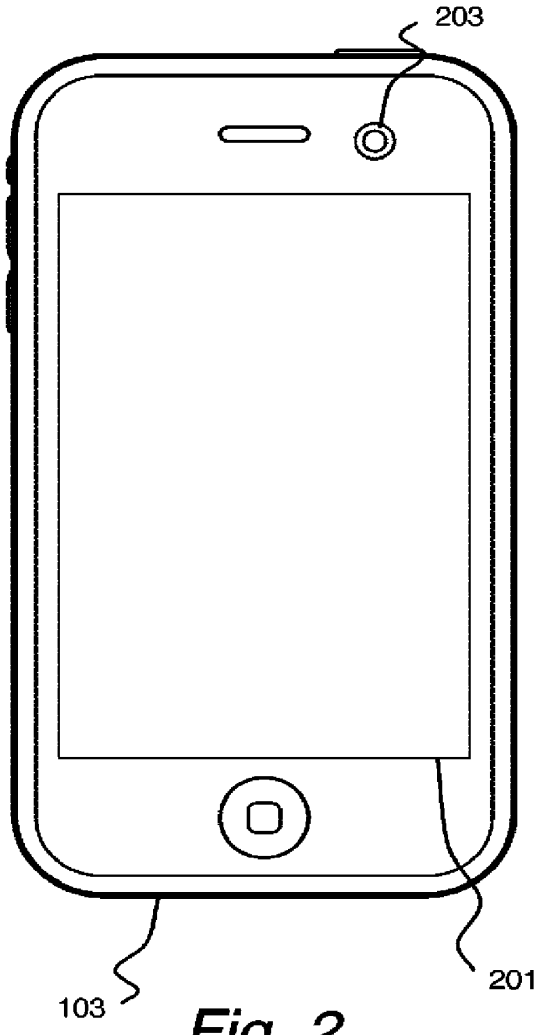

203
103
201

Fig. 2

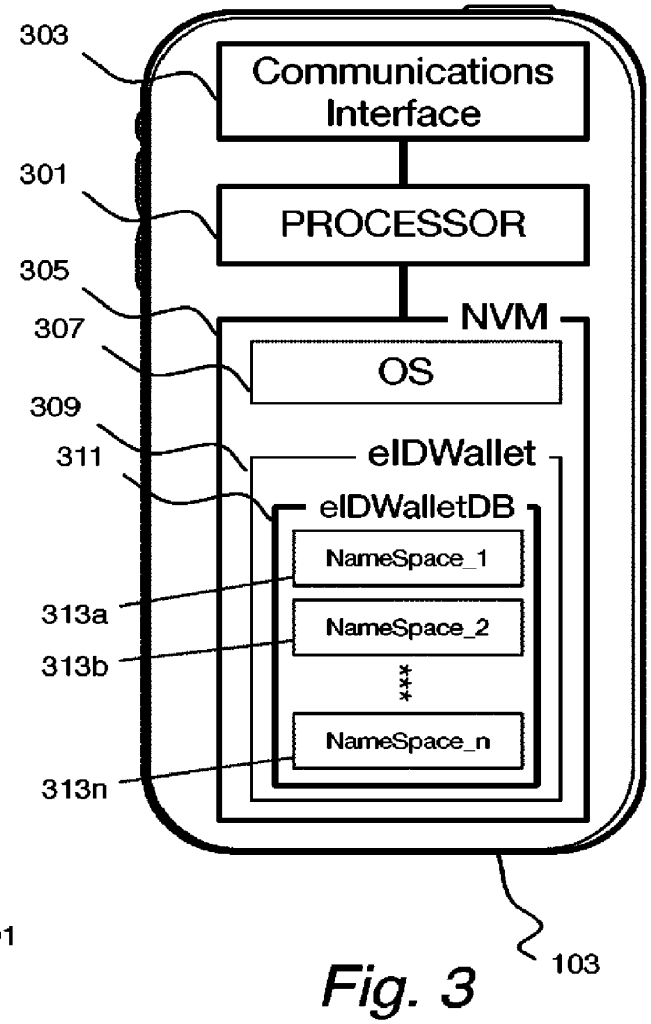

303
Communications Interface
301
PROCESSOR
305
NVM
307
OS
309
311
eIDWallet
eIDWalletDB
NameSpace_1
313a
NameSpace_2
313b
NameSpace_n
313n
103

Fig. 3

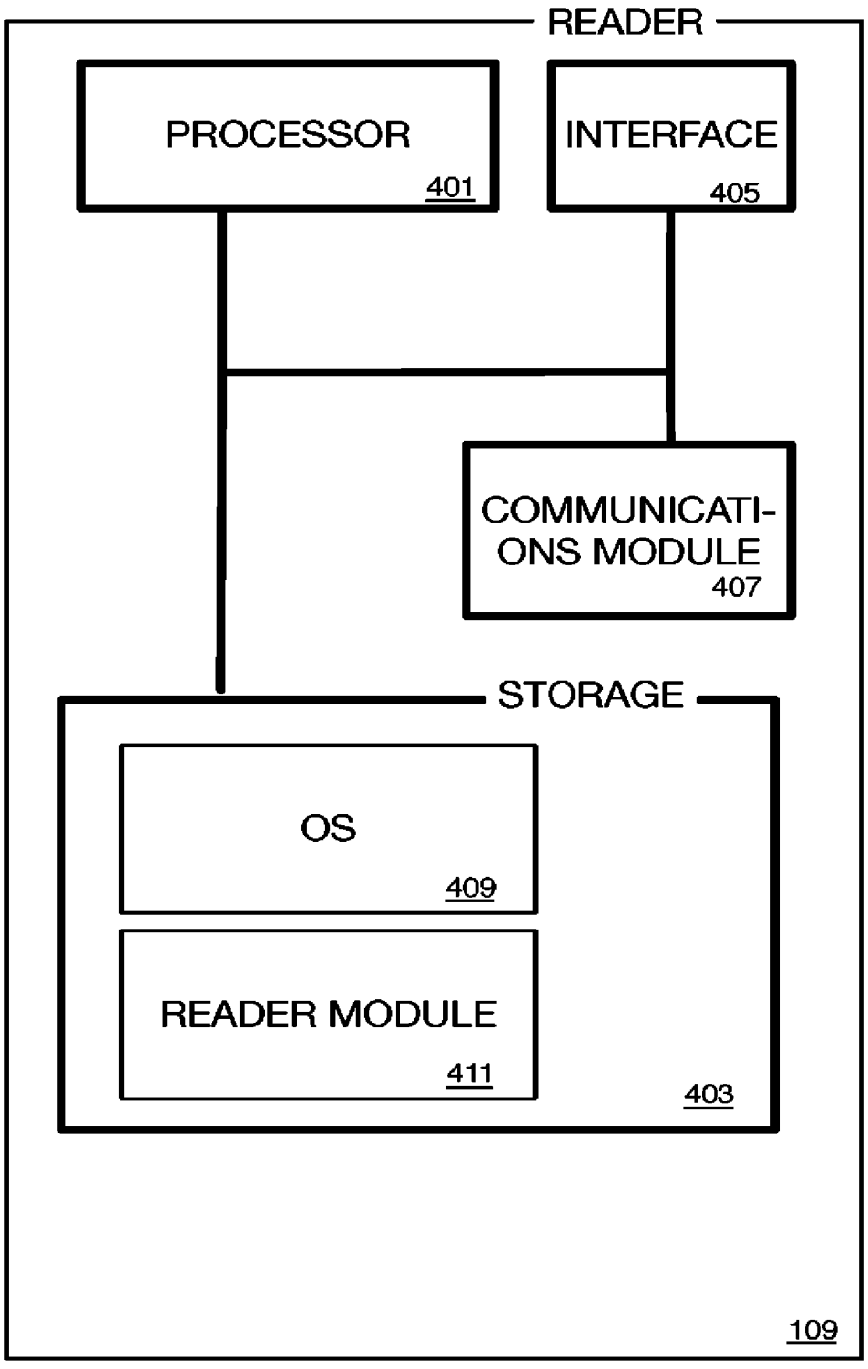

READER
PROCESSOR
401
INTERFACE
405
COMMUNICATI-
ONS MODULE
407
STORAGE
OS
409
READER MODULE
411
403
109

Fig. 4

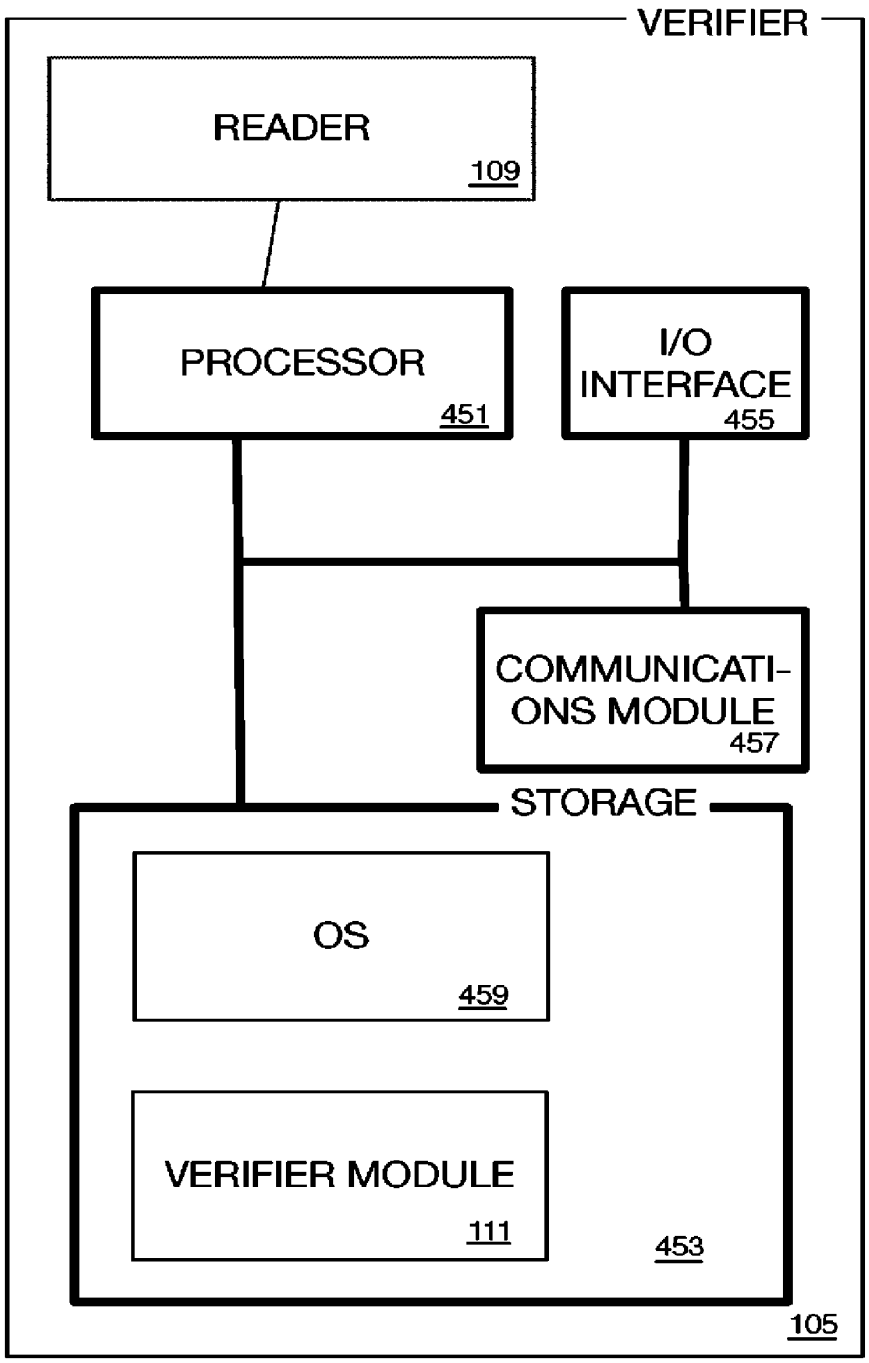

VERIFIER
READER
109
PROCESSOR
451
I/O
INTERFACE
455
COMMUNICATI-
ONS MODULE
457
STORAGE
OS
459
VERIFIER MODULE
111
453
105

