



Acknowledgement of receipt

We hereby acknowledge receipt of the following subsequently filed document(s):

Submission number	15017032	
Application number	EP20775659.4	
Date of receipt	21 January 2026	
Filing Office	European Patent Office, The Hague	
Procedural phase	All procedures	
Your reference	GMT4110EPT LS	
Documents submitted	package-data.xml epf1038.pdf (1 p.) CLMS-HWA-1.pdfGMT4110 - new claims without marks_.pdf (4 p.)	ep-sfd-request.xml CLMS-1.pdfGMT4110 - new claims with marks.pdf (4 p.) EPLETT-1.pdfGMT4110EPT Response to 94. 3.pdf (5 p.)
Submitted by	CN=secure.epoline.org	
Method of submission	Online	
Date and time receipt generated	21 January 2026, 16:25 (CET)	
Message Digest	24:72:0E:DD:F6:A4:03:D3:BE:E3:2E:A9:6F:44:92:E7:F7:1E:BF:A5	

/European Patent Office/

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; wherein each security policy specifies technical authentication requirements that must be satisfied by a reader before granting access to data in the corresponding namespace. 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, wherein the reader evaluates its technical capabilities against the authentication requirements specified in each security policy to determine which namespaces it can access.

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 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 ~~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 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 memrequired 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 memverifier 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
 5 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:
 10 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;~~
- 15 - in response to receiving the list of selected namespaces from the reader, evaluating technical authentication capabilities required for each selected namespace; 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.~~
- 20 - wherein the security rules specify technical parameters including required authentication protocols, hash types, signature schemes, and secure messaging options that the reader must implement to access data in the namespace.

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;
 30 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
 35 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.

5

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.

10

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

15

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;

20

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:

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 the verifier terminal can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the mobile device;

30

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.

35

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; wherein each security policy specifies technical authentication requirements that must be satisfied by a reader before granting access to data in the corresponding namespace, 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, wherein the reader evaluates its technical capabilities against the authentication requirements specified in each security policy to determine which namespaces it can access.

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 according to any previous claims, 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 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 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 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 according to any previous claims wherein memrequired authentication may be selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.

8. The 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 memverifier associates with each namespace in the plurality of supported namespaces.

9. The method 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 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 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, evaluating technical authentication capabilities required for each selected namespace; 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,

wherein the security rules specify technical parameters including required authentication protocols, hash types, signature schemes, and secure messaging options that the reader must implement to access data in the namespace.

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 according to any previous claim 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.



Letter accompanying subsequently filed items

Representative:
Luc SCHEER
THALES DIS FRANCE SAS
ZONE ATHELIA IV / Avenue du Jujubier
13705 FRANCE LA CIOTAT
France

Phone: 0442365373
E-mail: intellectual.property2@thalesgroup.com

80298 Munich
Germany
Tel. +49(0)89 2399-0

P.O. Box 5818
2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040

10958 Berlin
Germany
Tel. +49(0)30 25901-0

The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

Application number:

EP20775659.4

Applicant's or representative's reference

GMT4110EPT LS

Name of represented party

/Luc SCHEER/

	Description of document	Original file name	Assigned file name
1	Amended claims (clean copy)	GMT4110 - new claims with marks.pdf	CLMS-1.pdf
2	Amended claims with annotations	GMT4110 - new claims without marks_.pdf	CLMS-HWA-1.pdf
3	Letter relating to the search or examination procedure	GMT4110EPT Response to 94. 3.pdf	EPLETT-1.pdf

Signatures

Place: La Ciotat
Date: 21 January 2026
Signed by: /Luc Scheer/

Representative name: Luc SCHEER
Capacity: Representative
Function of person signing: Representative

Thales Digital France SAS
6, rue de la Verrerie
92197, Meudon Cedex
France
T: +33 (0) 1 55 01 50 00
www.thalesgroup.com

European Patent Office
80298 MUNICH
GERMANY

Ref.: Patent application 20 775 659.4

Our ref.: GMT4110 EPT - LS

Object: Answer to the communication according to Article 94(3)

La Ciotat, January 21 2026

Dear Sirs,

In answer to the communication in object dated October 30 2025, the Applicant presents hereunder his response to the Office Action and files a new set of claims.

I. AMENDMENTS TO THE CLAIMS

Claim 1 is amended as follows:

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, **wherein each security policy specifies technical authentication requirements that must be satisfied by a reader before granting access to data in the corresponding namespace**; 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, **wherein the reader evaluates its technical capabilities against the authentication requirements specified in each security policy to determine which namespaces it can access.**

Claim 11 is amended as follows:

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, evaluating technical authentication capabilities required for each selected namespace;** and
 - transmitting security rules associated with each selected namespace according to a defined bytestring template, **wherein the security rules specify technical parameters including required authentication protocols, hash types, signature schemes, and secure messaging options that the reader must implement to access data in the namespace.**

The other claims have been also amended for clarity purposes.

II. ARGUMENTS UNDER ARTICLE 56 EPC

A. Closest Prior Art and Problem-Solution Approach

The examiner correctly identifies D1 as the closest prior art, which discloses a digital wallet application containing multiple digital identification documents (driver's license, military ID, student ID, passport) and a system where a reader can request access to these documents.

However, the examiner's analysis fails to properly identify the distinguishing features and their technical effects.

B. Distinguishing Features and Technical Effects

Step 1: Distinguishing Features

The key distinguishing features of amended claim 1 over D1 are:

1. **Security policies associated with namespaces:** D1 does not disclose security policies associated with namespaces, and the examiner

acknowledges it is "not defined how the reader is aware of the security policies associated with namespaces" and "what may be the use of security policies".

2. **Technical authentication requirements specification:** The claimed security policies specify concrete technical requirements (authentication protocols, hash types, signature schemes) that readers must satisfy.
3. **Reader capability evaluation:** The reader evaluates its technical capabilities against these requirements to determine namespace accessibility.

Step 2: Technical Effects

Contrary to the examiner's assertion that "an actual technical effect of the differentiating feature is not apparent", these features provide clear technical effects:

1. **Automated compatibility assessment:** As described in the application (paragraphs 6, 61), security rules specify "technical information which has to be provided to the wallet by the reader in order to grant access to a data item in a namespace" and enable "selection of a rule specifying technical data which can be provided in view of the capability of the reader".
2. **Prevention of failed authentication attempts:** By communicating technical requirements upfront, the system prevents readers from attempting to access namespaces they cannot technically support.
3. **Optimized namespace selection:** The system enables selection based on "overhead of satisfying the rule for providing the required information", allowing readers to choose the most efficient namespace they can technically support.

Step 3: Objective Technical Problem

The objective technical problem is: "How to enable a reader to automatically determine which identity namespaces it can technically access based on its authentication capabilities, thereby avoiding failed access attempts and optimizing namespace selection."

C. Obviousness Analysis

The examiner suggests that "associated policies are generic policies also locally known from the requester for predefined kinds of EIDs" and that "selection of namespaces according to locally stored policies would be obvious". This analysis is flawed for several reasons:

1. **No motivation in prior art:** D1 provides no suggestion for communicating technical authentication requirements between mobile devices and readers. D1 only discloses that "the request may include the identity of the individual, company, or system requesting the identification" and basic accept/deny functionality.

2. **Different technical approach:** The examiner acknowledges that "the protocol defining this principle would appear to be neither disclosed nor derivable from the available prior art (D1, §28), confirming the inventive nature of the claimed approach.
3. **Technical complexity:** The claimed system requires sophisticated technical coordination between mobile devices and readers regarding cryptographic capabilities, hash algorithms, and secure messaging protocols - far beyond the simple business rules suggested by the examiner.

D. Response to Dependent Claims Objections

Claims 2, 8, 9

The examiner dismisses these as "administrative steps" and "obvious". However, these claims provide technical effects:

- **Technical confidence assessment:** Confidence levels reflect the cryptographic strength and authentication rigor of different namespaces, enabling technical security decisions.
- **Automated filtering:** Whitelists/blacklists enable automated technical compatibility filtering based on supported cryptographic protocols.

Claims 3, 4

The examiner characterizes these as "mere matter of choice" and "non-technical choice". However:

- **Technical privacy control:** User filtering prevents exposure of sensitive namespace information, providing technical privacy protection.
- **System efficiency:** Filtering reduces communication overhead by transmitting only relevant namespace data.

Claim 5

The examiner finds this "obvious to implement", but the claim specifically relates to transmitting technical authentication requirements, not generic business rules.

III. CONCLUSION

The examiner acknowledges that "the protocol defining this principle would appear to be neither disclosed nor derivable from the available prior art and could lead to allowable independent claims" and suggests that "present claim 16 appears to be the most promising basis for defining such claims".

The amended claims now clearly define the technical protocol for communicating authentication requirements between mobile devices and readers, providing concrete technical effects that solve the identified technical problem. The skilled person would not have been motivated to develop this specific technical solution based on the available prior art.

We respectfully request that the examiner reconsiders the inventive step objection in light of these amendments and arguments and allow the application to proceed to grant.

Sincerely Yours,

Luc Scheer - 77380

Encl.: New set of claims

Datum
Date 30.10.2025
Date

Blatt
Sheet 1
Feuille

Anmelde-Nr:
Application No: 20 775 659.4
Demande n°:

The examination is being carried out on the **following application documents**

Description, Pages

1-17 as published

Claims, Numbers

1-16 filed in electronic form on 05-12-2022

Drawings, Sheets

1/9-9/9 as published

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)

EMVCO: "EMV '96 Integrated Circuit Card Application Specification for Payment Systems",
EMV, EMVCO

D4 vol. 3.1.1 ; Contact 1 July 2006 (2006-07-01), pages 1-62, XP061034511,
Retrieved from the Internet:
URL: https://www.emvco.com/wp-content/uploads/documents/Emvapp_20090126073328.pdf
[retrieved on 2020-01-06]

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 Claims 1-16 appear to be allowable under Article 123(2) EPC.
- 3 The subject-matter of claim 1 is not inventive in the sense of Article 56 EPC for the following reasons:
- 3.1 D1 discloses (with the exception of ~~struck-out~~ features):

A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising: (see fig.1, par.23 "The client device 102a 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")

associating security policies with each of a plurality of supported namespaces on a mobile device; and (see par.31; fig.2 the wallet owner may accept or deny a request)

operating a reader executing a reader module to communicate with the mobile device (see fig.2; par.27) and to select a namespace to access a data item stored on the mobile device (see par.28 "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")
~~based on the security policies associated with the plurality of supported namespaces on the mobile device.~~

- 3.2 D1 does not disclose:

based on the security policies associated with the plurality of supported namespaces on the mobile device

3.3 It is noted that it is not defined 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.

It is also noted that D1 discloses that it may be decided which eid to request (see par.28) but does not elaborate how such selection is performed.

In the present formulation, it may be considered that associated policies are 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 (see D1 par.31 which shows providing location information in order to access eid information from a client device). Selection of namespaces according to locally stored policies would be obvious to implement for the skilled person at the level defined in present claim 1.

3.4 Hence, claim 1 is not inventive, Article 56 EPC.

4 Dependent claims 2-4, 6-10 are not deemed to be inventive in the sense of Article 56 EPC for the following reasons:

4.1 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. Thus, claims 2, 8 and 9 are not inventive.

4.2 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.

4.3 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. D1 also discloses that a user may accept/deny transmission eid information (see fig.2). Thus, claim 4 is not inventive.

4.4 The subject-matter of claim 5 is understood as the transmission of business rules for selection purpose. This step would be obvious to implement for the skilled person. Claim 5 is not inventive.

4.5 D1 discloses user consent (see fig.2). Claim 7 is not inventive.

4.6 Claim 10 defines obvious implementation choices. Thus, claim 10 is not inventive.

5 The subject-matter of claim 11 is not inventive in the sense of Article 56 EPC for the following reasons:

5.1 D1 discloses (with the exception of ~~struck-out~~ features):

- 6 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: (see fig.1)
receive a list of selected namespaces from a reader; (see par.28)
~~in response to receiving the list of selected namespaces from the reader, (see par.28)
transmitting security rules associated with each selected namespace according to a defined bytestring template.~~
- 6.1 D1 does not disclose:
in response to ... transmitting security rules associated with each selected namespace according to a defined bytestring template
- 6.2 It is noted that it is not defined what may be done by the reader with the transmitted security rules it receives (the nature and purpose of the rules is not defined) such that a technical effect of the transmission step is not apparent.