Fig. 5

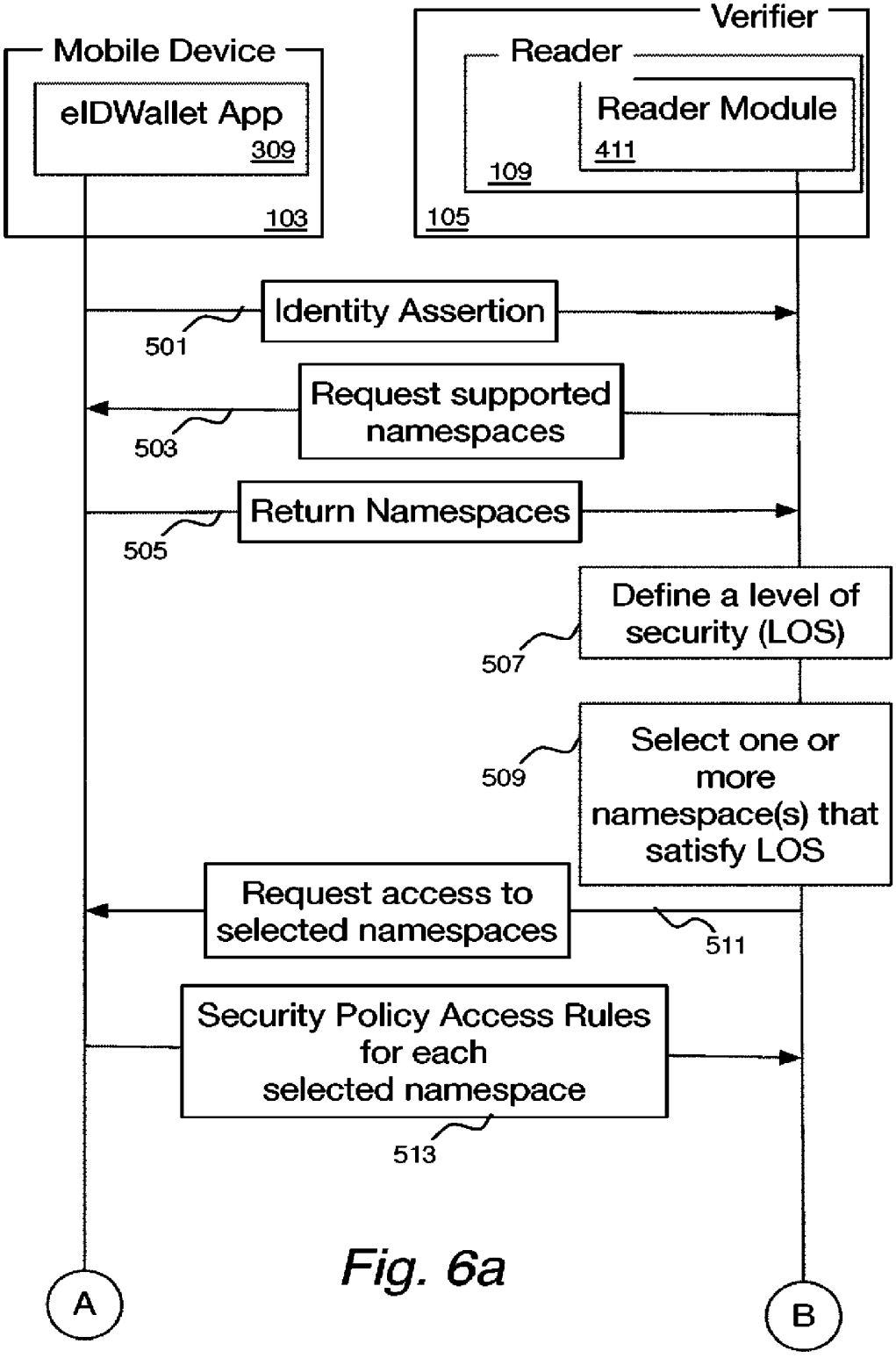

Mobile Device
eIDWallet App
309
103
Verifier
Reader
Reader Module
411
109
105
Identity Assertion
501
Request supported namespaces
503
Return Namespaces
505
Define a level of security (LOS)
507
Select one or more namespace(s) that satisfy LOS
509
Request access to selected namespaces
511
Security Policy Access Rules for each selected namespace
513
A
B

Fig. 6a

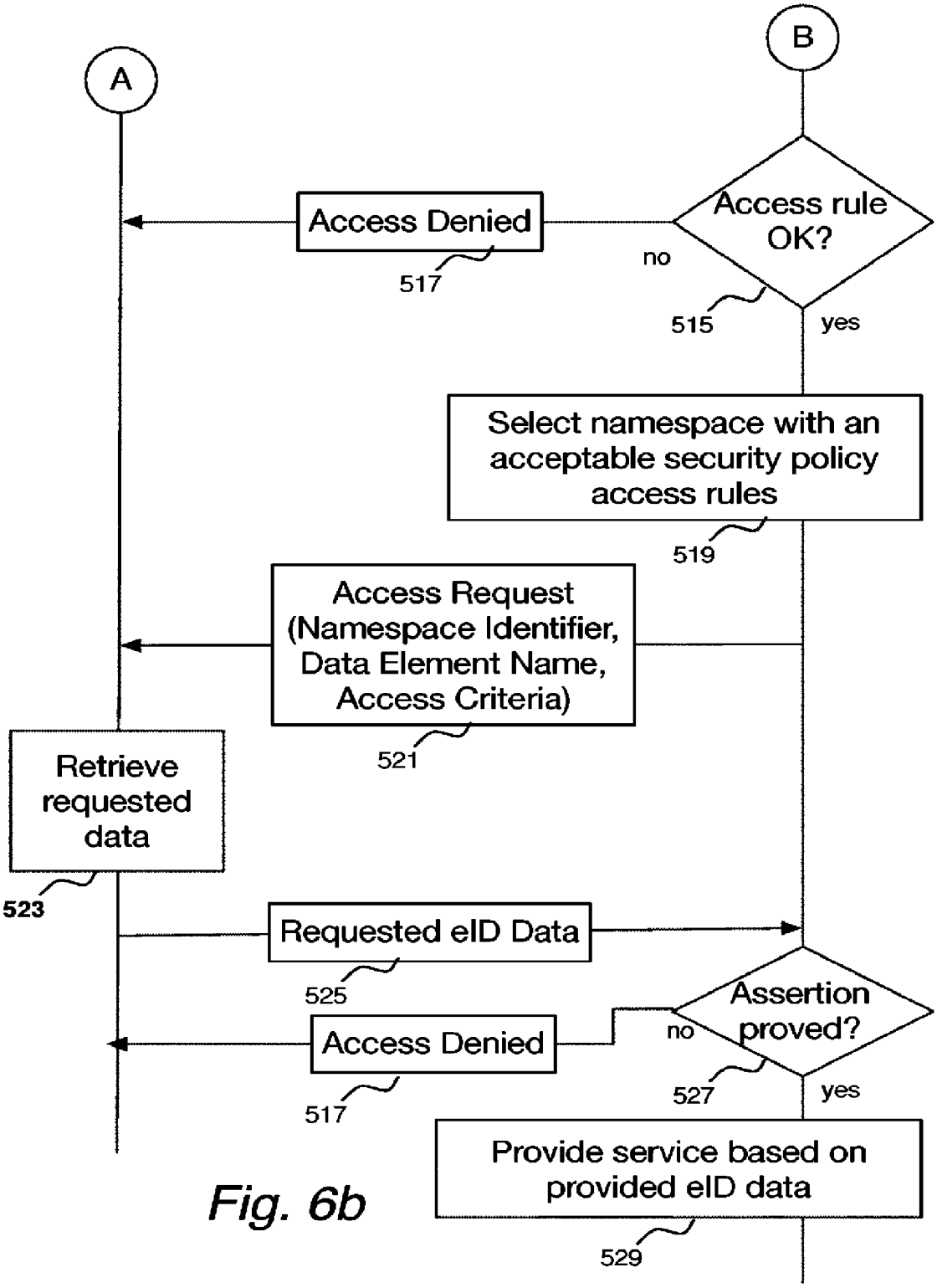

A
B
Access Denied
517
Access rule OK?
no
515
yes
Select namespace with an acceptable security policy access rules
519
Access Request (Namespace Identifier, Data Element Name, Access Criteria)
521
Retrieve requested data
523
Requested eID Data
525
Assertion proved?
no
Access Denied
517
527
yes
Provide service based on provided eID data
529

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

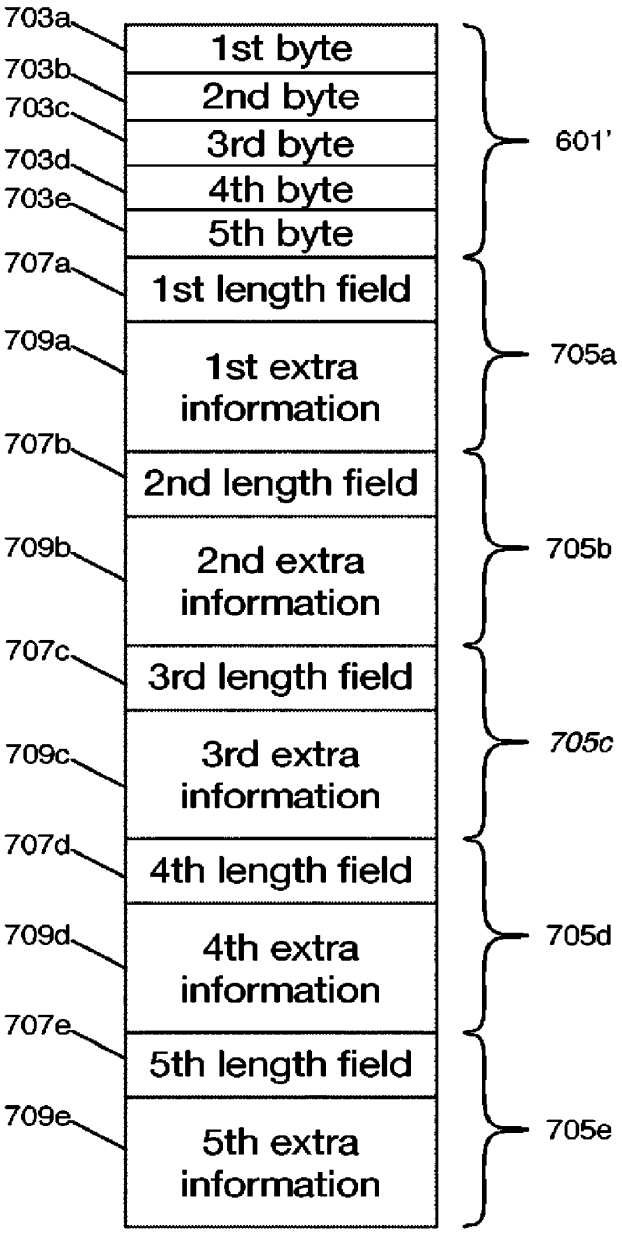

703a
1st byte
703b
2nd byte
703c
3rd byte
703d
4th byte
703e
5th byte
601'
707a
1st length field
709a
1st extra information
705a
707b
2nd length field
709b
2nd extra information
705b
707c
3rd length field
709c
3rd extra information
705c
707d
4th length field
709d
4th extra information
705d
707e
5th length field
709e
5th extra information
705e