The rules are undefined and may even be considered as business information provided to the reader for an unknown purpose. Such step would obvious to implement by the skilled person at the level of definition of claim 11.

Transmission of information as a bytestring template is a well-known in the context of transmitting information between a digital wallet and a reader. Such an implementation choice would be to implement by the skilled person.
- 6.3 Hence, claim 11 is not inventive, Article 56 EPC.
- 7 Dependent claims 12-14, 16 are not deemed to inventive in the sense of Article 56 EPC for the following reasons:
- 7.1 Claims 13-14, 16 are not inventive in the sense of Article 56 EPC for substantially the reasons raised against claims 1, 4-5.
- 7.2 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.
- 7.3 D1 shows that a verifier can verify an identity assertion and provide an answer such as yes/no (see), reader may provide information such location information as a business rule (see par.31) The step "determine for which of the candidate namespaces the reader can satisfy the security policy of the namespace", is interpreted in a broad manner as determining whether business

information may be provided to the reader; this is would obvious to implement for the skilled person. Reasons given for claims 1, and 11 also apply to present claim 16. Thus, claim 16 is not inventive.

8 In view of the arguments of the applicant in the letter received on 05.12.2022, it is noted that:

8.1 It is also noted that the concept of namespace used to characterize a family of information is a well-known principle. The use of such a principle for expressing user identity information cannot be deemed to be inventive, and identities defined in the wallet of D1 are deemed to be functionally equivalent.

8.2 The concept of level of security (LOS) appears to relate to a level of trust a verifier may have in specific IDs according to their source, for instance a national ID card may be preferred over a student ID card by a bank, this selection of an ID may even be performed by a human being (see par.44, 49-51 of the description). This concept appears to be an administrative requirement rather than a technical one and cannot contribute to an inventive step. This concept does not appear to be connected to the one of security rules. Moreover, this LOS concept is not defined in any of the independent claims.

9 When considering the application description, it is understood that security rules regard the technical information which has to be provided to the wallet by the reader in order to grant access to a data item in a namespace (see par.6, 61), and, selecting a namespace according to security rules regards the selection of a rule specifying technical data which can be provided in view of the capability of the reader or/and an overhead of satisfying the rule for providing the required information (see par.6, 12, 61).

It is noted that the protocol defining this principle would appear to be neither disclosed nor derivable from the available prior art and could lead to allowable independent claims which would clearly express this subject-matter. Present claim 16 appears to be the most promising basis for defining such claims; the subject-matter of claims 6 and 15 should also be taken into account while amending claims.



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication?
Contact Customer Services at
www.epo.org/contact



Quintero Romero, Manuel
Thales Dis France SAS
Intellectual Property Department
6, rue de la Verrerie
92190 Meudon
FRANCE

Application No. 20 775 659.4 - 1218	Ref. GMT4110-EPT/MQ	Date 30.10.2025
Applicant Thales Dis France SAS		

Communication pursuant to Article 94(3) EPC

The examination of the above-identified application has revealed that it does not meet the requirements of the European Patent Convention for the reasons enclosed herewith. If the deficiencies indicated are not rectified the application may be refused pursuant to Article 97(2) EPC.

You are invited to file your observations and insofar as the deficiencies are such as to be rectifiable, to correct the indicated deficiencies within a period

of 4 months

from the notification of this communication, this period being computed in accordance with Rules 126(2) and 131(2) and (4) EPC. One set of amendments to the description, claims and drawings is to be filed within the said period on separate sheets (R. 50(1) EPC).

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

In case you withdraw the application within the above-mentioned period, the examination fee will be refunded at a rate of 50% (Art. 11(b) RFees).

Failure to comply with this invitation in due time will result in the application being deemed to be withdrawn (Art. 94(4) EPC).

Registered Letter

EPO Form 2001 04.25AUWF (27.10.2025)



Nicoli, Felix
Primary Examiner
For the Examining Division

Enclosure(s): Applicants not using the Mailbox can access patent literature via Espacenet
5 page/s reasons (EPO Form 2906)



Application No.: 20775659.4

Substantive examination has started on 23.10.25 (see Notice from the European Patent Office dated 29.01.2013, OJ EPO 2013, 153).

For the Examining Division



Central Fee Payment –
Automatic debit order

Thank you for your automatic debit order submitted to the EPO on 16.10.2023 at 12:20 hrs (CET).

The automatic debit order will be effective as from 16.10.2023.

Deposit account:	28040233
Deposit account holder:	Thales Dis France SAS
Requested by:	Amelie Bricks
Procedure:	EP
Application No.:	20775659.4
Your reference:	GMT4110-EPT/MQ
Effective from:	16.10.2023

It has been recorded in the Central Fee Payment service that, under the arrangements for the automatic debiting procedure, any fees falling due in relation to the application shown above are to be debited automatically from deposit account 28040233 held with the European Patent Office.

The EPO will debit that deposit account in respect of all fees for which automatic debiting is allowed as they arise in respect of the proceedings specified in the automatic debit order in question, and treat them as paid in time, provided they fall due on or after the date of receipt of the order and that the deposit account concerned contains sufficient funds.



Central Fee Payment –

Revocation of automatic debit order

Thank you for your instruction to revoke the automatic debit order submitted to the EPO on 16.10.2023 at 12:16 hrs (CET).

The revocation will be effective as from 16.10.2023.

Deposit account:	28040183
Deposit account holder:	Thales Dis France SA
Requested by:	Amelie Bricks
Procedure:	EP
Application No.:	20775659.4
Reference:	GMT4110-EPT/MQ
Effective from:	16.10.2023



Acknowledgement of receipt

We hereby acknowledge receipt of the following subsequently filed document(s):

Submission number	11551885	
Application number	EP20775659.4	
Date of receipt	05 December 2022	
Filing Office	European Patent Office, The Hague	
Procedural phase	All procedures	
Your reference	GMT4110-EPT/MQ	
Documents submitted	<div>package-data.xml epf1038.pdf (1 p.) CLMS-HWA-1.pdf2-2. GMT4110 EPT_Amended claims_with annotations.pdf (4 p.)</div>	<div>ep-sfd-request.xml WOREPLY-1.pdf3-1. GMT4110 EPT_Response to R161&162 EPC as Filed.pdf (3 p.) CLMS-1.pdf2-3. GMT4110 EPT_Amended claims_clean copy.pdf (4 p.)</div>
Submitted by	CN=secure.epoline.org	
Method of submission	Online	
Date and time receipt generated	05 December 2022, 16:56 (CET)	
Message Digest	34:9F:93:67:05:96:C1:1B:AF:A9:0F:F5:D0:4D:B8:9E:08:69:7B:45	

/European Patent Office/

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 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 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 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 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 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 a 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 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;
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. 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:

- 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.

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 a~~ verifier module executing on ~~the 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 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 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 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 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 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 a~~ 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~~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;
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. TheA 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:

- 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.

Thales Digital Identity & Security
6, Rue de la Verrerie

92190 Meudon
France
T: +33 (0) 1 55 01 50 00
www.thalesgroup.com

EUROPEAN PATENT OFFICE

D-80298 MUNCHEN
ALLEMAGNE

Meudon, December 5, 2022

O/Ref.:

GMT4110 EPT/MQ

European Patent Application No.
Filed on
Owner

20775659.4 - 1213
25 Sep 2020
THALES DIS FRANCE SAS

Re: Communication pursuant to Rule R.161(1) & 162

Dear Madam, Dear Sir,

In response to the communication pursuant to Rules 161(2) and 162 EPC dated May 30, 2022 in connection with the above-mentioned European patent application, the Applicant hereby files the following:

1. Amendments

The dependency of claim 16 has been adapted to any of previous claims.

The missing antecedent basis for the terms listed in section 6.1 of the written opinion of the International Search Report (WO-ISR), have been corrected. Correction is requested under R.139 EPC, second sentence.

2. Novelty and Inventive Step

The WO-ISR acknowledges the novelty of the claim set but considers it does not involve an inventive step. Applicant respectfully disagrees with this opinion for the ensuing reasons.

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

The Applicant considers that it is more that this administrative policy and, actually, the present invention 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 present invention 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 invention 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.

So, the present invention is not defining mere data stored on 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 that the only alleged technical 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 invention is made, the Applicant wishes to address the cited documents D1 and D2.

Regarding 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 place 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.

Concerning document **D2**:

D1 is not addressing the same topic as the present invention. 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 present invention.

Finally, concerning section 3.3 of the WO-ISA, 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 actual invention feature related to security policy divulcation for selected namespaces intervenes.

In conclusion, it is considered that claim 1 does involve an inventive step with the meaning of Art. 56 EPC. The dependent claims are also new and inventive by virtue of their dependencies.

3. Conclusion

It is believed from the foregoing that the claim set is now in order and satisfies all the requirements of the EPC. Nevertheless, if any outstanding objections remain, the Examiner is invited to either contact the undersigned by telephone or issue a communication under Art. 94(3) EPC.

Solely as a precaution in the event the Examiner is minded to refuse the application, Oral Proceedings are formally requested under Art. 116 EPC throughout the examination procedure.

Yours faithfully,

Manuel QUINTERO ROMERO
European Patent Attorney
Tel: +33 155016194
Email: intellectual.property@thalesgroup.com

Enc.: - Amended claims (clean and working copies)



Letter accompanying subsequently filed items

Representative:

Manuel QUINTERO ROMERO
Thales Dis France SAS
Intellectual Property Department
6 Rue de la Verrerie
92190 Meudon
France

Phone: +33155016194

E-mail: intellectual.property@thalesgroup.com

80298 Munich
Germany
Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818
2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin
Germany
Tel. +49(0)30 25901-0 | Fax -840

The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

Application number:

EP20775659.4

Applicant's or representative's reference

GMT4110-EPT/MQ

	Description of document	Original file name	Assigned file name
1	Reply to search opinion/written opinion/IPER	3-1. GMT4110 EPT_Response to R161&162 EPC as Filed.pdf	WOREPLY-1.pdf
2	Amended claims with annotations	2-2. GMT4110 EPT_Amended claims_with annotations.pdf	CLMS-HWA-1.pdf
3	Amended claims (clean copy)	2-3. GMT4110 EPT_Amended claims_clean copy.pdf	CLMS-1.pdf

Signatures

Place: **Meudon**
Date: **05 December 2022**
Signed by: **/Manuel Quintero Romero/**
Representative name: **Manuel QUINTERO ROMERO**
Capacity: **Representative**
Function of person signing: **Representative**

Thales DIS France SAS
6, rue de la Verrerie
92197, Meudon Cedex
France
T: +33 (0) 1 55 01 50 00
www.thalesgroup.com

European Patent Office
Eric BIHL
80298 MUNICH
GERMANY

Ref: Our telephone conversation on the 08/08/2023

Object :

La Ciotat August 09, 2022

Dear Sir

This letter refers to the phone conversation of the 08/08/2022.

Thank you for your message advising us to update Thales recent legal form's name [**Thales Dis France SAS**] on the addresses of our representatives. Indeed they were still domiciliated to Thales dis France SA.

We thus kindly ask you to update and record this legal form name for each representative from Thales Dis France SA to Thales Dis France SAS.