Fig. 8

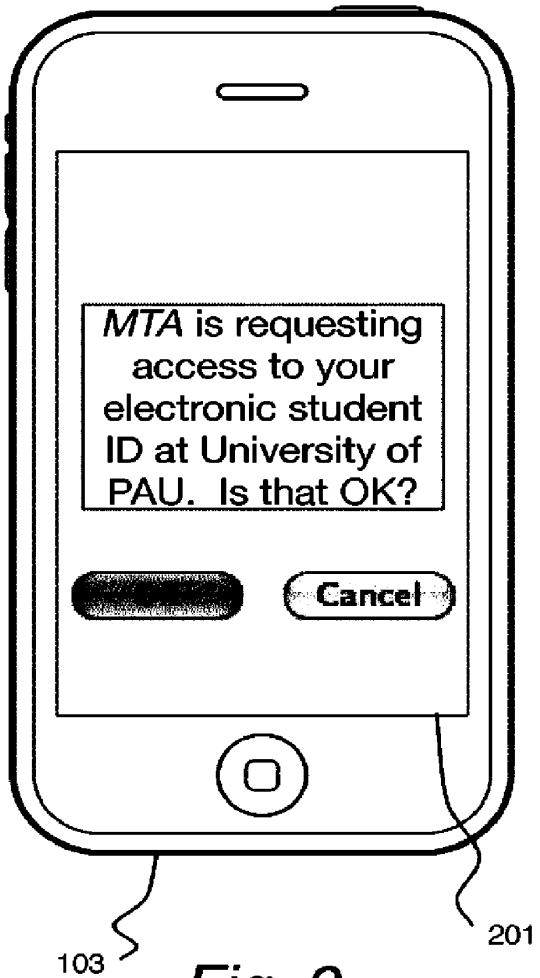

MTA is requesting access to your electronic student ID at University of PAU. Is that OK?
Cancel
103
201

Fig. 9

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 *(day/month/year)*
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 *(day/month/year)*
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 Searching Authority
☐ the Authority(ies) specified for supplementary search
☐ the International Preliminary Examining Authority
☒ the designated Offices concerned
☐ 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

CA 03154428 2022-4-11

Form PCT/IB/306 (revised January 2020) I/UFXDGK9CPUZQX0

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING SUBMISSION, OBTENTION OR TRANSMITTAL OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

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

Date of mailing *(day/month/year)* 02 October 2020 (02.10.2020)	
Applicant's or agent's file reference GMT4110 WO/YL	**IMPORTANT NOTIFICATION**
International application No. PCT/EP2020/076906	International filing date *(day/month/year)* 25 September 2020 (25.09.2020)
International publication date *(day/month/year)* **Not yet published**	Priority date *(day/month/year)* 18 October 2019 (18.10.2019)
Applicant THALES DIS FRANCE SA	

The applicant is hereby notified of the date of receipt (or of obtaining by the International Bureau) of the priority document(s) relating to all earlier application(s) whose priority is claimed. Unless otherwise indicated by the letters "NR", in the right-hand column or by an asterisk appearing next to the date of receipt, **the priority document concerned was submitted or transmitted to or obtained by the International Bureau in compliance with Rule 17.1(a), (b) or (b-*bis*)**. This Form replaces any previously issued notification concerning submission, transmittal or obtaining of priority documents.

Priority date	Priority application No.	Country or regional Office or PCT receiving Office	Date of receipt of priority document
18 October 2019 (18.10.2019)	19306357.5	EP	30 September 2020 (30.09.2020)

The letters "NR" denote a priority document which, on the date of mailing of this Form, had not yet been received or obtained by the International Bureau in compliance with Rule 17.1(a), (b) or (b-*bis*). Where the applicant has failed to either submit, request to prepare and transmit, or to request the International Bureau to obtain the priority document within the applicable time limit under that Rule, the attention of the applicant is directed to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

An asterisk "*" next to a date of receipt, denotes a priority document submitted or transmitted to or obtained by the International Bureau but not in compliance with Rule 17.1(a), (b) or (b-*bis*) (the priority document was received after the time limit prescribed in Rule 17.1(a); the request to prepare and transmit the priority document was submitted to the receiving Office after the applicable time limit under Rule 17.1(b) or the request to the International Bureau to obtain the priority document was made after the applicable time limit under Rule 17.1(b-*bis*)). Even though the priority document was not furnished in compliance with Rule 17.1(a), (b) or (b-*bis*), the International Bureau will nevertheless transmit a copy of the document to the designated Offices, for their consideration. In case such a copy is not accepted by the designated Office as the priority document, Rule 17.1(c) provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Authorized officer
Nora Lindner
e-mail pct.team5@wipo.int
Telephone No. +41 22 338 74 05

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)
EPO-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

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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	Date of mailing of the international search report
12 November 2020	20/11/2020

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Nicoli, Félix

1

Form PCT/ISA/210 (second sheet) (April 2005)

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

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

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

Form PCT/ISA/210 (patent family annex) (April 2005)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 April 2021 (22.04.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/073853 A1

(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

(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.

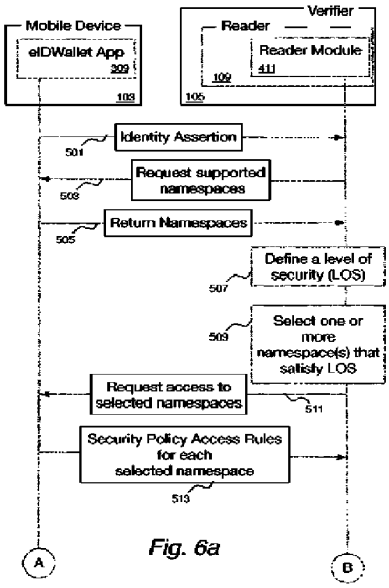


Fig. 6a

WO 2021/073853 A1

ROBIC

COMMISSIONER OF PATENTS
GATINEAU, QUEBEC, K1A 0C9

Montreal, April 11, 2022

Our File: 014211-0023

REQUEST FOR ENTRY INTO NATIONAL PHASE IN CANADA

Commissioner:

Please enter the Canadian national phase of International Patent Application **PCT/EP2020/076906** in the name of **THALES DIS FRANCE SAS** according to the following particulars:

Documents and relevant information

Copy of front page(s) of international publication is(are) enclosed:	[ ]
Certified copy(ies) of the priority application(s) is(are) enclosed:	[ ] [#]
Copy(ies) of the priority application(s) is(are) available at the IB: **DAS Code:**_____	**[X]**
Translation of international patent application specification is enclosed:	[ ]
Form(s) IB/306 is(are) enclosed:	[ ] [#]
Statement of entitlement is enclosed:	**[X]**
Declaration of entitlement is available at the IB (Rule 4.17(ii) *Regulations under the PCT*):	[ ]
Related document is enclosed (Section 124 of the *Patent Rules*):	[ ]
Document(s) evidencing a name change is(are) enclosed (Section 125 of the *Patent Rules*)	[ ] [#]
Document(s) evidencing a transfer is(are) enclosed (Section 126 of the *Patent Rules*)	[ ] [#]
Applicant(s) claim(s) the small entity (Subsection 44(2) of the *Patent Rules*) and a Declaration is enclosed:	[ ]
Sequence listing in .txt form is enclosed:	[ ]
Examination is requested under Subsection 35(1) of the *Patent Act*:	**[X]**

[ ] The common representative is:
[ ] The reinstatement of rights for late national phase entry is requested and the applicant(s) confirm(s) that the failure to request the national phase entry before the deadline of 30 months was unintentional.
[ ] A new filing certificate is requested.

Instructions and remarks

Only boxes **[ ]** that are marked with " **X** " are to be considered.

All correspondence for the present patent application is to be sent by email to **opic.brevets@robic.com**. CIPO may still send original documents such as patents by mail.

ROBIC, L.L.P.
www.robic.ca
info@robic.com

MONTREAL
630 René-Lévesque Boulevard West
20th Floor
Montreal, Quebec, Canada H3B 1S6
Tel.: +1 514 987-6242 Fax: +1 514 845-7874

QUEBEC
Le Delta Building
2875 Laurier Boulevard, Delta 3 - suite 700
Quebec, Quebec, Canada G1V 2M2
Tel.: +1 418 653-1888 Fax.: +1 418 653-0006

Fee(s)

Please charge to our designated credit card the following prescribed fee(s):

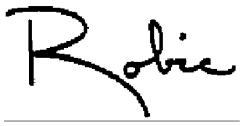
Basic national fee:	$407.18
Registration fee(s):	
Maintenance fee(s):	
Fee for reinstatement:	
Examination fee:	$814.37
Total fee(s):	**$1221.55**

Should the amount(s) indicated in this letter be insufficient to cover all of the fee(s) for which payment(s) is(are) explicitly or implicitly requested by this letter, or should a fee payment cannot be charged to the designated credit card, CIPO is hereby **unconditionally, clearly and unequivocally authorized** to debit any amount required to pay or complete any applicable fee from our deposit account **600000233**.

The applicant(s) accordingly hereby request(s) commencement of national phase procedures consequent to the designation of Canada in the present international application and request(s) that a patent for the invention described and claimed therein be granted.

The applicant(s) hereby appoint(s) the agents of ROBIC, 630 René-Lévesque Boulevard West – 20th Floor, Montréal, Québec, Canada, H3B 1S6, as its(their) patent agents at the Patent Office.

Respectfully submitted,



ROBIC S.E.N.C.R.L. / LLP
Avocats, agents de brevets et de marques de commerce /
Lawyers, Patent and Trademark Agents

Agent(e) de brevets / Patent Agent: Julien FLEURANCE

STATEMENT OF ENTITLEMENT

Applicant(s): **THALES DIS FRANCE SAS**
Inventor(s): **FAHER, Mourad; and, BAYLE, Carole**
Entry into the national phase in Canada of **PCT/EP2020/076906** application
O/Ref.: **014211-0023**

[**X**] The applicant or the applicants is(are) entitled to apply for a patent.

[ ] The applicant is the sole inventor of the subject-matter of the invention for which an exclusive privilege or property is claimed or the applicants are the sole inventors of that subject-matter.

ROBIC S.E.N.C.R.L. / LLP
Avocats, agents de brevets et de marques de commerce /
Lawyers, Patent and Trademark Agents

Agent(e) de brevets / Patent Agent: Julien FLEURANCE

Date: April 11, 2022

Only box [ ] that is marked with "X" is to be considered.