Please do not hesitate to come back to us, should you need firther explanations,

Best Regards,

Emmanuel Grevin
European patent attorney





Letter accompanying subsequently filed items

Representative:

Emmanuel GREVIN
THALES DIS FRANCE SAS
Intellectual Property
Zone Athelia IV
Avenue du Jujubier
13705 LA CIOTAT
France

80298 Munich
Germany
Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818
2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin
Germany
Tel. +49(0)30 25901-0 | Fax -840

The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

Application number

00000000.0

Applicant's or representative's reference

OEB_Eric BIHL

	Description of document	Original file name	Assigned file name
1	Document concerning representation	OEB_ Update of representatives legal form's address.pdf	FREP-1.pdf

	Payment	
1	Method of payment	Not specified

Signatures

Place: LA CIOTAT
Date: 09 August 2022
Signed by: Emmanuel Grevin 17228
Representative name: Emmanuel GREVIN
Capacity: (Representative)

OEB_Eric BIHL



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication?
Contact Customer Services at www.epo.org/contact



Quintero Romero, Manuel
Thales Dis France SA
Intellectual Property Department
6, rue de la Verrerie
92190 Meudon
FRANCE

Date	27.07.2022
------	------------

Reference GMT4110-EPT/MQ	Application No./Patent No. 20775659.4 - 1218 / 4046126
Applicant/Proprietor Thales Dis France SAS	

Communication of European publication number and information on the application of Article 67(3) EPC

Provisional protection under Article 67(1) and (2) EPC in the individual contracting states becomes effective when the conditions referred to in Article 67(3) EPC have been fulfilled. Provisional protection in the individual extension and validation states is governed by the national laws of the countries concerned. For more details, see Chapter III of the EPO brochure "National Law relating to the EPC" (www.epo.org/law-practice/legal-texts/national-law.html), which also contains information about the extension and validation system. Further information can also be found in the Official Journal of the European Patent Office.

Pursuant to Article 153(3) EPC the publication under Article 21 PCT of an international application for which the European Patent Office is a designated or elected Office takes the place of the publication of a European patent application.

The bibliographic data of the above-mentioned Euro-PCT application will be published on 24.08.22 in Section I.1 of the European Patent Bulletin. The European publication number is 4046126.

In all future communications to the European Patent Office, please quote the application number plus Directorate number.

For the Examining Division





European Patent Office
80298 MUNICH
GERMANY

Questions about this communication?
Contact Customer Services at www.epo.org/contact



Quintero Romero, Manuel
Thales Dis France SA
Intellectual Property Department
6, rue de la Verrerie
92190 Meudon
FRANCE

Date	30.05.2022
------	------------

Reference GMT4110-EPT/MQ	Application No./Patent No. 20775659.4 - 1213
Applicant/Proprietor Thales Dis France SAS	

Communication pursuant to Rules 161(1) and 162 EPC

1. Correction of deficiencies noted in the written opinion and amendment of the application (R. 161(1) EPC)

The above-mentioned international (Euro-PCT) application has entered the European phase.

The EPO as International Searching Authority and, where a demand under Article 31 PCT was filed, also as International Preliminary Examining Authority has drawn up a written opinion on this application or the EPO as Supplementary International Searching Authority has issued explanations pursuant to Rule 45*bis*.7(e) PCT to the supplementary international search report.

You are invited to correct any deficiencies noted in the written opinion of the International Searching Authority or in the International Preliminary Examination Report, or in the explanations to the supplementary international search report and to amend the description, claims and any drawings within a **non-extendable period of six months** after notification of the present invitation.

Should you not comply with or comment on this invitation within the time limit, **the application will be deemed to be withdrawn** in accordance with Rule 161(1) EPC.

2. Amendment of application

Under Articles 28, 41 PCT and Rules 52, 78 PCT the application may be amended before a designated or elected Office, and in accordance with Rule 137(2) EPC the applicant may amend the description, claims and drawings of his own volition together with any comments, corrections or amendments made in response to the communication under Rule 161(1) EPC.

Whether or not you have already done so, you now have a further opportunity to file amended claims or other application documents within the above-mentioned period.

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

The claims applicable on expiry of the above period, i.e. those filed on entry into the European phase or in response to the present communication, will form the basis for the calculation of any claims fee to be paid (see page 2).

Registered Letter

EPO Form 1226AA 12.17 (NFS) EUCL (20/05/22)

page 1 of 3

--2/

3. Claims fees under Rule 162 EPC

If the application documents on which the European grant procedure is to be based comprise more than fifteen claims, a claims fee shall be payable for the sixteenth and each subsequent claim within the period provided for in Rule 159(1) EPC.

- ☐ Based on the application documents currently on file, all necessary claims fees have already been paid (or the documents do not comprise more than 15 claims).
- ☒ All necessary fees will be debited automatically according to the automatic debit order.
- ☐ The claims fees due for the claims to were not paid within the above-mentioned period.

Any outstanding claims fee, either based on the current set of claims or on any amended claims to be filed pursuant to Rule 161 EPC (see page 1), may still be validly paid within a **non-extendable period of six months** after notification of this communication (R. 162(2) EPC).

If a payment is made for only some of the claims, you must indicate for which claims it is intended. If a claims fee is not paid in due time, the claim concerned is deemed to be abandoned (R. 162(4) EPC).

If claims fees have already been paid, but on expiry of the above-mentioned period there is a new set of claims containing fewer fee-incurring claims than before, the claims fees in excess of those due under Rule 162(2), second sentence EPC will be refunded (R. 162(3) EPC).

The claims fee is currently

EUR 250,00 for the 16th and each subsequent claim up to the limit of 50
EUR 630,00 for the 51st and each subsequent claim

Making payments

For payments made via deposit account, please note that as from 1 December 2017 debit orders will only be carried out if filed in an electronically processable format (xml), using an accepted means of filing as laid down in the Arrangements for deposit accounts (ADA), published in the Supplementary publication in the Official Journal.

All relevant information related to the modes of payment of fees to the EPO can be retrieved from the EPO website at **"Making Payments"**.

Information concerning fee amounts

Procedural fees are usually adjusted every two years, on even years, with effect from 1 April. Therefore, before making a payment, parties should verify the amounts actually due on the date of payment using the applicable version of the Schedule of fees and expenses, published as a Supplement to the Official Journal of the EPO, available on the EPO website (www.epo.org) at www.epo.org/schedule-of-fees. The "Schedule of fees" table allows the viewing, downloading and searching of individual fee amounts, both current and previous.

Important note to users of the automatic debiting procedure

Unless the EPO receives prior instructions to the contrary, the fees for all claims incurring fees will be debited on the last day of the period for payment.

For the Examining Division



DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
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	INV. G06Q50/26 G06Q20/32 G06Q20/36
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	
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	TECHNICAL FIELDS SEARCHED (IPC) G06Q G07G
The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of the search 24 April 2020	Examiner Nicoli, Félix
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

1
EPO FORM 1503 03/82 (P04C01)

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	<p>Anonymous: "Thales lance son nouveau portefeuille d'identité numérique - vos documents d'identité accessibles où que vous soyez Thales Group",</p> <p>29 July 2019 (2019-07-29), pages 1-7, XP055689283,</p> <p>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 *</p> <p>-----</p>	1-16	
			TECHNICAL FIELDS SEARCHED (IPC)
The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of the search 24 April 2020	Examiner Nicoli, Félix
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p>		<p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons</p> <p>..... & : member of the same patent family, corresponding document</p>	

1
EPO FORM 1503 03/82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 19 30 6357

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

24-04-2020

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

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

The examination is being carried out on the **following application documents**

Description, Pages

1-17 as originally filed

Claims, Numbers

1-16 as originally filed

Drawings, Sheets

1/9-9/9 as originally filed

1 Reference is made to the following documents; the numbering will be adhered to in the rest of the procedure.

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/](https://www.emvco.com/wp-content/uploads/documents/Emvapp_20090126073328.pdf)

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-](https://www.thalesgroup.com/fr/group/journaliste/press_release/thales-lance-son-nouveau-portefeuille-didentite-numerique-vos)

nouveau-portefeuille-didentite-numerique-vos

[retrieved on 2020-04-24]

2 The subject-matter of claims 2-4, 7, 8 and 10 is not clear, in the sense of Article 84 EPC, for the following reasons:

2.1 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.

2.2 Claim 7 depends on claim 1 and defines "the required authentication" "; no antecedent for this feature can be found in claim 1.

3 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, Article 84 EPC and Rule 43(4) EPC.

4 The subject-matter of claim 16 not deemed to be inventive in the sense of Article 56 EPC for the following reasons:

4.1 Claim 16 reads:

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.

4.1.1 The scheme underlying present claim 16 is as follows:

A method for managing security policies for data items of a user, comprising:

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

transmitting the security policy of each of the plurality of supported namespaces to a service provider

selecting, by the service provider, at least one of the namespaces as candidate namespaces, and transmitting from service provider to the user, a list containing the candidate namespaces;

transmitting to the service by the user, the security policy associated with each of the selected candidate namespaces;

the service provider performs the following steps:

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

if the service can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the service provider can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the user;

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

upon successful demonstration by the service provider to the user of satisfaction of the security policy of the selected namespace, granting access to the data item by the user to the service provider.

Basically, a user wishes to access a service for which he/she needs to provide identification information. The user can provide several sorts of identification information but each information needs an accreditation level to be consulted. The service provider aware of its own level of accreditation selects the user identification information it may use to check for allowing or disallowing access to the requested service. If the service provider does not have a sufficient level of accreditation level for any of the user identification information, it abandons its request and the user cannot access to the initially requested service.

A security policy is understood as a required level of accreditation and a namespace as a category/kind of user identification information.

Thus, such a scheme is deemed to be an administrative scheme for checking the legitimacy of a user to access a service (Is he/she old enough to buy alcohol ? for example); such a scheme is not relevant for assessing inventive step.

4.1.2 When considering the wording of this claim, the only technical features appear to be by a mobile device with digital wallet in communication with a reader. Any other feature is deemed to relate to an administrative step. The non-technical features do not interact with the identified technical features to produce a further technical effect.

- 4.2 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).
- 4.3 The only apparent technical problem appears then to reside in the implementation of the considered administrative scheme (see item 4.1.1) when starting from the identified closest prior art (see item 4.2). The skilled person made aware of such a scheme would implement it as a routine activity at the level defined in the claims.
- 4.4 Hence, claim 16 is not inventive, Article 56 EPC.
- 5 The subject-matter of claims 1-10 corresponds to a large extent to the subject-matter of claim 1 such that the objections, under Article 56 EPC, raised against claim 16 also apply to present claims 1-10. Claims 1-10 are not inventive in the sense of Article 56 EPC for the following reasons:
- 5.1 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.
- 5.2 The definition of level confidence for namespaces is an administrative step which appears merely to define that 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 a administrative criteria. Thus, claims 2 and 9 are not inventive, Article 56 EPC.
- 5.3 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 56 EPC.
- 5.4 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 56 EPC.
- 5.5 Claims 6 and 7 are mere implementation choices relating the provision of policy information and the required authentication levels from a service provider. Thus, claim 6 and 7 are not inventive, Article 56 EPC.
- 5.6 Claim 10 defines obvious implementation choices. Thus, claim 10 is not inventive, Article 56 EPC.
- 5.7 Thus, claims 1-10 are not deemed to be inventive, Article 56 EPC.
-

- 6 Claim 11, 13-15 are not inventive in the sense of Article 56 EPC for substantially the reasons raised against claims 1, 4-6.
- 6.1 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 56 EPC.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44bis)

Applicant's or agent's file reference GMT4110 WO/YL	FOR FURTHER ACTION		See item 4 below
International application No. PCT/EP2020/076906	International filing date (<i>day/month/year</i>) 25 September 2020 (25.09.2020)	Priority date (<i>day/month/year</i>) 18 October 2019 (18.10.2019)	
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237			
Applicant THALES DIS FRANCE SAS			

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 bis.1(a).
2. This REPORT consists of a total of 9 sheets, including this cover sheet.

In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

- | | | |
|-------------------------------------|--------------|---|
| ☒ | Box No. I | Basis of the report |
| ☐ | 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 Article 35(2) with regard to novelty, inventive step or 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 |

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44bis.3(c) and 93bis.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44bis .2).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Date of issuance of this report 19 April 2022 (19.04.2022)
	Authorized officer Nora Lindner e-mail pct.team5@wipo.int

Form PCT/IB/373 (revised January 2020)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY (PCT Rule 43bis.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.
PCT/EP2020/076906

International filing date (day/month/year)
25.09.2020

Priority date (day/month/year)
18.10.2019

International Patent Classification (IPC) or both national classification and IPC
INV. G06Q50/26 G06Q20/32 G06Q20/36

Applicant
THALES DIS FRANCE SA

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:



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

Date of completion of
this opinion

see form
PCT/ISA/210

Authorized Officer

Nicoli, Félix

Telephone No. +31 70 340-0



**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/EP2020/076906

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:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/EP2020/076906

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

1. Statement

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

2. Citations and explanations

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

1 Re Item V

**Reasoned statement with regard to novelty, inventive step or industrial
applicability; citations and explanations supporting such statement**

1.1 Reference is made to the following documents:

D1 US 2016/294831 A1 (BORUNDA ADRIAN [US] ET AL) 6 October 2016
(2016-10-06)

D2 WO 2015/036957 A1 (TORO DEV LTD [CN]) 19 March 2015 (2015-03-19)

D3 US 2016/156386 A1 (VAN NIEUWENHUYZE OLIVIER [BE] ET AL) 2 June 2016
(2016-06-02)

EMVCO: "EMV '96 Integrated Circuit Card Application Specification for Payment
Systems",
EMV, EMVCO

D4 vol. 3.1.1 ; Contact 1 July 2006 (2006-07-01), pages 1-62, XP061034511,
Retrieved from the Internet:
URL: [https://www.emvco.com/wp-content/uploads/documents/
Emvapp_20090126073328.pdf](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](https://www.thalesgroup.com/fr/group/journaliste/press_release/thales-lance-son-nouveau-portefeuille-didentite-numerique-vos)
[retrieved on 2020-04-24]

**2 The subject-matter of claim 16 not deemed to be inventive in the sense of Article 33(3) PCT for
the following reasons:**

2.1 Claim 16 reads:

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

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

 transmitting the security policy of each of the plurality of supported namespaces to a read-

er connected to a verifier;

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

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

operating the reader to:

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

if the verifier can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the verifier terminal can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the mobile device; if the verifier cannot satisfy the security policy of any of the candidate namespaces, rejecting access to the data item; and

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

2.2.1 The scheme underlying present claim 16 is as follows:

A method for managing security policies for data items of a user, comprising:

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

transmitting the security policy of each of the plurality of supported namespaces to a service provider

selecting, by the service provider, at least one of the namespaces as candidate namespaces, and transmitting from service provider to the user, a list containing the candidate namespaces;

transmitting to the service by the user, the security policy associated with each of the selected candidate namespaces;

the service provider performs the following steps:

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

if the service can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the service provider can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the user;

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

upon successful demonstration by the service provider to the user of satisfaction of the security policy of the selected namespace, granting access to the data item by the user to the service provider.

Basically, a user wishes to access a service for which he/she needs to provide identification information. The user can provide several sorts of identification information but each information needs an accreditation level to be consulted. The service provider aware of its own level of accreditation selects the user identification information it may use to check for allowing or disallowing access to the requested service. If the service provider does not have a sufficient level of accreditation level for any of the user identification information, it abandons its request and the user cannot access to the initially requested service.

A security policy is understood as a required level of accreditation and a namespace as a category/kind of user identification information.

Thus, such a scheme is deemed to be an administrative scheme for checking the legitimacy of a user to access a service (Is he/she old enough to buy alcohol ? for example); such a scheme is not relevant for assessing inventive step.

2.2.2 When considering the wording of this claim, the only technical features appear to be a mobile device with a digital wallet in communication with a reader. Any other feature is deemed to relate to an administrative step. The non-technical features do not interact with the identified technical features to produce a further technical effect.

2.3 In view of the claim, the closest prior art appears to be a mobile phone including a digital wallet storing personal user information which can be accessed by a reader. Such a system was well-known in the art at the priority date of the application as this is shown for instance in D1 and D2 (see the citations in the search report).

2.4 The only apparent technical problem appears then to reside in the implementation of the considered administrative scheme (see item 2.2.1) when starting from the identified closest prior art (see item 2.3). The skilled person made aware of such a scheme would implement it as a routine activity at the level defined in the claims.

2.5 Hence, claim 16 is not inventive, Article 33(3) PCT.

3 The subject-matter of claims 1-10 corresponds to a large extent to the subject-matter of claim 16 such that the objections, under Article 33(3) PCT, raised against claim 16 also apply to present claims 1-10. Claims 1-10 are not inventive in the sense of Article 33(3) PCT for the following reasons:

3.1 Claims 1 and 5 are not inventive for the reasons raised against claim 16.

It is also noted that the concept of namespace used to characterize a family of information is also a well-known principle. The use of such a principle for user identity information cannot be deemed to be inventive.

- 3.2 The definition of level confidence for namespaces is an administrative step which appears merely to define, for instance, that a passport may be more trustworthy than a club member card. The use of blacklists or whitelists for expressing such a confidence cannot be deemed inventive. The overhead associated with a security policy is understood as the capacity of a service provider to demonstrate a sufficient level of accreditation; this is also at such level of definition an administrative criteria. Thus, claims 2 and 9 are not inventive, Article 33(3) PCT.
- 3.3 Manual selection of a namespace by a user representing the service provider is a mere matter of choice. The use of a user interface for that purpose is obvious to the skilled person. Thus, claim 3 is not inventive, Article 33(3) PCT.
- 3.4 The filtering out of namespaces merely materialises that the user selects which identity information she/he accepts to disclose for a given purpose. This is a non-technical choice which would be implemented as a routine activity at the level of definition of the claim 4. Thus, claim 4 is not inventive, Article 33(3) PCT.
- 3.5 Claims 6 and 7 are mere implementation choices relating the provision of policy information and the required authentication levels from a service provider. Thus, claims 6 and 7 are not inventive, Article 33(3) PCT.
- 3.6 Claim 10 defines obvious implementation choices. Thus, claim 10 is not inventive, Article 33(3) PCT.
- 3.7 Thus, claims 1-10 are not deemed to be inventive, Article 33(3) PCT.
- 4 Claim 11, 13-15 are not inventive in the sense of Article 33(3) PCT for substantially the reasons raised against claims 1, 4-6.
- 4.1 Claim 12 appears to define that the service provider may request to be made aware of the nature of the identity information that may be used from the wallet. It is noted that such a disclosure of wallet possibilities is a well-known principle as this is exemplified by digital wallets including payment applications which are communicated to a reader -see D4 (see the citations in the search report). The mere use of such a well-known principle for a digital wallet including user identity information cannot be deemed to be inventive. Thus, claim 12 is not inventive, Article 33(3) PCT.

5 Re Item VII

Certain defects in the international application

- 5.1 It appears that all features of claim 1 are included in present claim 16 such that claim 16 should be made dependent on claim 1, Rule 6 PCT.

6 **Re Item VIII**

Certain observations on the international application

- 6.1 The application does not meet the requirements of Article 6 PCT, because claims 2-4, 7, 8 and 10 are not clear for the following reasons:
- 6.1.1 Claim 2 depends on claim 1 and defines "the verifier module" and "the verifier"; no antecedent for these features can be found in claim 1.
- A similar objection also applies to claims 3, 4, 8 and 10 which may all depend on claim 1 and define features such as "the verifier module", "the verifier", the "verifier terminal" which cannot be found in claim 1.
- 6.1.2 Claim 7 depends on claim 1 and defines "the required authentication" "; no antecedent for his feature can be found in claim 1.



Acknowledgement of receipt

We hereby acknowledge receipt of the form for entry into the European phase (EPO as designated or elected Office) as follows:

Submission number	10858148	
PCT application number	PCT/EP2020/076906	
EP application number	20775659.4	
Date of receipt	14 April 2022	
Receiving Office	European Patent Office, The Hague	
Your reference	GMT4110-EPT/MQ	
Applicant		
Country		
Documents submitted	package-data.xml application-body.xml	ep-euro-pct.xml epf1200.pdf (4 p.)
Submitted by	CN=secure.epoline.org	
Method of submission	Online	
Date and time receipt generated	14 April 2022, 14:19 (CEST)	
Message Digest	84:C8:AE:F6:BB:8E:D9:E0:9E:48:16:4D:3C:F0:2E:CE:90:C7:1E:60	

/European Patent Office/



Entry into the European phase (EPO as designated or elected Office)

To the European Patent Office

European application number	EP20775659.4
PCT application number	PCT/EP2020/076906
PCT publication number	WO2021073853
Applicant's or representative's reference	GMT4110-EPT/MQ
International Filing Date	25.09.2020
International Searching Authority (ISA)	EP
International Preliminary Examining Authority (IPEA)	not applicable
1. Applicant Indications concerning the applicant(s) are contained in the international publication or were recorded by the International Bureau after the international publication. Changes which have not yet been recorded by the International Bureau are set out here:	☒ ☐
2. Representative Representative 1 Representative or association of representatives to be listed in the Register of European Patents and to whom communications are to be notified	Name: QUINTERO ROMERO Manuel Company: Thales Dis France SAS Department: Intellectual Property Department Address of place of business: 6 Rue de la Verrerie 92190 Meudon France Telephone: +33155016194 E-mail: intellectual.property@thalesgroup.com
3. Authorisation Representative 1 An individual authorisation is attached. A general authorisation has been registered under No: A general authorisation has been filed, but not yet registered. The authorisation filed with the EPO as PCT receiving Office expressly includes the European phase.	☐ ☐ ☐ ☐
4. Request for examination Examination of the application under Art. 94 EPC is hereby requested. The examination fee is being (has been, will be) paid. Request for examination in an admissible non-EPO language: The/Each applicant hereby declares that he is an entity or a natural person under Rule 6(4) EPC.	☒ ☐ ☐
5. Copies Additional copies of the documents cited in the supplementary European search report are requested. Number of additional sets of copies	☐
6. Documents intended for proceedings before the EPO Number of claims on entry into the European phase: 6.1 Proceedings before the EPO as designated Office (PCT I) are to be based on the following documents the application documents published by the International Bureau; where the publication includes a set of claims amended under Article 19 PCT, the latter replaces the originally filed claims	16 ☒

<p>unless replaced by the amendments attached.</p>	☐
<p>comments on the written opinion established by the EPO as the International Searching Authority and/or observations or, where applicable, on the explanations given in the Supplementary International Search Report established by the EPO as the Supplementary International Searching Authority (Rule 45bis.7(e) PCT)</p>	☐
<p><i>Where necessary, further details should be attached as "Other documents"</i></p>	
<p>6.2 Proceedings before the EPO as elected Office (PCT II) are to be based on the following documents:</p>	
<p>the documents on which the international preliminary examination report is based, including any annexes</p>	☐
<p>unless replaced by the amendments attached.</p>	☐
<p>comments on the international preliminary examination report established by the EPO as the International Preliminary Examining Authority and/or observations are enclosed.</p>	☐
<p><i>Where necessary, further details should be attached as "Other documents"</i></p>	
<p>If the EPO as International Preliminary Examining Authority has been supplied with test reports, these may be used as the basis of proceedings before the EPO.</p>	☐
<p>6.3 A copy of the results of the search carried out by the authority with which the previous application(s) whose priority is claimed was (were) filed is attached (R. 141(1) EPC).</p>	☐
<p>7. Translations</p>	
<p>Translations in one of the official languages of the EPO (English, French, German) are attached as crossed below:</p>	☐
<p><i>* In proceedings before the EPO as designated or elected Office (PCT I + II):</i></p>	
<p>7.1 Translation of the international application (description, claims, any text in the drawings) as originally filed, of the abstract as published and of any indication under Rule 13bis.3 and 13bis.4 PCT regarding biological material</p>	☐
<p>7.2 Translation of the priority application(s) (to be filed only at the EPO's request, Rule 53(3) EPC)</p>	☐
<p>7.3 It is hereby declared that the international application as originally filed is a complete translation of the previous application (Rule 53(3) EPC)</p>	☐
<p><i>* In addition, in proceedings before the EPO as designated Office (PCT I):</i></p>	
<p>7.4 Translation of amended claims and any statement under Art. 19 PCT, if the claims as amended are to form the basis for the proceedings before the EPO (see Section 6).</p>	☐
<p><i>* In addition, in proceedings before the EPO as elected Office (PCT II):</i></p>	
<p>7.5 Translation of any annexes to the international preliminary examination report</p>	☐
<p>8. Biological material</p>	
<p>The invention uses and/or relates to biological material deposited under Rule 31 EPC.</p>	☐
<p>The particulars referred to in Rule 31(1)(c) EPC (if not yet known, the depositary institution and the identification reference(s)) [number, symbols, etc.] of the depositor are given in the international publication or in the translation submitted in Section 7 on:</p>	☐
<p>page(s) / line(s)</p>	
<p>The receipt(s) of deposit issued by the depositary institution</p>	
<p>is (are) enclosed.</p>	☐
<p>will be filed later.</p>	☐
<p>Waiver of the right to an undertaking from the requester pursuant to Rule 33(2) EPC attached.</p>	☐
<p>9. Nucleotide and amino acid sequences</p>	
<p>The international application discloses nucleotide and/or amino acid sequences.</p>	☐
<p>9.1 The sequence listing was filed under Rule 5.2(a) PCT, or furnished to the EPO as ISA under Rule 13ter.1(a) PCT, or is otherwise available to the EPO, in computer-readable format in accordance with WIPO ST.25.</p>	☐
<p>9.2</p>	
<p>The sequence listing is attached in computer-readable format in accordance with</p>	☐