Date Submitted: 2022/04/11

CA App. No.: 3154428

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, of 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 filed 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.

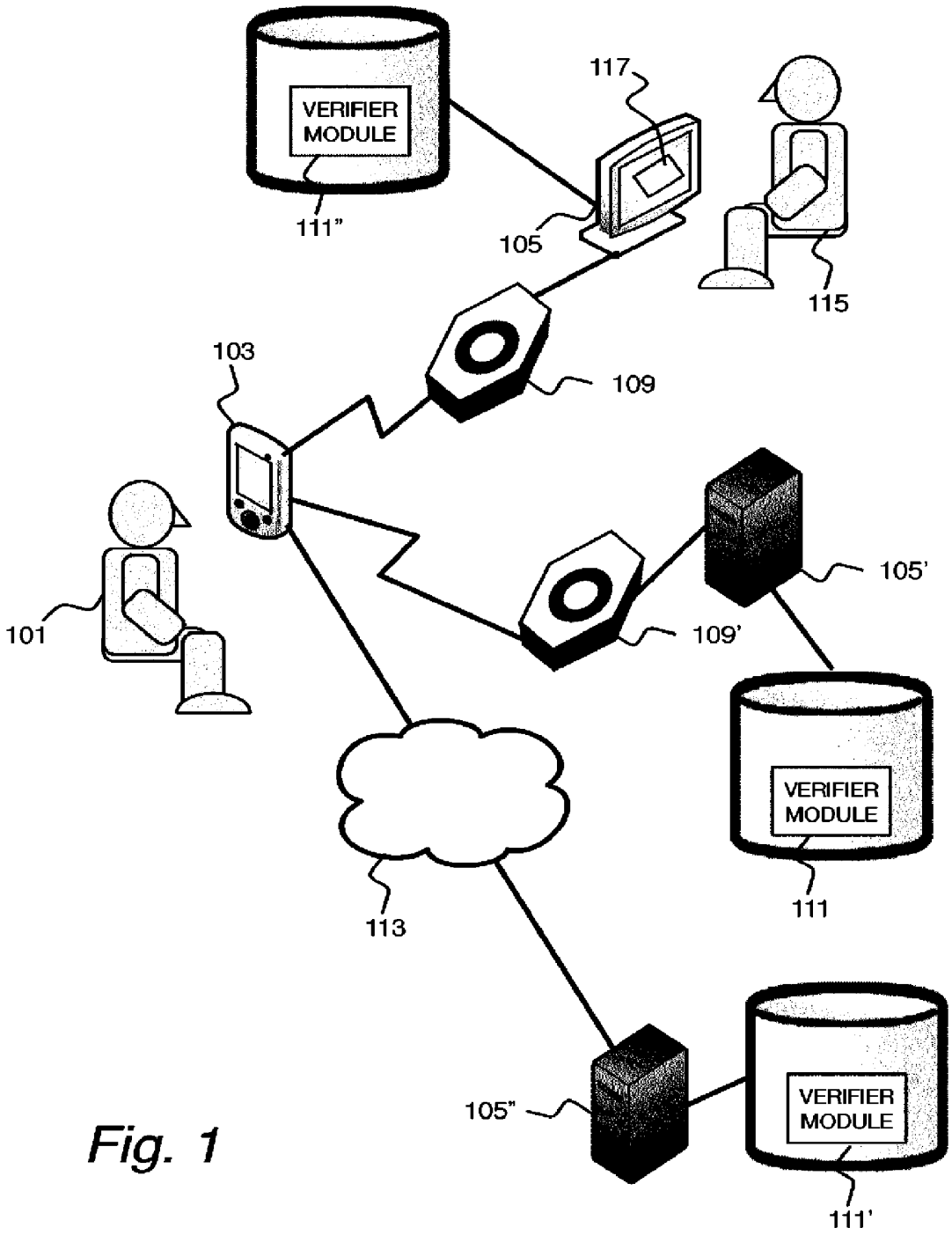

VERIFIER MODULE
111"
117
105
115
103
109
101
105'
109'
VERIFIER MODULE
111
113
105"
VERIFIER MODULE
111'

Fig. 1

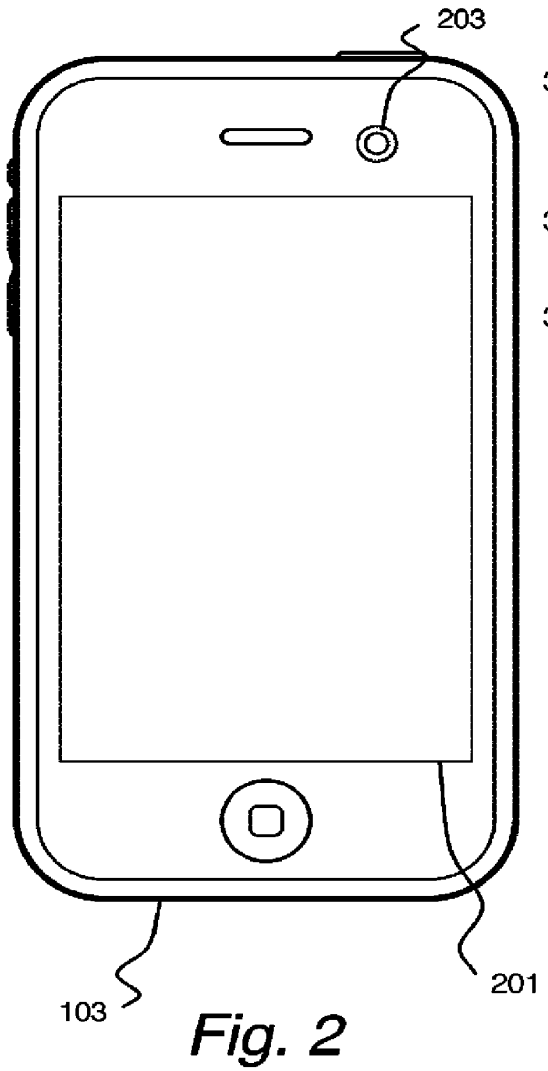

203
103
201

Fig. 2

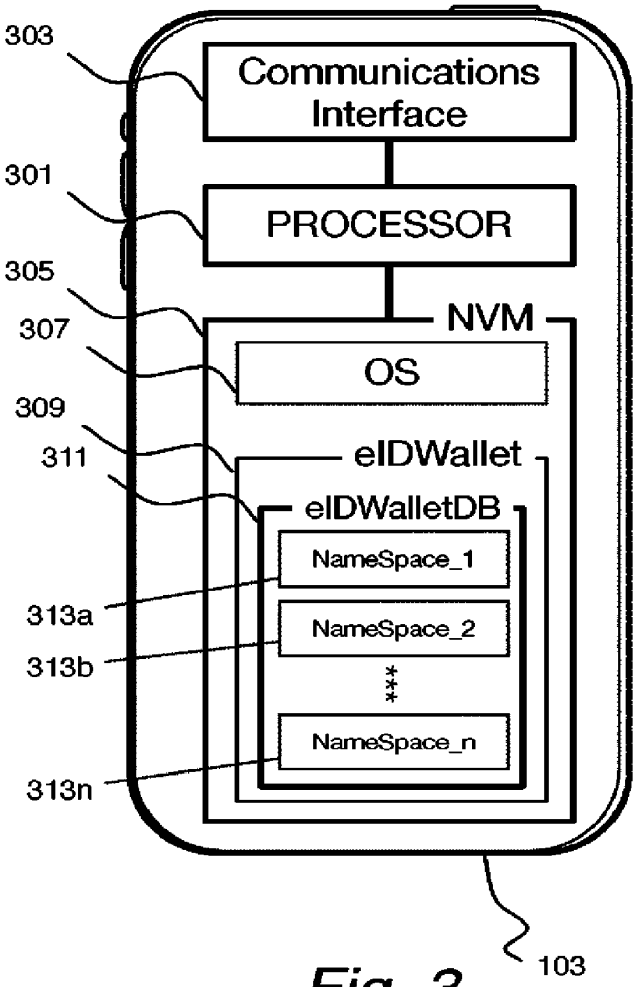

303
Communications Interface
301
PROCESSOR
305
NVM
307
OS
309
311
eIDWallet
eIDWalletDB
NameSpace_1
313a
NameSpace_2
313b
NameSpace_n
313n
103