Table for section 6 of Form 1200.3

In accordance with the Notice from the European Patent Office dated 26 January 2009 concerning the 2009 fee structure (OJ EPO 2009, 118, and Guidelines for Examination in the EPO, April 2009, A-III, 13.2), the amount of the additional fee (Art. 2, item 1a, Rules relating to Fees) for the pages of this European patent application is calculated as follows:

Documents intended for proceedings before the EPO (R. 159 (1) (b) EPC) and for calculating the additional fee (Art. 2, item 1a, RFees):

	Page(s) from ... to ...	Number of pages
Description: International application as published	1 - 17	17
Claims: International application as published	18 - 21	4
Drawings: International application as published	1 - 9	9
Abstract: Default count: one page		1
Total number of pages		31
Fee-exempt pages (Art. 2, item 1a, RFees)		-35
Number of pages to be paid for		0
		(x 16 EUR per page)
Total amount payable	EUR	0



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication?
Contact Customer Services at www.epo.org/contact



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

Date	25.02.2022
------	------------

Reference	Application No./Patent No. 20775659.4 - 1213 PCT/EP2020076906
Applicant/Proprietor THALES DIS FRANCE SAS	

Entry into the European phase before the European Patent Office

The following information describes the procedural steps required for entry into the European phase before the European Patent Office (EPO) as designated/elected Office. You are advised to read it carefully because failure to take the necessary action in due time can lead to a loss of rights.

1. The above mentioned international patent application has been given the **European application No. 20775659.4**. This application number is to be used in correspondence with the EPO.
2. Applicants **without a residence or their principal place of business** in an EPC Contracting State may themselves initiate European processing of their international applications, provided they do so before expiry of the 31st month from the priority date.

During the European phase before the EPO as designated or elected Office, however, such applicants **must** be represented by a professional representative (Art. 133(2) and Art. 134(1) and (8) EPC).

Where, at the expiry of the time period laid down in Rule 163(5) EPC, the requirements of Article 133(2) EPC have not been complied with, the European patent application will be **refused**, pursuant to Rule 163(6) EPC.

Please note that a professional representative authorised to act before the EPO and who acted for the applicant during the international phase does not automatically become the representative for the European phase. Applicants are therefore strongly advised to appoint in good time any representative they wish to initiate the European phase for them; otherwise the EPO has to send all communications directly to the applicant.

3. Applicants **with a residence or their principal place of business** in an EPC Contracting State are not obliged to appoint for the European phase a professional representative authorised to act before the EPO. However, in view of the complexity of the procedure it is recommended that they do so.
4. Applicants and professional representatives are also strongly advised to initiate the European phase using **EPO Form 1200**. It is available free of charge from the EPO or via the EPO website at www.epo.org. Similarly, it can be generated using the Online Filing software, obtainable free of charge from the EPO, or using Online Filing 2.0. The use of the form is not compulsory.
5. Applicants wishing to use an address for correspondence which is different from the address of their

seat or residence are advised to indicate this address in section 1 of EPO Form 1200. When acting as designated or elected Office, the EPO will accept an address for correspondence only if no professional representative must be or is appointed (Art. 133 and 134 EPC). This address must be the applicant's own address and must be located in an EPC Contracting State. Any address for correspondence accepted for the procedure in the international phase which does not fulfil those conditions will not be accepted in the procedure before the EPO in the European phase.

6. To enter the European phase before the EPO as designated or elected Office (Art. 22(1) and (3) and 39(1) PCT), the **following acts** must be performed by the applicant within **31 months** from the date of filing of the international application or (where applicable) the earliest priority date:
- a) Supply a translation of the international application into an EPO official language, if the International Bureau did not publish the application in such language (Art. 22(1) PCT and R. 159(1)(a) EPC);
 - b) Specify the application documents, as originally filed or as amended, on which the European grant procedure is to be based (R. 159(1)(b) EPC);
 - c) Pay the filing fee and, where applicable, the additional fee for a European patent application comprising more than 35 pages (R. 159(1)(c) EPC, Art. 2(1), items 1, 1a Rules relating to Fees (RFees));
 - d) Pay the search fee where a supplementary European search report has to be drawn up (R. 159(1)(e) EPC);
 - e) Pay the designation fee if the time limit laid down in Rule 39(1) EPC (i.e. six months after publication of the international search report) has expired before the 31-month period pursuant to Rule 159(1) EPC (R. 159(1)(d) EPC);
 - f) File the written request for examination and pay the examination fee if the time limit laid down in Rule 70(1) EPC has expired before the 31-month period pursuant to Rule 159(1) EPC (R. 159(1)(f) EPC);
 - g) Pay the renewal fee in respect of the third year, if the fee has fallen due (see Rule 51(1) EPC) before expiry of the 31-month period pursuant to Rule 159(1) EPC (R. 159(1)(g) EPC);
 - h) File, where applicable, the certificate of exhibition referred to in Article 55(2) and Rule 25 EPC (R. 159(1)(h) EPC);
 - i) Pay the claims fees for the sixteenth and each subsequent claim when the application documents on which the European grant procedure is to be based comprise more than fifteen claims (R. 162(1) EPC). A higher amount is payable for the 51st and each subsequent claim (Art.2(1), item 15 RFees).

If either the translation of the international application or the request for examination is not filed in time, or if the filing fee, the additional fee, the search fee, the designation fee or the examination fee is not paid in due time, the application shall be deemed to be withdrawn (R. 160(1) EPC).

7. Making payments

For payments made via deposit account, please note that as from 1 December 2017 debit orders will only be carried out if filed in an electronically processable format (xml), using an accepted means of filing as laid down in the Arrangements for deposit accounts (ADA), published in a Supplementary publication to the Official Journal.

All relevant information related to the modes of payment of fees to the EPO can be retrieved from the EPO website at "**Making Payments**".

Information concerning fee amounts

Procedural fees are usually adjusted every two years, on even years, with effect from 1 April. Therefore, before making a payment, parties should verify the amounts actually due on the date of payment using the applicable version of the Schedule of fees and expenses, published as a Supplement to the Official Journal of the EPO, available on the EPO website (www.epo.org) at www.epo.org/schedule-of-fees . The "Schedule of fees" table allows the viewing, downloading and searching of individual fee amounts, both current and previous.

8. Restoration of priority right

Where the international application contains a priority claim to an earlier application and it has been filed within two months from the expiration of the 12-month priority period, a request for restoration before the EPO as designated Office (R. 49ter.2 PCT) applies under the following circumstances:

- a) No request for restoration filed before the receiving Office (RO) during the international phase (R. 26bis.3 PCT)
- b) Negative decision by the RO irrespective of the criterion applied (due care/unintentionality)
- c) Positive decision by the RO based on the unintentionality criterion.

For a request to be admissible, it must be filed and the requisite fee must be paid (R. 49ter.2(b)(iii) and R. 49ter.2(d) PCT, Art.2(1), item 13 RFees) within the one-month time limit under R. 49ter.2(b)(i) PCT for filing the request, which starts from the expiry of the 31-month time limit pursuant to Rule 159(1)EPC and Article 22(3) or 39(1)(b) PCT or, where applicable, from the date on which an effective request for early processing (Art. 23(2) or 40(2) PCT) is filed ('Notice from the European Patent Office dated 21 February 2013 concerning the request for early processing', OJ EPO 2013, 158). The request for restoration also needs to state the reasons for the failure to file the international application within the priority period (Rule 49ter.2(b)(ii) PCT).

9. Incorporation by reference of correct application documents under Rule 20.5bis(d) PCT - incompatibility of Rule 20.5bis(d) PCT with the EPC

If the receiving Office considered correct application documents to be incorporated by reference under Rule 20.5bis(d) PCT without changing the filing date, this incorporation will not be effective in the proceedings before the EPO as designated or elected Office as a result of the EPO's notification of incompatibility of Rule 20.5bis(a)(ii) and (d) PCT with the EPC (OJ EPO 2020, A81).

In such cases, applicants may inform the EPO within the 31-month time limit under Rule 159(1) EPC:

- a) that they wish to pursue the application containing the correct application documents with the date of receipt of those application documents as its filing date, or
- b) that the correct application documents are to be disregarded and the initial filing date is to be maintained.

If the EPO is not so informed within the 31-month time limit, the procedure laid down in the Notice of the EPO dated 14 June 2020 concerning the applicability of new Rule 20.5bis PCT on the correction of erroneous filings in proceedings before the EPO (OJ EPO 2020, A81) will apply.

-
10. If the applicant had appointed a representative during the application's international phase, the present Form will be sent to the representative, asking him to inform the applicant accordingly. All subsequent communications will be sent to the applicant, or - if the EPO is informed of his appointment in time - to the applicant's European representative.
11. For more details about time limits and procedural acts before the EPO as designated or elected Office, see the EPO brochure Euro-PCT Guide: PCT procedure at the EPO. This brochure, the list of professional representatives before the EPO, Form 1200 and details of the latest fees are available on the EPO website (www.epo.org) .

12. Programme for accelerated prosecution of European patent applications - "PACE"

Applicants wishing to accelerate proceedings before the EPO as designated or elected Office may request accelerated prosecution under the PACE programme (Notice from the European Patent Office dated 30 November 2015 concerning the programme for accelerated prosecution of European patent applications - "PACE", OJ EPO 2015, A93).

Receiving Section



Copy for (RO-EP) 32
PATENT COOPERATION TREATY

PCT/EP2020/076906

From the INTERNATIONAL BUREAU

PCT

**NOTIFICATION OF THE RECORDING
OF A CHANGE**

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

To:

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

Date of mailing (<i>day/month/year</i>) 28 October 2021 (28.10.2021)		
Applicant's or agent's file reference GMT4110 WO/YL	IMPORTANT NOTIFICATION	
International application No. PCT/EP2020/076906	International filing date (<i>day/month/year</i>) 25 September 2020 (25.09.2020)	

1. The following indications appeared on record concerning:

☒ the applicant
 ☐ the inventor
 ☐ the agent
 ☐ the common representative

Name and Address THALES DIS FRANCE SA 6, rue de la Verrerie 92190 MEUDON FRANCE	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 <p align="center">Blanc Veronique</p> e-mail pct.team5@wipo.int Telephone No. +41 22 338 74 05
---	--

Copy for (DO-EP) 31
PATENT COOPERATION TREATY

PCT/EP2020/076906

From the INTERNATIONAL BUREAU

PCT

**NOTIFICATION OF THE RECORDING
OF A CHANGE**

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

To:

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

Date of mailing (<i>day/month/year</i>) 28 October 2021 (28.10.2021)		
Applicant's or agent's file reference GMT4110 WO/YL	IMPORTANT NOTIFICATION	
International application No. PCT/EP2020/076906	International filing date (<i>day/month/year</i>) 25 September 2020 (25.09.2020)	

1. The following indications appeared on record concerning:

☒ the applicant
 ☐ the inventor
 ☐ the agent
 ☐ the common representative

Name and Address THALES DIS FRANCE SA 6, rue de la Verrerie 92190 MEUDON FRANCE	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 <p align="center">Blanc Veronique</p> e-mail pct.team5@wipo.int Telephone No. +41 22 338 74 05
---	--

**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)

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

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

Document details: Country/Office: EP

Filing date: 18 Oct 2019 (18.10.2019)

Application number: 19306357

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

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

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

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

Bescheinigung

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

Certificate

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

Attestation

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

Patentanmeldung Nr.