Fig. 3

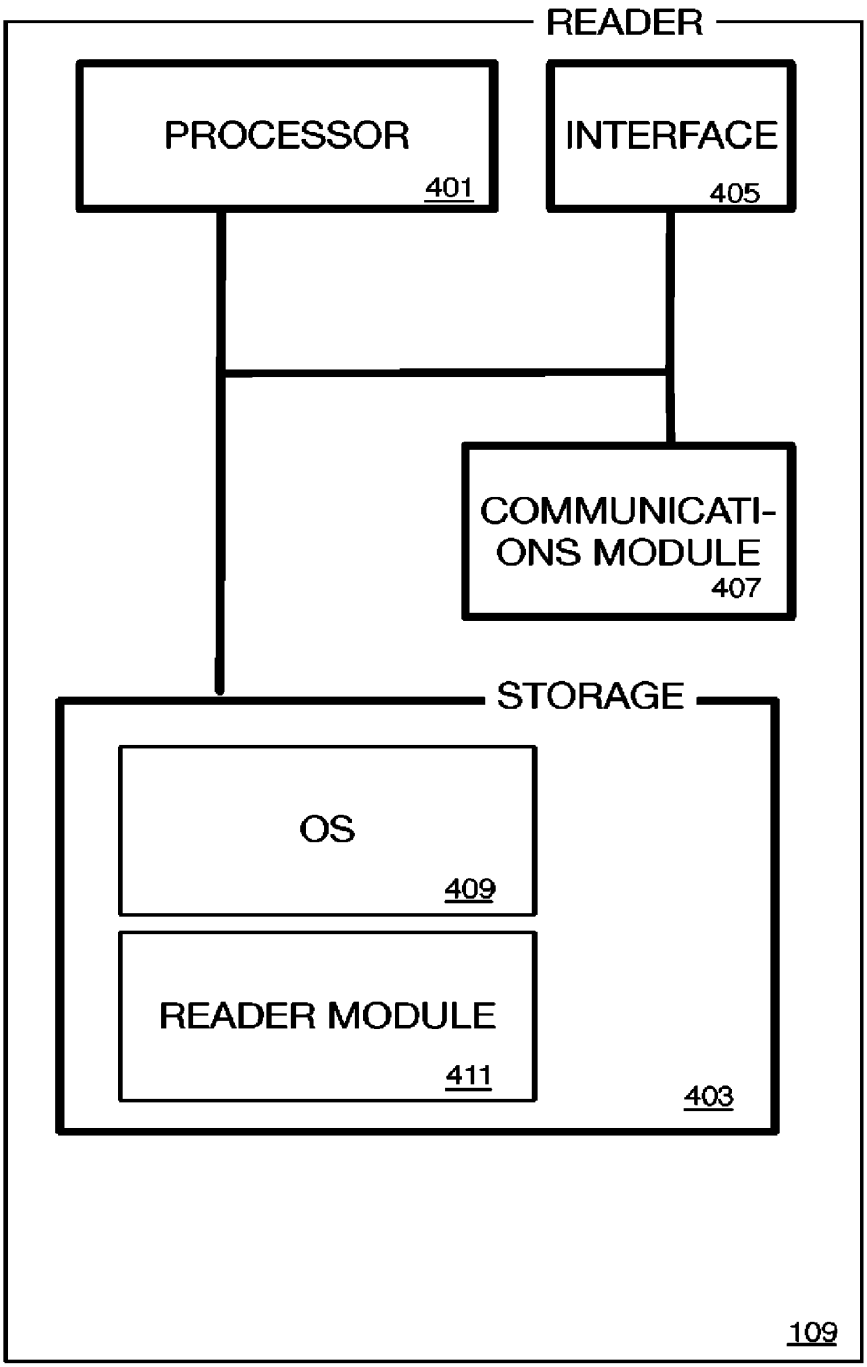

READER
PROCESSOR
401
INTERFACE
405
COMMUNICATI-
ONS MODULE
407
STORAGE
OS
409
READER MODULE
411
403
109

Fig. 4

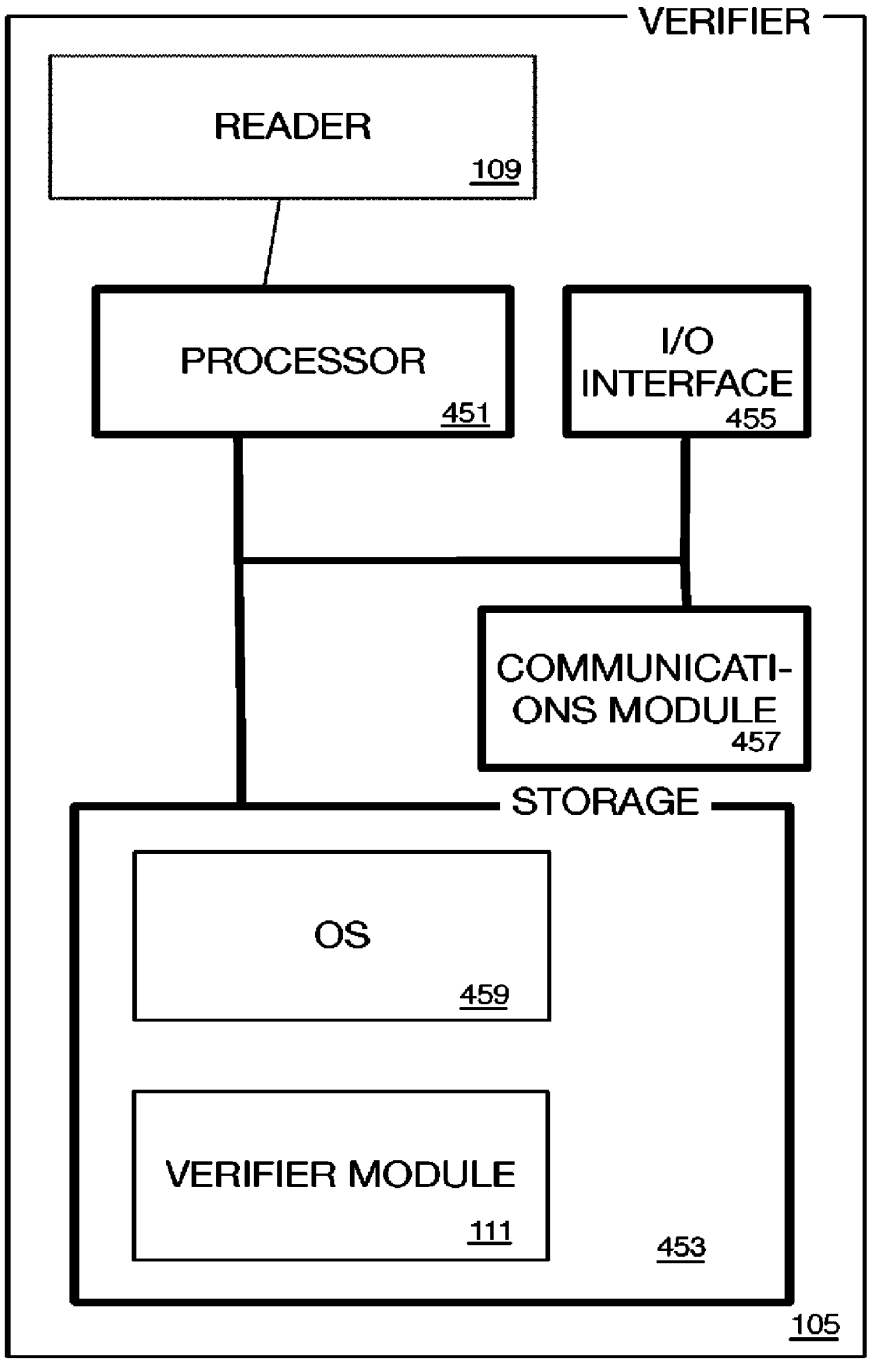

VERIFIER
READER
109
PROCESSOR
451
I/O
INTERFACE
455
COMMUNICATI-
ONS MODULE
457
STORAGE
OS
459
VERIFIER MODULE
111
453
105

Fig. 5

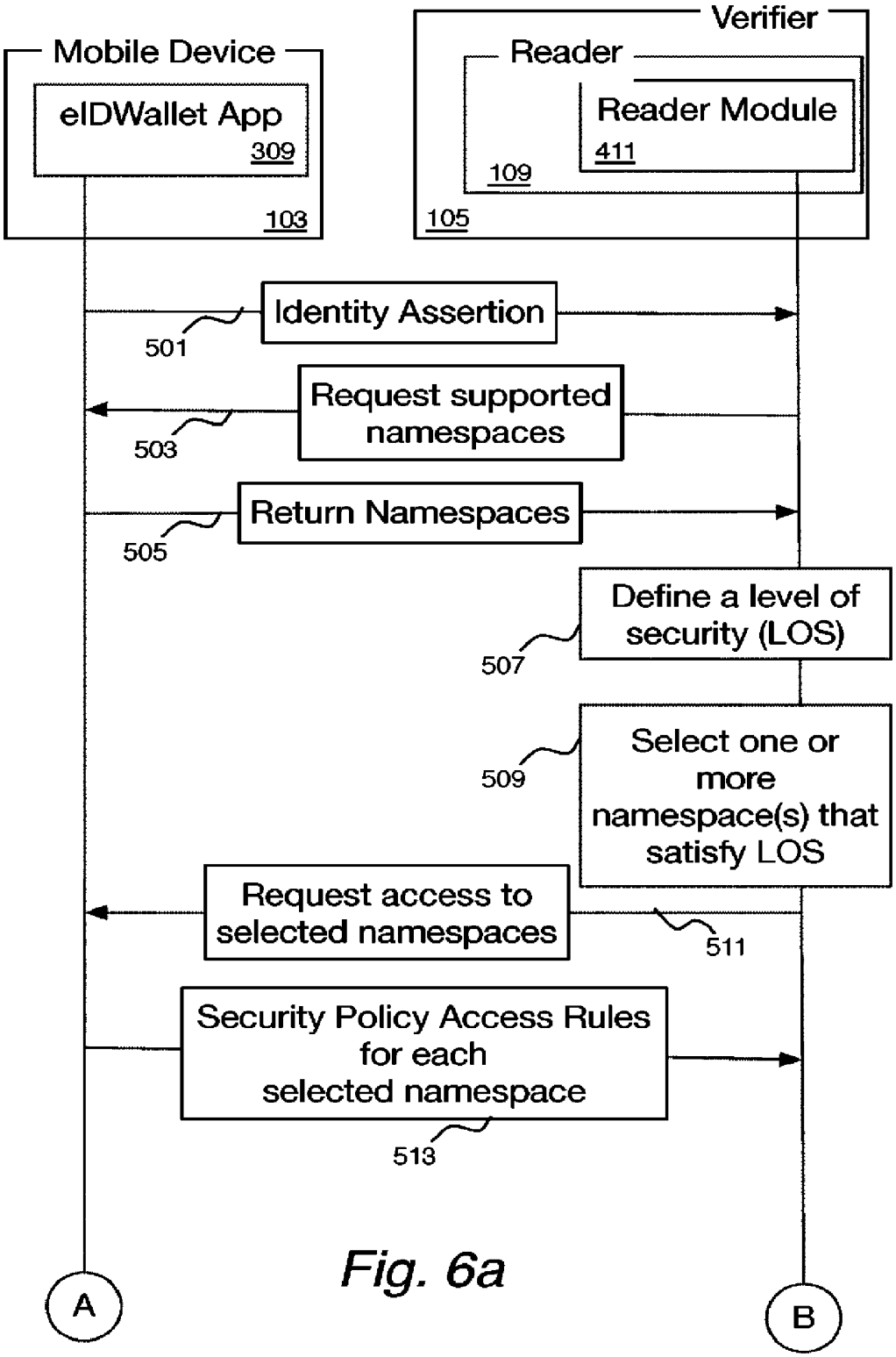

Mobile Device
eIDWallet App
309
103
Verifier
Reader
Reader Module
411
109
105
Identity Assertion
501
Request supported namespaces
503
Return Namespaces
505
Define a level of security (LOS)
507
Select one or more namespace(s) that satisfy LOS
509
Request access to selected namespaces
511
Security Policy Access Rules for each selected namespace
513
A
B