Patent application No.

Demande de brevet n°

19306357.5 / EP19306357

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

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

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



V. Joseph

Anmeldung Nr:
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 Vertragsstaaten / Contracting States designated at date of filing / Etats contractants désignés lors du dépôt:

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

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

BACKGROUND OF THE INVENTION

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

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

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

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

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

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

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

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

SUMMARY

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Another aspect of the invention is a mobile device comprising:

a processor; and

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

receive a list of selected namespaces from a reader;

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

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

receive a request for supported namespaces from a reader;

transmit a list of supported name spaces to the reader.

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

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

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

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

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

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

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

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

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

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

- operating the reader to:

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

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

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

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

BRIEF DESCRIPTION OF THE DRAWINGS

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

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

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

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

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

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

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

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

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

DETAILED DESCRIPTION OF THE INVENTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

where

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

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

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

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

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

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

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

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

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

[0076] We Claim:

CLAIMS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

operating the reader to:

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

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

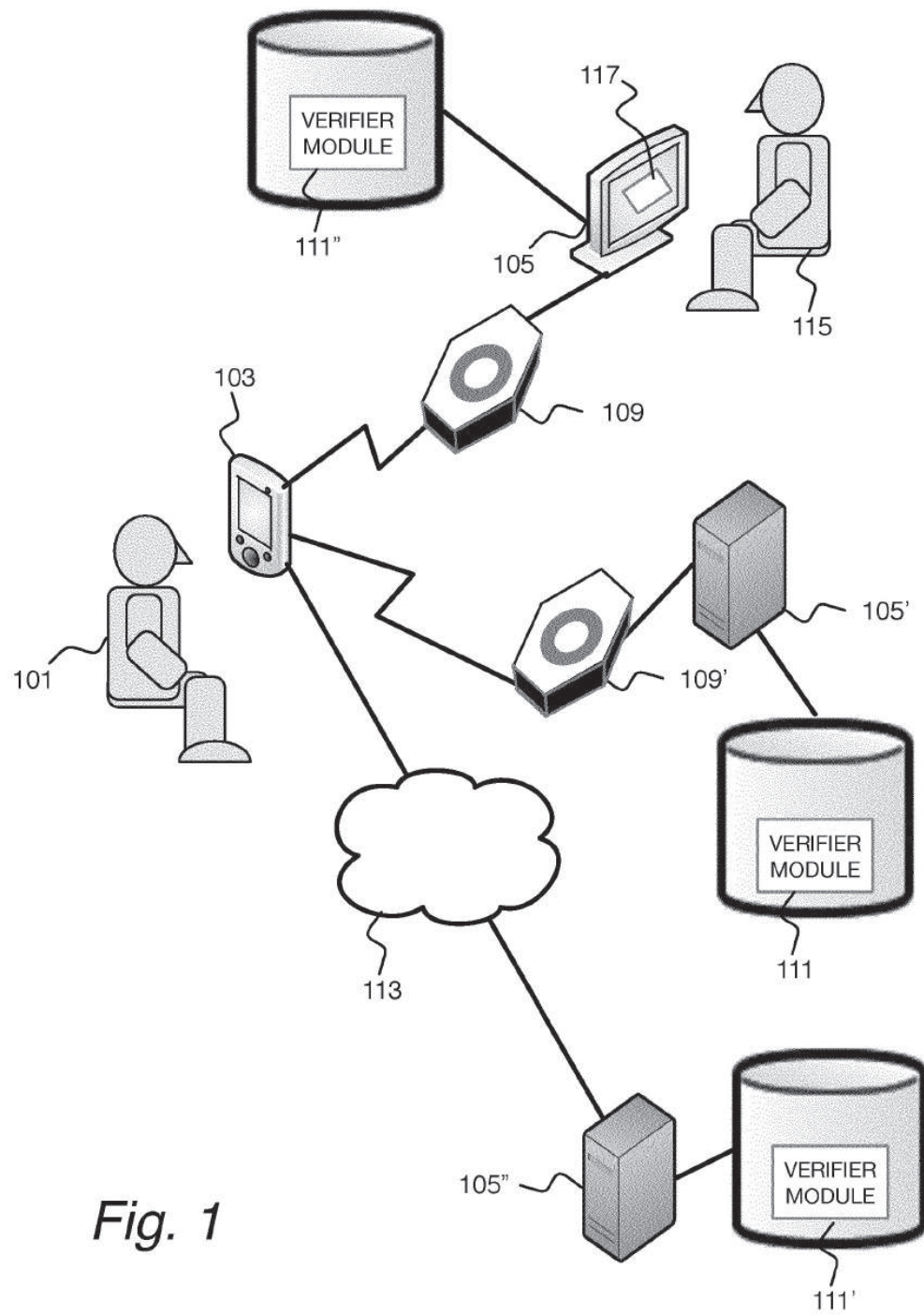
if the verifier cannot satisfy the security policy of any of the candidate namespaces, rejecting access to the data item; and

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

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

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

Figure 6a

*Fig. 1*

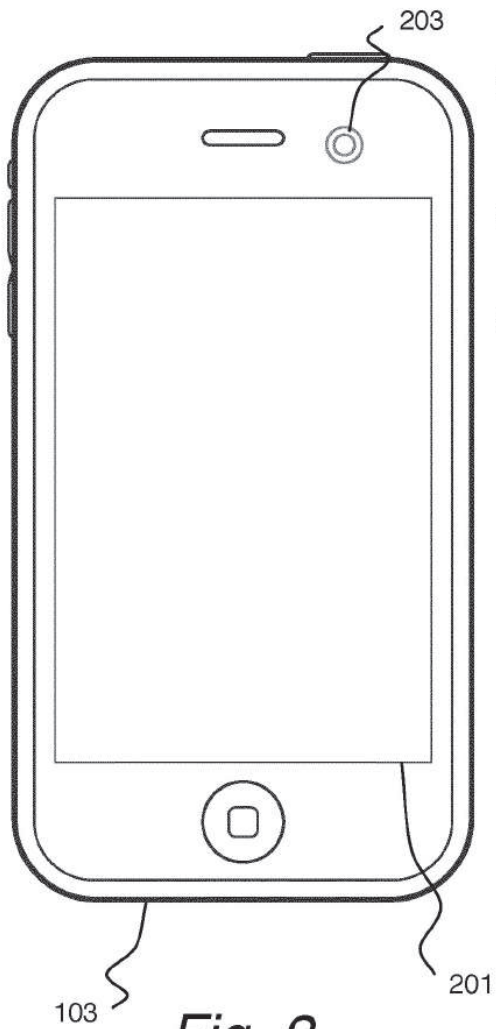


Fig. 2

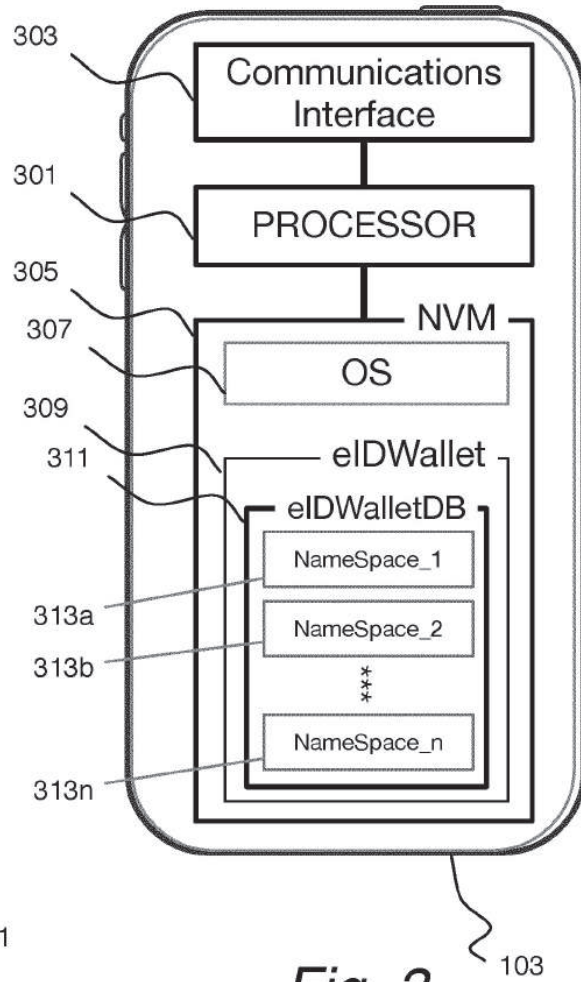
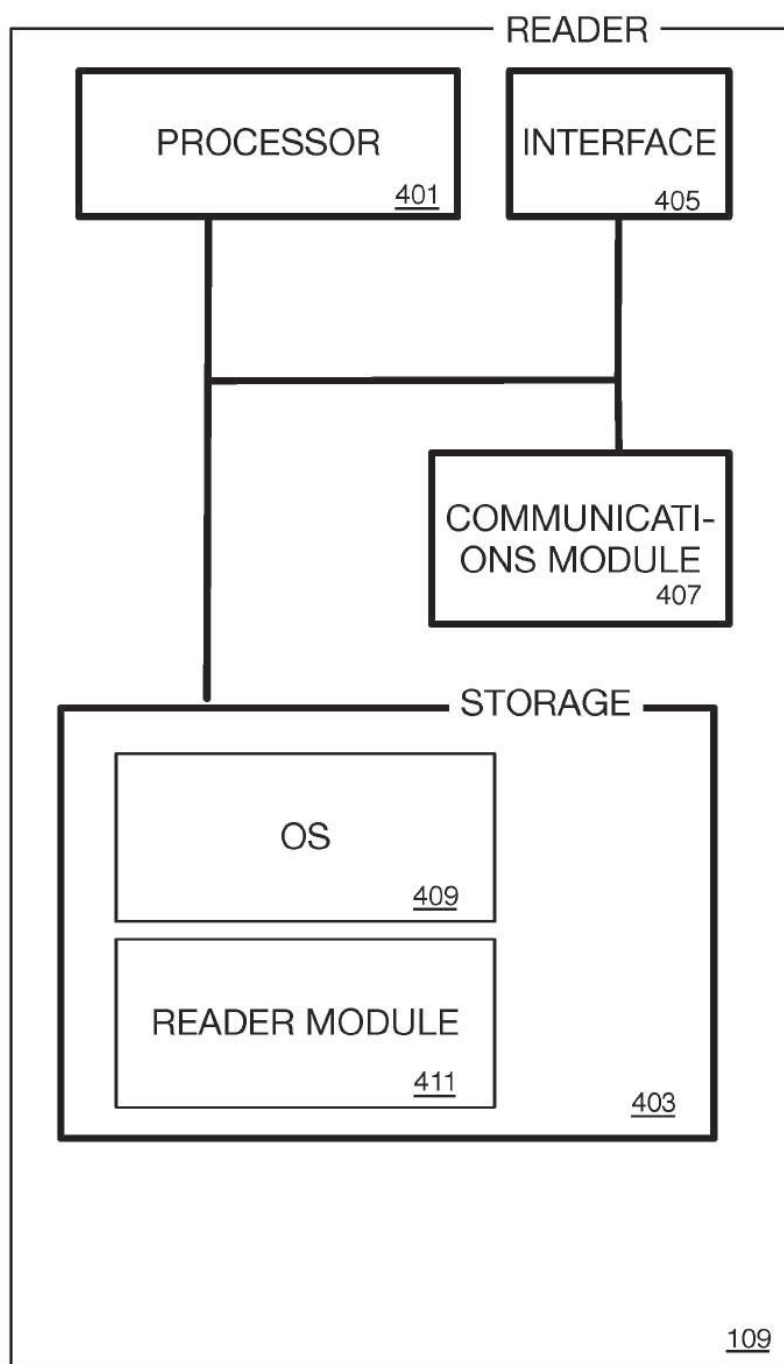
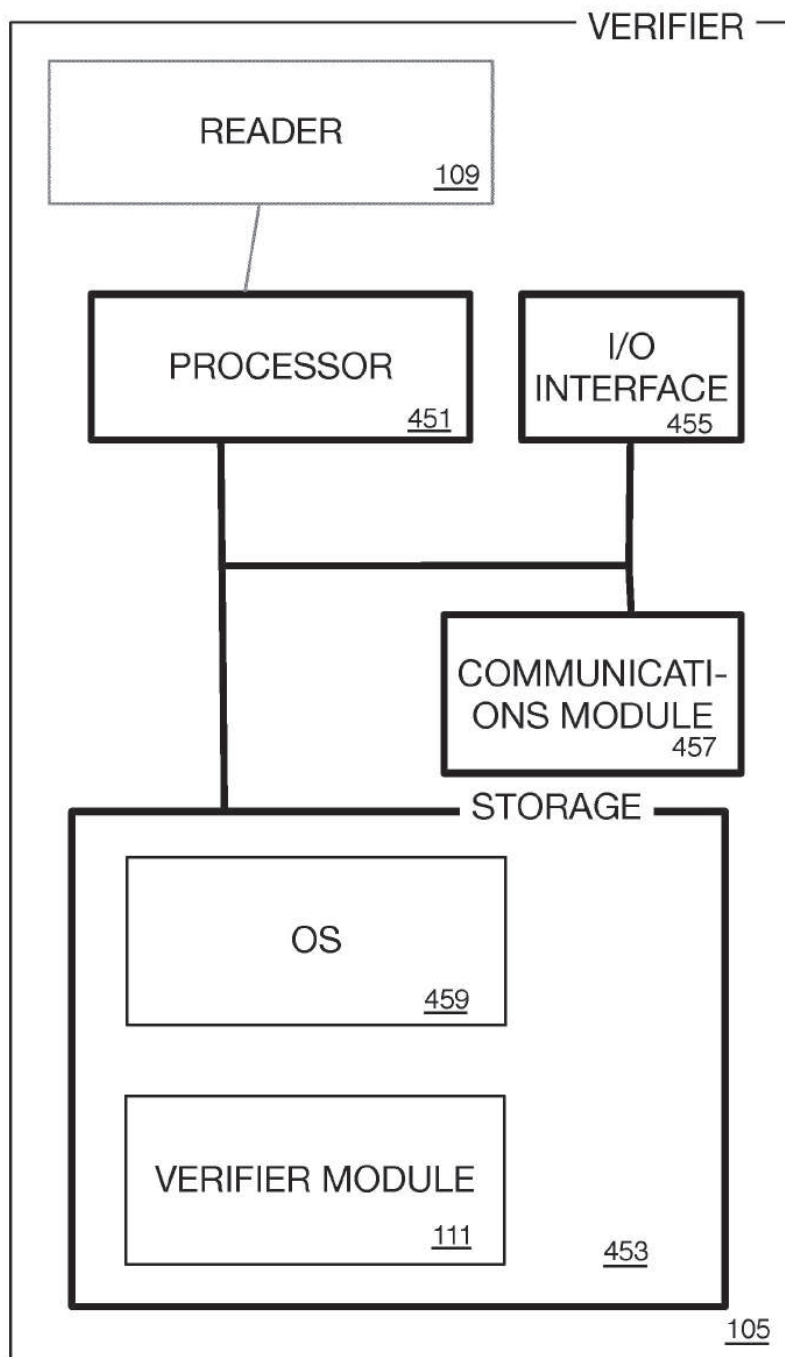


Fig. 3

*Fig. 4*

*Fig. 5*

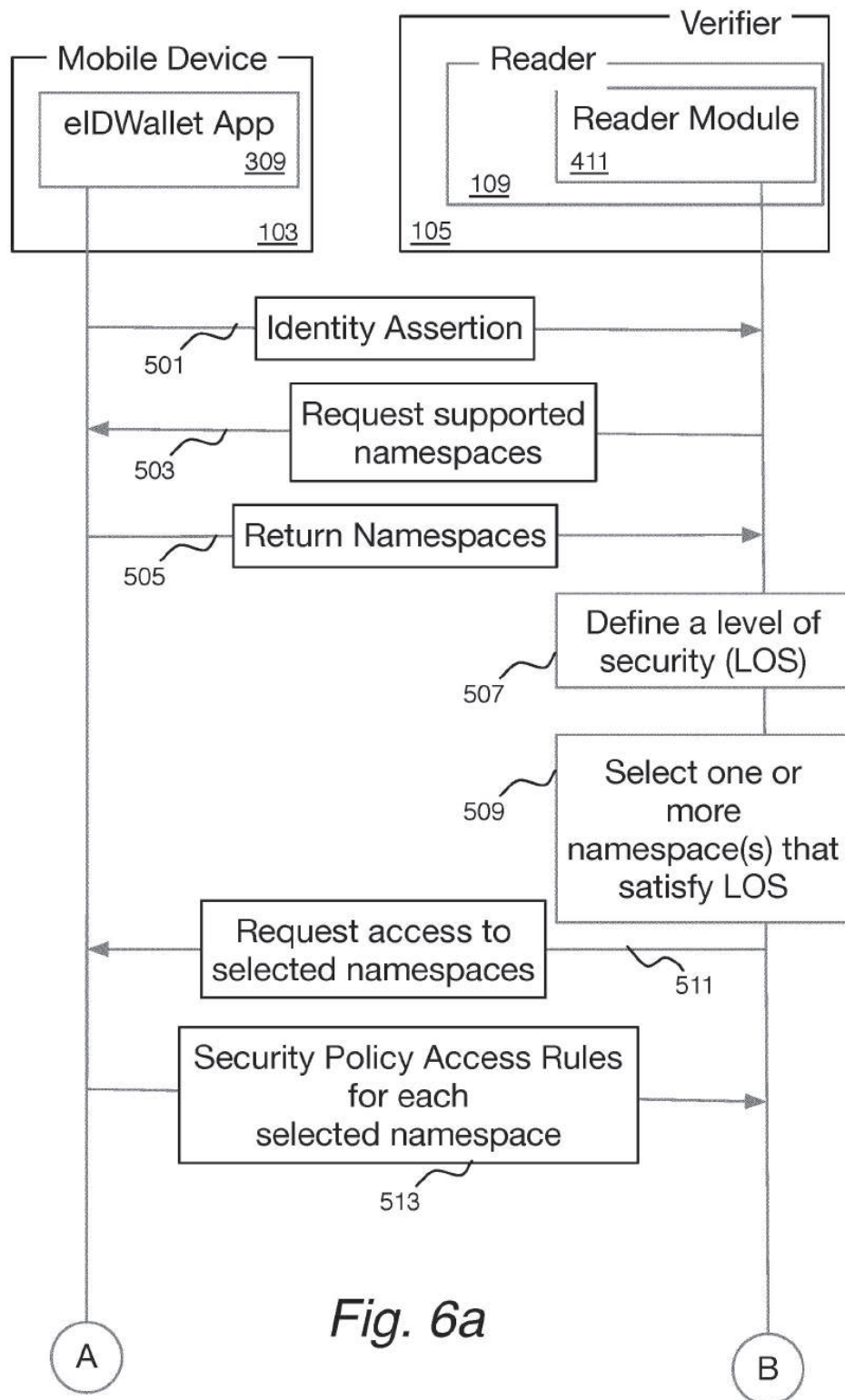
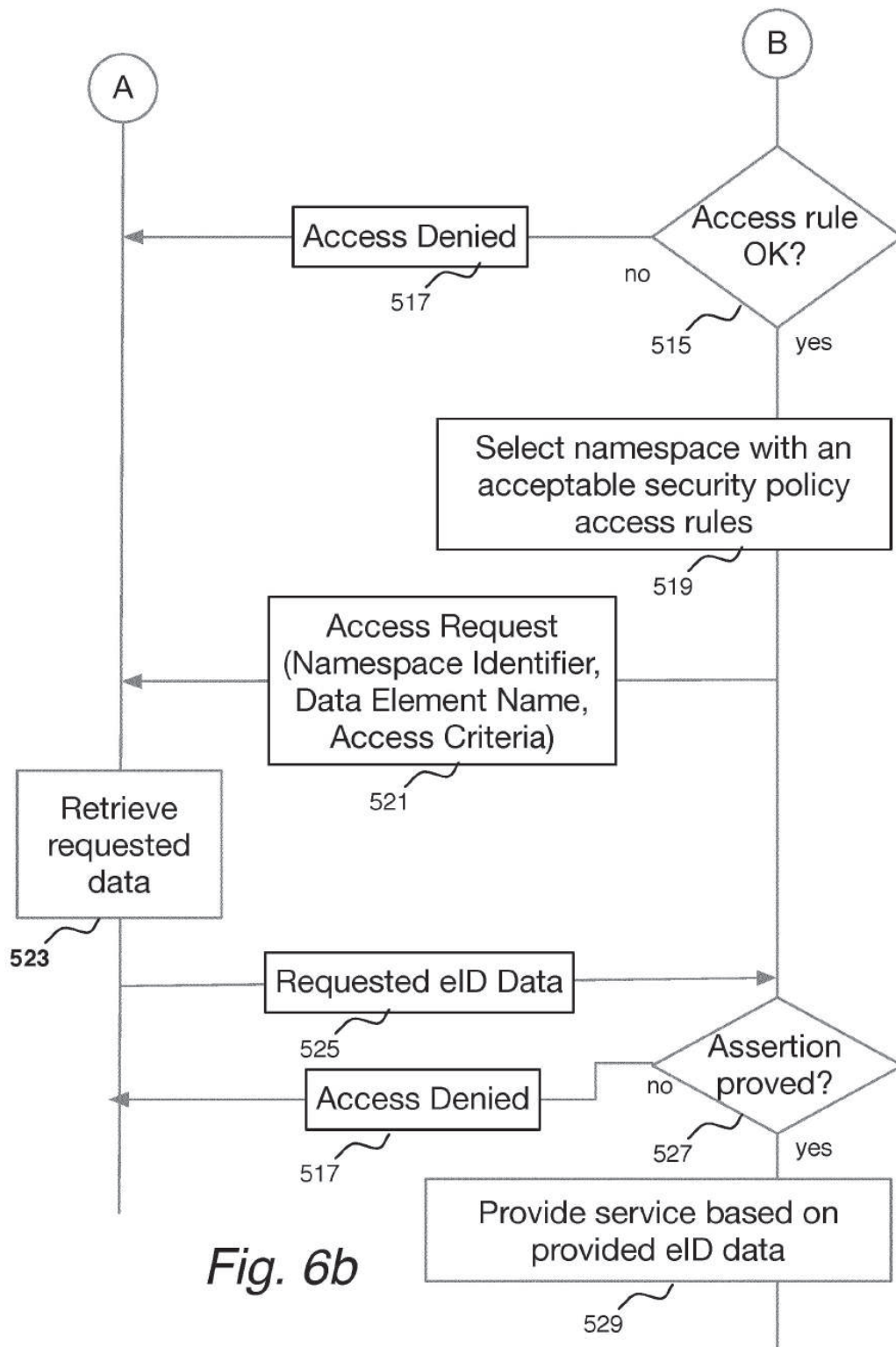