Fig. 6a

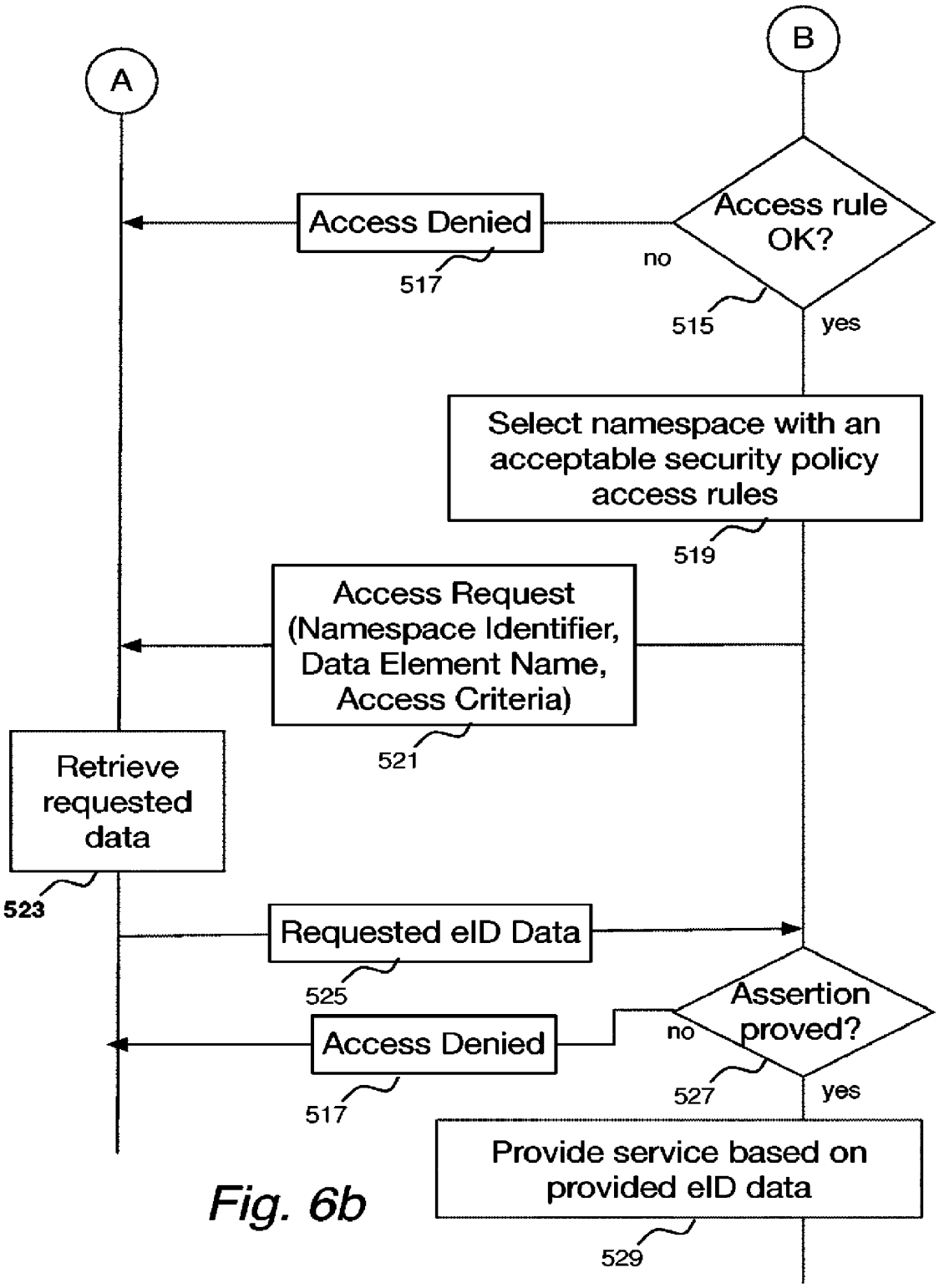

A
B
Access Denied
517
Access rule OK?
no
515
yes
Select namespace with an acceptable security policy access rules
519
Access Request (Namespace Identifier, Data Element Name, Access Criteria)
521
Retrieve requested data
523
Requested eID Data
525
Assertion proved?
no
Access Denied
517
527
yes
Provide service based on provided eID data
529

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

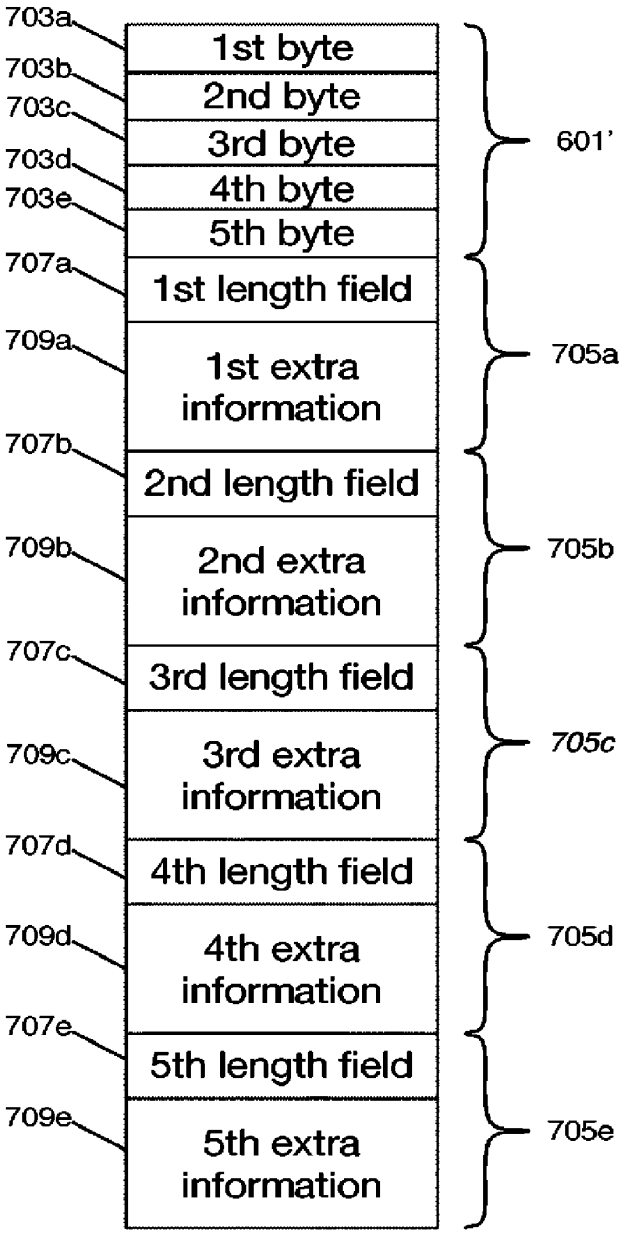

703a
1st byte
703b
2nd byte
703c
3rd byte
703d
4th byte
703e
5th byte
601'
707a
1st length field
709a
1st extra information
705a
707b
2nd length field
709b
2nd extra information
705b
707c
3rd length field
709c
3rd extra information
705c
707d
4th length field
709d
4th extra information
705d
707e
5th length field
709e
5th extra information
705e

Fig. 8

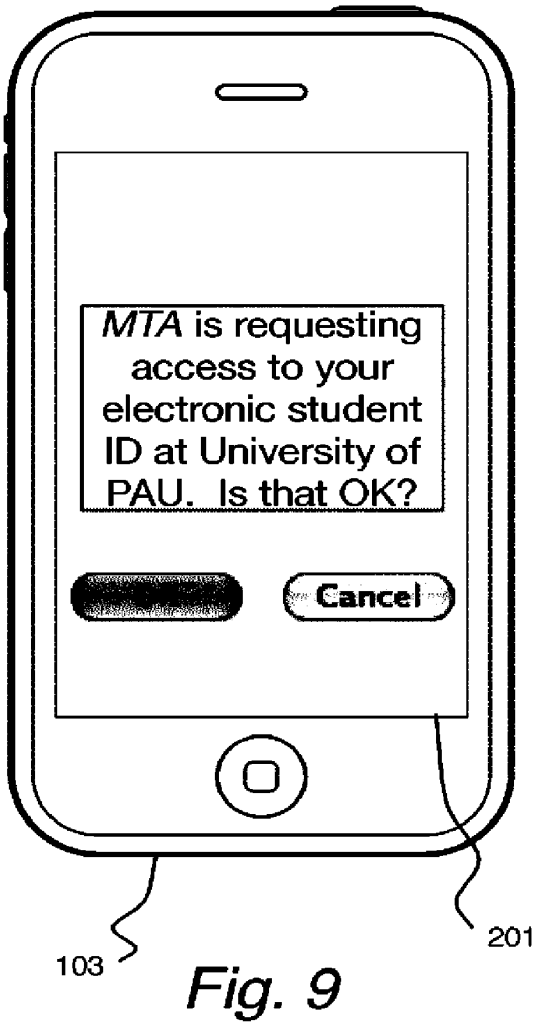
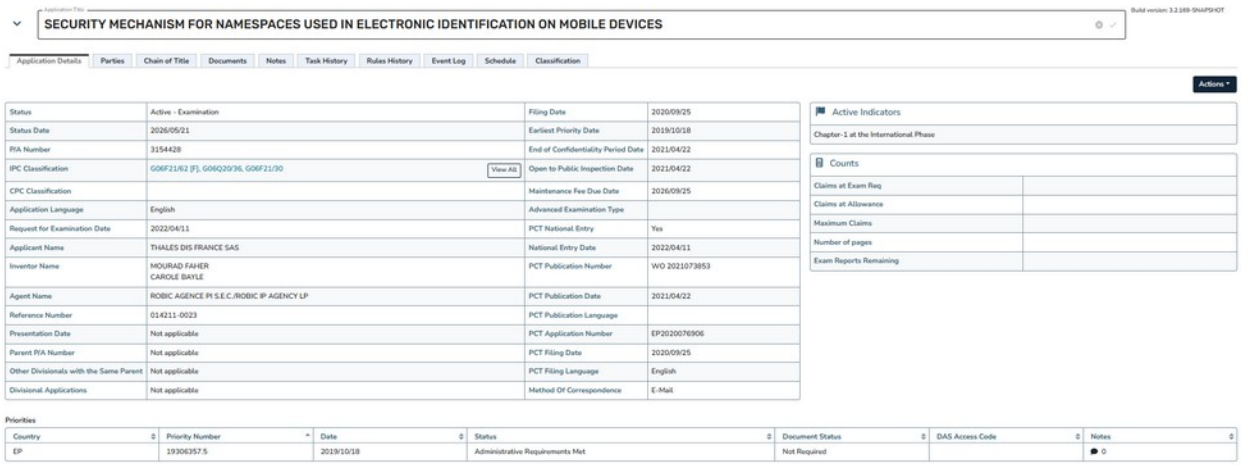

MTA is requesting access to your electronic student ID at University of PAU. Is that OK?
Cancel
103
201

Fig. 9



SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Application Details | Parties | Chain of Title | Documents | Notes | Task History | Rules History | Event Log | Schedule | Classification

Actions

Status	Active - Examination	Filing Date	2020/09/25
Status Date	2026/05/21	Earliest Priority Date	2019/10/18
PIA Number	3154428	End of Confidentiality Period Date	2021/04/22
IPC Classification	G06F21/62 [F], G06Q20/36, G06F21/30 View All	Open to Public Inspection Date	2021/04/22
CPC Classification		Maintenance Fee Due Date	2026/09/25
Application Language	English	Advanced Examination Type	
Request for Examination Date	2022/04/11	PCT National Entry	Yes
Applicant Name	THALES DIS FRANCE SAS	National Entry Date	2022/04/11
Inventor Name	MOURAD FAHER CAROLE BAYLE	PCT Publication Number	WO 2021073853
Agent Name	ROBIC AGENCE PI S.E.C./ROBIC IP AGENCY LP	PCT Publication Date	2021/04/22
Reference Number	014211-0023	PCT Publication Language	
Presentation Date	Not applicable	PCT Application Number	EP2020076906
Parent P/A Number	Not applicable	PCT Filing Date	2020/09/25
Other Divisionals with the Same Parent	Not applicable	PCT Filing Language	English
Divisional Applications	Not applicable	Method Of Correspondence	E-Mail

Active Indicators

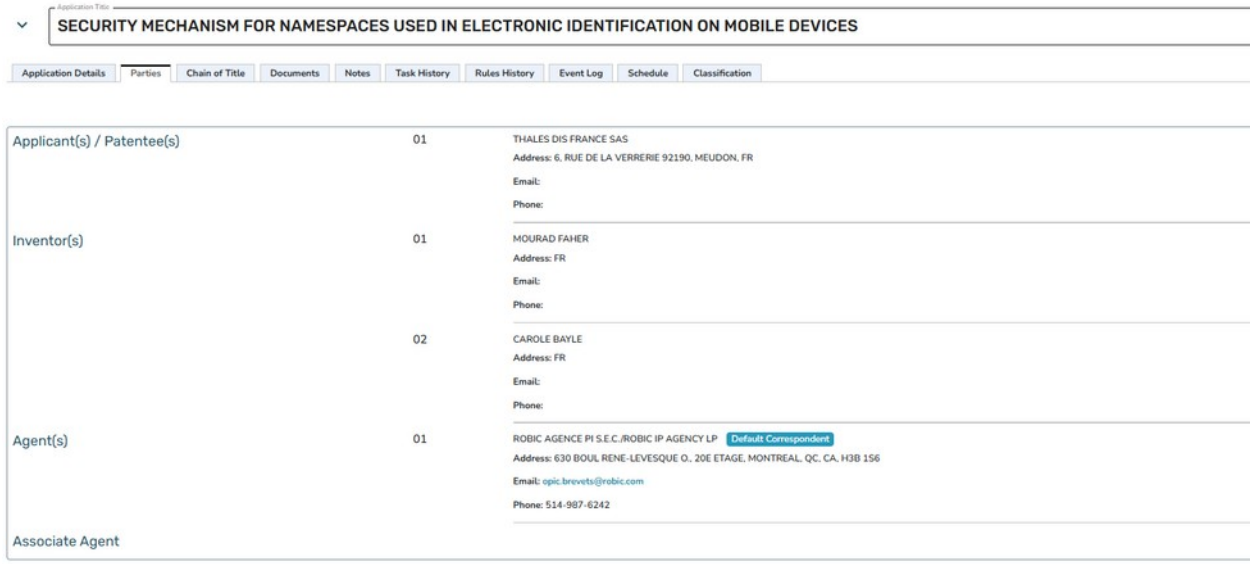
Chapter-1 at the International Phase

Counts

Claims at Exam Req	
Claims at Allowance	
Maximum Claims	
Number of pages	
Exam Reports Remaining	

Priorities

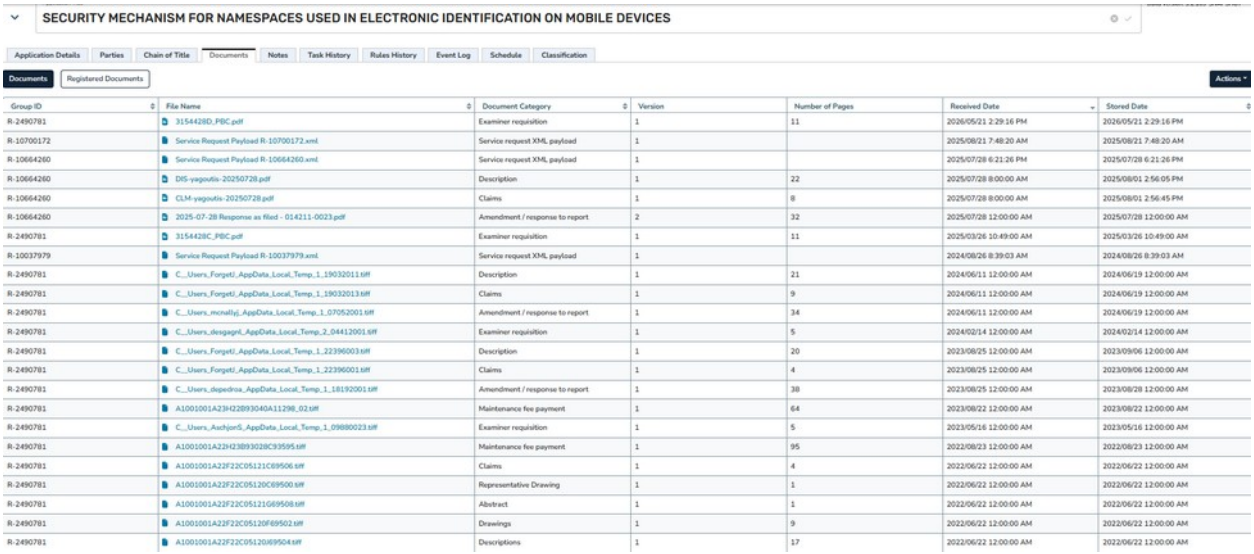
Country	Priority Number	Date	Status	Document Status	DAS Access Code	Notes
EP	19306357.5	2019/10/18	Administrative Requirements Met	Not Required		0



SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Application Details | Parties | Chain of Title | Documents | Notes | Task History | Rules History | Event Log | Schedule | Classification

Applicant(s) / Patentee(s)	01	THALES DIS FRANCE SAS **Address:** 6, RUE DE LA VERRERIE 92190, MEUDON, FR **Email:** **Phone:**
Inventor(s)	01	MOURAD FAHER **Address:** FR **Email:** **Phone:**
	02	CAROLE BAYLE **Address:** FR **Email:** **Phone:**
Agent(s)	01	ROBIC AGENCE PI S.E.C./ROBIC IP AGENCY LP Default Correspondent **Address:** 630 BOUL RENE-LEVESQUE O., 20E ETAGE, MONTREAL, QC, CA, H3B 1S6 **Email:** opic.brevets@robic.com **Phone:** 514-987-6242
Associate Agent		



SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Application Details | Parties | Chain of Title | Documents | Notes | Task History | Rules History | Event Log | Schedule | Classification

Documents | Registered Documents

Actions

Group ID	File Name	Document Category	Version	Number of Pages	Received Date	Stored Date
R-2490781	3154428D_PBC.pdf	Examiner requisition	1	11	2026/05/21 2:29:16 PM	2026/05/21 2:29:16 PM
R-10700172	Service Request Payload R-10700172.xml	Service request XML payload	1		2025/08/21 7:48:20 AM	2025/08/21 7:48:20 AM
R-10664260	Service Request Payload R-10664260.xml	Service request XML payload	1		2025/07/28 6:21:26 PM	2025/07/28 6:21:26 PM
R-10664260	DIS-yagoutis-20250728.pdf	Description	1	22	2025/07/28 8:00:00 AM	2025/08/01 2:56:05 PM
R-10664260	CLM-yagoutis-20250728.pdf	Claims	1	8	2025/07/28 8:00:00 AM	2025/08/01 2:56:45 PM
R-10664260	2025-07-28 Response as filed - 014211-0023.pdf	Amendment / response to report	2	32	2025/07/28 12:00:00 AM	2025/07/28 12:00:00 AM
R-2490781	3154428C_PBC.pdf	Examiner requisition	1	11	2025/03/26 10:49:00 AM	2025/03/26 10:49:00 AM
R-10037979	Service Request Payload R-10037979.xml	Service request XML payload	1		2024/08/26 8:39:03 AM	2024/08/26 8:39:03 AM
R-2490781	C__Users_ForgetJ_AppData_Local_Temp_1_19032011.tiff	Description	1	21	2024/06/11 12:00:00 AM	2024/06/19 12:00:00 AM
R-2490781	C__Users_ForgetJ_AppData_Local_Temp_1_19032013.tiff	Claims	1	9	2024/06/11 12:00:00 AM	2024/06/19 12:00:00 AM
R-2490781	C__Users_mcnallyj_AppData_Local_Temp_1_07052001.tiff	Amendment / response to report	1	34	2024/06/11 12:00:00 AM	2024/06/19 12:00:00 AM
R-2490781	C__Users_desgagnl_AppData_Local_Temp_2_04412001.tiff	Examiner requisition	1	5	2024/02/14 12:00:00 AM	2024/02/14 12:00:00 AM
R-2490781	C__Users_ForgetJ_AppData_Local_Temp_1_22396003.tiff	Description	1	20	2023/08/25 12:00:00 AM	2023/09/06 12:00:00 AM
R-2490781	C__Users_ForgetJ_AppData_Local_Temp_1_22396001.tiff	Claims	1	4	2023/08/25 12:00:00 AM	2023/09/06 12:00:00 AM
R-2490781	C__Users_depedroa_AppData_Local_Temp_1_18192001.tiff	Amendment / response to report	1	38	2023/08/25 12:00:00 AM	2023/08/28 12:00:00 AM
R-2490781	A1001001A23H22B93040A11298_02.tiff	Maintenance fee payment	1	64	2023/08/22 12:00:00 AM	2023/08/22 12:00:00 AM
R-2490781	C__Users_AuchjonS_AppData_Local_Temp_1_09880023.tiff	Examiner requisition	1	5	2023/05/16 12:00:00 AM	2023/05/16 12:00:00 AM
R-2490781	A1001001A22H23B93028C93595.tiff	Maintenance fee payment	1	95	2022/08/23 12:00:00 AM	2022/08/23 12:00:00 AM
R-2490781	A1001001A22F22C05121C69506.tiff	Claims	1	4	2022/06/22 12:00:00 AM	2022/06/22 12:00:00 AM
R-2490781	A1001001A22F22C05120C69500.tiff	Representative Drawing	1	1	2022/06/22 12:00:00 AM	2022/06/22 12:00:00 AM
R-2490781	A1001001A22F22C05121G69508.tiff	Abstract	1	1	2022/06/22 12:00:00 AM	2022/06/22 12:00:00 AM
R-2490781	A1001001A22F22C05120F69502.tiff	Drawings	1	9	2022/06/22 12:00:00 AM	2022/06/22 12:00:00 AM
R-2490781	A1001001A22F22C05120J69504.tiff	Descriptions	1	17	2022/06/22 12:00:00 AM	2022/06/22 12:00:00 AM

R-2490781	A1001001A22F14B91137D94660.tiff	Cover Page	1	1	2022/06/14 12:00:00 AM	2022/06/14 12:00:00 AM
R-2490781	A1001001A22F14B30034B92771.tiff	Cover Page	1	1	2022/06/14 12:00:00 AM	2022/06/14 12:00:00 AM
R-2490781	3154428_177.pdf	Courtesy - Acknowledgement of Request for Examination	1	1	2022/05/23 8:00:00 PM	2022/05/23 8:00:00 PM
R-2490781	C__Users_beaucham_AppData_Local_Temp_2_16180003.tiff	Sensitive information document	1	147	2022/04/27 12:00:00 AM	2022/05/13 12:00:00 AM
R-2490781	C__Users_beaucham_AppData_Local_Temp_2_16180001.tiff	Amendment / response to report	1	5	2022/04/27 12:00:00 AM	2022/05/13 12:00:00 AM
R-2490781	C__Users_pachecad_AppData_Local_Temp_1_16308004.tiff	Change to the Method of Correspondence	1	3	2022/04/27 12:00:00 AM	2022/05/11 12:00:00 AM
R-2490781	A1001001A22D11B45448G84801.tiff	Abstract	1	1	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B45401J84773.tiff	Drawings	1	9	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B45355C84771.tiff	Claims	1	4	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B45351G84769.tiff	Description	1	17	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B45337A84763.tiff	Representative drawing	1	1	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B45442A84795.tiff	Courtesy - Letter Acknowledging PCT National Phase Entry	1	2	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B45447D84799.tiff	National entry request	1	9	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B45438I84791.tiff	PCT nat. entry written opinion chpt. I	1	8	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B45433C84787.tiff	Priority request - PCT	1	35	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B45406G84779.tiff	Patent cooperation treaty (PCT)	1	1	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B4540BC84781.tiff	Patent cooperation treaty (PCT)	1	1	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B45405B84775.tiff	International search report	1	3	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B45338I84765.tiff	Patent cooperation treaty (PCT)	1	1	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B45334F84759.tiff	National entry request	1	2	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM
R-2490781	A1001001A22D11B45335F84761.tiff	Declaration of entitlement	1	1	2022/04/11 12:00:00 AM	2022/04/11 12:00:00 AM

Application Title

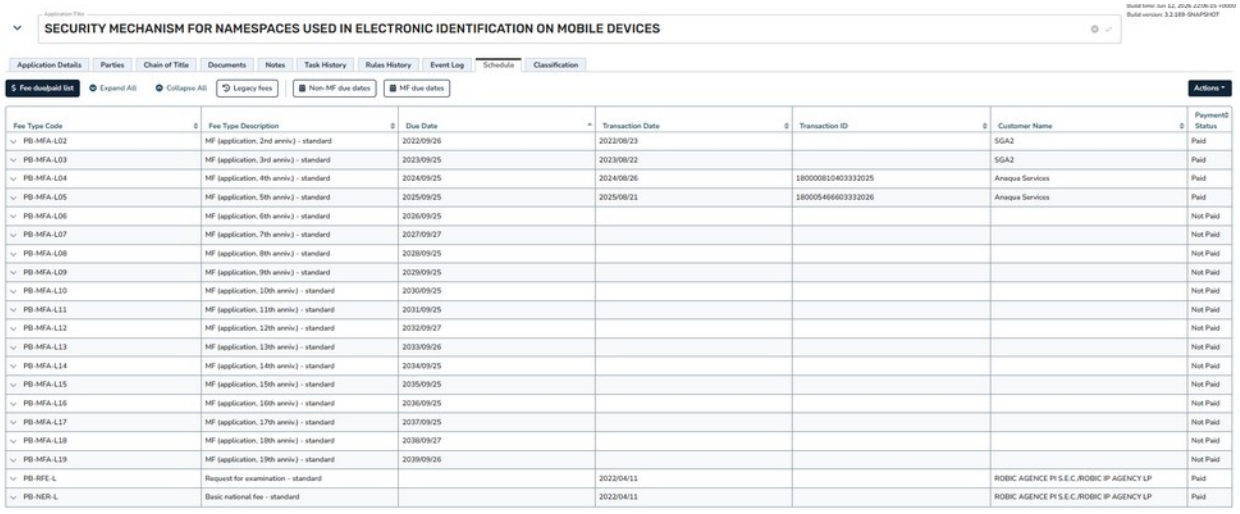
SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Build version: 3.2.169-SNAPSHOT

Application Details | Parties | Chain of Title | Documents | Notes | Task History | Rules History | Event Log | Schedule | Classification

Actions

Event Date	Code	Event Description	Status Event Code (state + stage + event)	Supplementary Event Data	Error (Yes/No)	Select
2021/04/22	SC130	Application Published (Open to Public Inspection)	A-2-2-Q10-Q12-xxx-X000		No	
2022/04/11	SC391	Request for Examination Requirements Determined Compliant	A-1-2-D10-D00-xxx-D118		No	
2022/04/11	SC151	Letter sent	A-1-1-W10-W00-xxx-W100	Courtesy - Letter Acknowledging PCT National Phase Entry	No	
2022/04/11	SC165	Priority Claim Requirements Determined Compliant	A-1-1-P10-P18-xxx-P105		No	
2022/04/11	SC102	Application Received - PCT	A-0-1-A10-A00-xxx-A101		No	
2022/04/11	SC104	National Entry Requirements Determined Compliant	A-1-1-A10-A15-xxx-X000		No	
2022/04/11	SCL074	Archived Event: IPC assigned	A-1-1-W00-W00-uns-W128		No	
2022/04/11	SCL074	Archived Event: IPC assigned	A-1-1-W00-W00-uns-W128		No	
2022/04/11	SCL074	Archived Event: IPC assigned	A-1-1-W00-W00-uns-W128		No	
2022/04/11	SC164	Request for Priority Received	A-1-1-P10-P18-xxx-P104		No	
2022/04/11	SC258	All Requirements for Examination Determined Compliant	A-1-2-D10-D11-xxx-D155		No	
2022/04/13	SCL005	Archived Event: First IPC assigned	A-1-1-W00-W00-uns-W005		No	
2022/04/27	SC213	Change of Address or Method of Correspondence Request Received	A-1-1-R10-R00-xxx-R113		No	
2022/04/27	SC159	Amendment Received - Voluntary Amendment	A-1-1-P10-P11-xxx-P101		No	
2022/05/24	SCL069	Archived Event: Applicant deleted	A-1-1-W00-W00-uns-W120		Yes	
2022/05/24	SC392	Letter Sent	A-2-2-W10-W00-xxx-W100	Acknowledgement of Request for Examination	No	
2022/06/07	SCL239	Archived Event: Submission of Prior Art	A-2-2-W00-W00-uns-W523		No	
2022/06/14	SCL277	Archived Event: Cover page published	A-2-2-W00-W00-uns-W160		No	
2023/04/27	SCL158	Archived Event: Report - No QC	A-2-2-W00-W00-uns-W290		No	
2023/05/16	SC327	Examiner's Report	A-2-2-D10-D15-xxx-D126	Examiner's Report #1	No	
2023/08/25	SC158	Amendment Received - Response to Examiner's Requisition	A-2-2-P10-P11-xxx-P100		No	
2023/08/25	SC159	Amendment Received - Voluntary Amendment	A-2-2-P10-P11-xxx-P101		No	
2023/12/31	SCL075	Archived Event: IPC removed	A-2-2-W00-W00-uns-W129		No	
2024/01/01	SCL122	Archived Event: IPC expired	A-2-2-W00-W00-uns-W210		No	
2024/01/24	SCL005	Archived Event: First IPC assigned	A-2-2-W00-W00-uns-W005		No	
2024/01/24	SCL074	Archived Event: IPC assigned	A-2-2-W00-W00-uns-W128		No	
2024/01/24	SCL074	Archived Event: IPC assigned	A-2-2-W00-W00-uns-W128		No	
2024/01/24	SCL075	Archived Event: IPC removed	A-2-2-W00-W00-uns-W129		No	
2024/02/13	SCL158	Archived Event: Report - No QC	A-2-2-W00-W00-uns-W290		No	
2024/02/14	SC328	Examiner's Report	A-2-2-D10-D15-xxx-D126	Examiner's Report #2	No	
2024/06/11	SC158	Amendment Received - Response to Examiner's Requisition	A-2-2-P10-P11-xxx-P100		No	
2024/06/11	SC159	Amendment Received - Voluntary Amendment	A-2-2-P10-P11-xxx-P101		No	
2024/08/26	SC318	Maintenance Request Received	A-2-2-U10-U00-xxx-U101		No	
2024/08/26	SC319	Maintenance Fee Payment Paid In Full	A-2-2-U10-U11-xxx-U102		No	
2025/03/26	SC329	Examiner's Report	A-2-2-D10-D15-xxx-D126	Examiner's Report #3	No	
2025/07/28	SC158	Amendment Received - Response to Examiner's Requisition	A-2-2-P10-P11-xxx-P100		No	
2025/07/31	SC363	Correspondent Determined Compliant	A-2-2-W10-W00-xxx-W111		No	
2025/08/01	SC160	Amendment Determined Compliant	A-2-2-P10-P11-xxx-P102		No	
2025/08/01	SC161	Application Amended	A-2-2-P10-P13-xxx-X000		No	
2025/08/21	SC318	Maintenance Request Received	A-2-2-U10-U00-xxx-U101		No	
2025/08/21	SC319	Maintenance Fee Payment Paid In Full	A-2-2-U10-U11-xxx-U102		No	
2026/05/21	SC330	Examiner's Report	A-2-2-D10-D15-xxx-D126	Examiner's Report #4	No	



SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Application Details | Parties | Chain of Title | Documents | Notes | Task History | Rules History | Event Log | Schedule | Classification

$ Fee due/paid list | Expand All | Collapse All | Legacy fees | Non-MF due dates | MF due dates | Actions

Fee Type Code	Fee Type Description	Due Date	Transaction Date	Transaction ID	Customer Name	Payment Status
PB-MFA-L02	MF (application, 2nd anniv.) - standard	2022/09/26	2022/08/23		SGA2	Paid
PB-MFA-L03	MF (application, 3rd anniv.) - standard	2023/09/25	2023/08/22		SGA2	Paid
PB-MFA-L04	MF (application, 4th anniv.) - standard	2024/09/25	2024/08/26	1800008104033332025	Anaqua Services	Paid
PB-MFA-L05	MF (application, 5th anniv.) - standard	2025/09/25	2025/08/21	1800054666033332026	Anaqua Services	Paid
PB-MFA-L06	MF (application, 6th anniv.) - standard	2026/09/25				Not Paid
PB-MFA-L07	MF (application, 7th anniv.) - standard	2027/09/27				Not Paid
PB-MFA-L08	MF (application, 8th anniv.) - standard	2028/09/25				Not Paid
PB-MFA-L09	MF (application, 9th anniv.) - standard	2029/09/25				Not Paid
PB-MFA-L10	MF (application, 10th anniv.) - standard	2030/09/25				Not Paid
PB-MFA-L11	MF (application, 11th anniv.) - standard	2031/09/25				Not Paid
PB-MFA-L12	MF (application, 12th anniv.) - standard	2032/09/27				Not Paid
PB-MFA-L13	MF (application, 13th anniv.) - standard	2033/09/26				Not Paid
PB-MFA-L14	MF (application, 14th anniv.) - standard	2034/09/25				Not Paid
PB-MFA-L15	MF (application, 15th anniv.) - standard	2035/09/25				Not Paid
PB-MFA-L16	MF (application, 16th anniv.) - standard	2036/09/25				Not Paid
PB-MFA-L17	MF (application, 17th anniv.) - standard	2037/09/25				Not Paid
PB-MFA-L18	MF (application, 18th anniv.) - standard	2038/09/27				Not Paid
PB-MFA-L19	MF (application, 19th anniv.) - standard	2039/09/26				Not Paid
PB-RFE-L	Request for examination - standard		2022/04/11		ROBIC AGENCE PI S.E.C./ROBIC IP AGENCY LP	Paid
PB-NER-L	Basic national fee - standard		2022/04/11		ROBIC AGENCE PI S.E.C./ROBIC IP AGENCY LP	Paid

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

Application Details | Parties | Chain of Title | Documents | Notes | Task History | Rules History | Event Log | Schedule | Classification

$ Fee due/paid list | Expand All | Collapse All | Legacy fees | Non-MF due dates | MF due dates | Actions

Fee Type	Anniversary #	Entry Type	New Fee Type	Due Date	Due Amount	Paid Date	Paid Amount	Status Type	Paid With MRUID
RFE	1	Large	PB-RFE-L		814.37	2022/04/11	814.37	paid	10144197
FIL	1	Large	PB-NER-L		407.18	2022/04/11	407.18	paid	10144197
MAN	2	Large	PB-MFA-L02	2022/09/26	100	2022/08/23	100	paid	10516627
MAN	3	Large	PB-MFA-L03	2023/09/25	100	2023/08/22	100	paid	15837373

CIPO File No.	Client File No.	Ref	Description	User	Amount($)	Ind
3154428		No	TM (demande, 5e anniv.) - générale	strategis	289.19	
3154428		No	TM (demande, 4e anniv.) - générale	strategis	125.00	
3154428	014211-0023	No	SECURITY MECHANISM FOR NAMESPACES U ▶	strategis	100.00	
3154428	014211-0023	No	SECURITY MECHANISM FOR NAMESPACES U ▶	strategis	100.00	
					614.19	