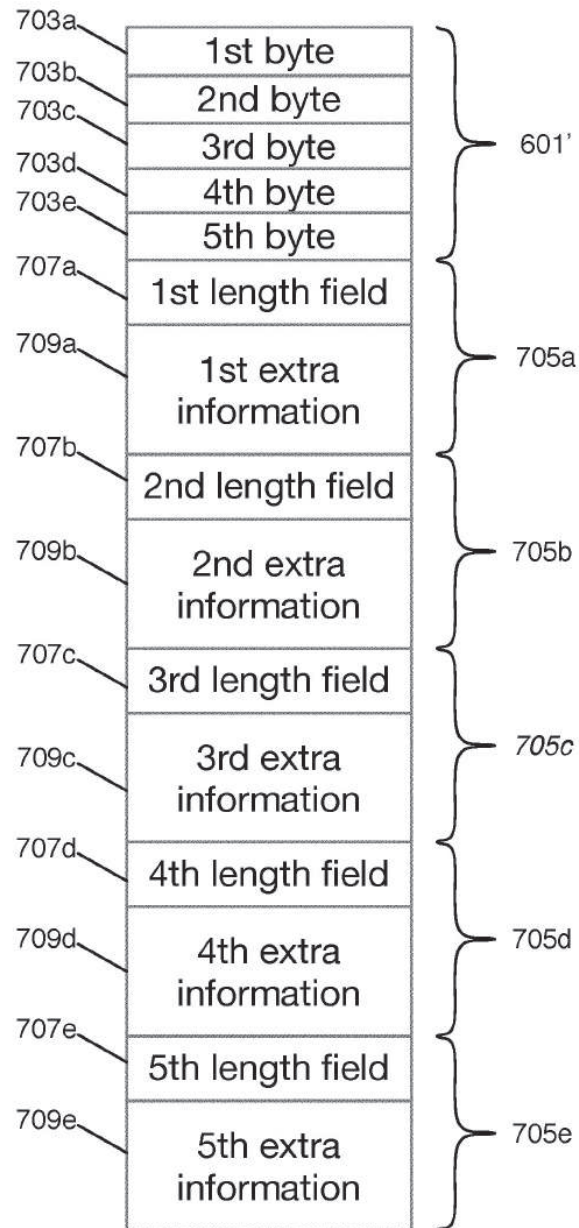
Fig. 6a

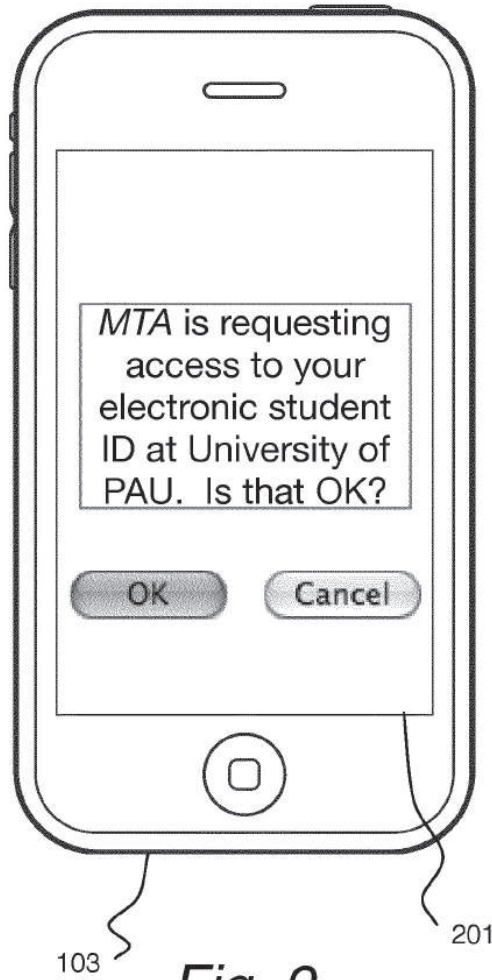
*Fig. 6b*

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

601

Fig. 7

*Fig. 8*

*Fig. 9*

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

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

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

12 November 2020

Date of mailing of the international search report

20/11/2020

Name and mailing address of the ISA/

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

Authorized officer

Nicoli, Félix

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/076906

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2020/076906

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016294831 A1	06-10-2016	AU 2016242966 A1	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



(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.

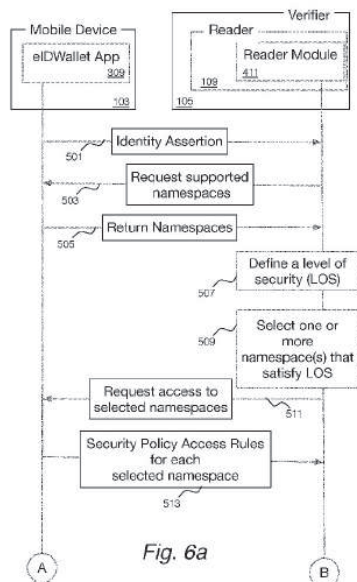


Fig. 6a

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

BACKGROUND OF THE INVENTION

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

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

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

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

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

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

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

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

SUMMARY

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Another aspect of the invention is a mobile device comprising:

a processor; and

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

receive a list of selected namespaces from a reader;

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

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

receive a request for supported namespaces from a reader;

transmit a list of supported name spaces to the reader.

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

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

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

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

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

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

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

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

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

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

- operating the reader to:

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

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

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

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

BRIEF DESCRIPTION OF THE DRAWINGS

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

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

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

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

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

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

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

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

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

DETAILED DESCRIPTION OF THE INVENTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

where

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

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

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

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

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

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

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

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

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

[0076] We Claim:

CLAIMS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- operating the reader to:

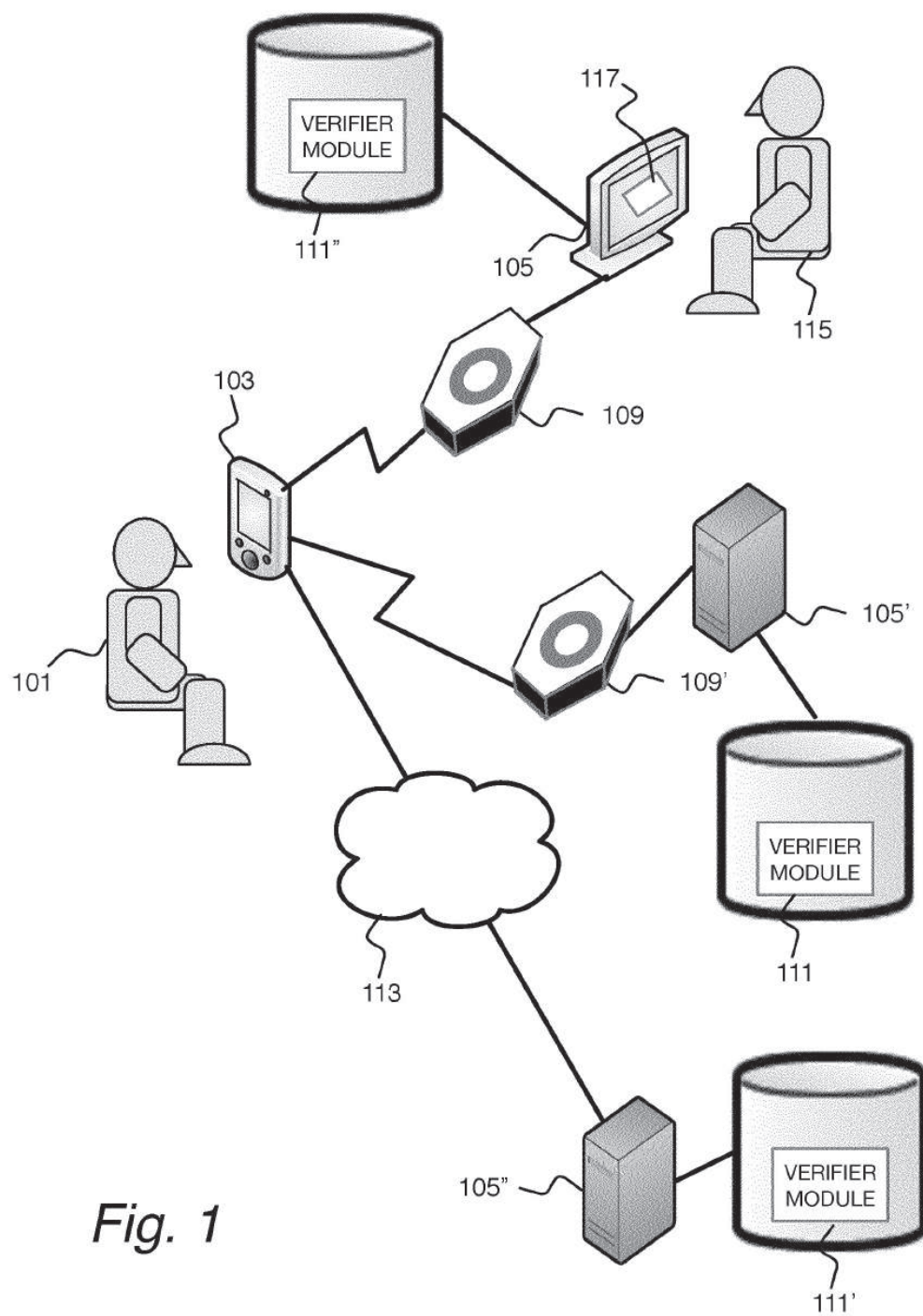
- determine for which of the candidate namespaces the reader can satisfy the security policy of the namespace; and

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

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

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

1/9

*Fig. 1*

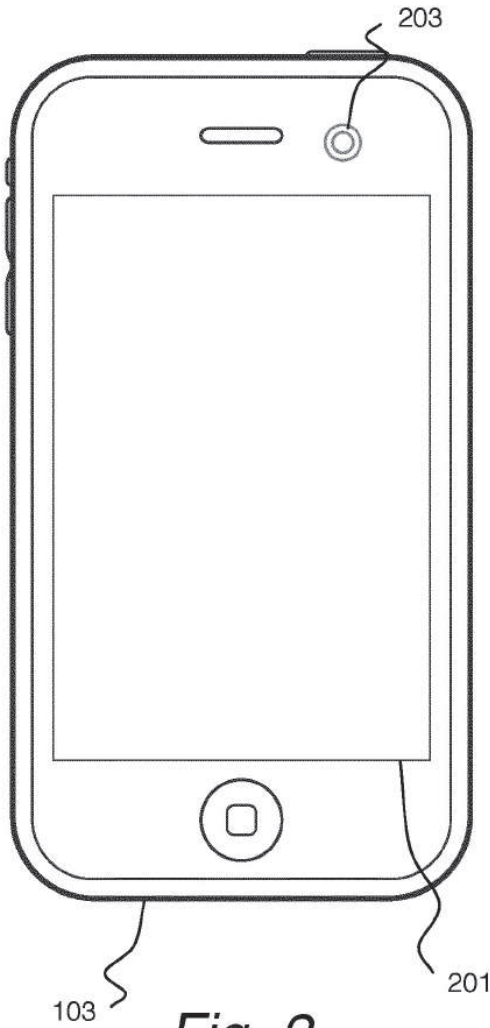


Fig. 2

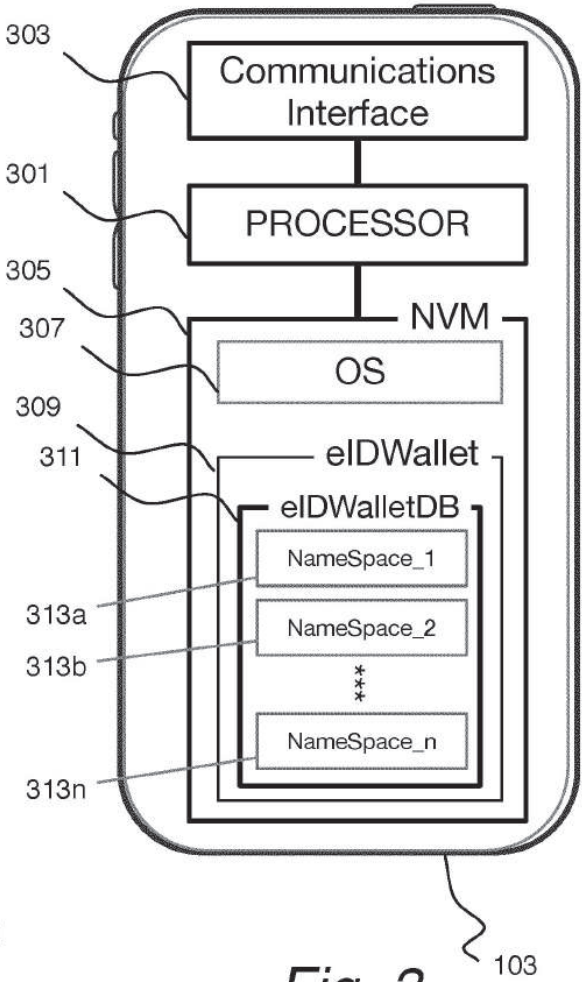
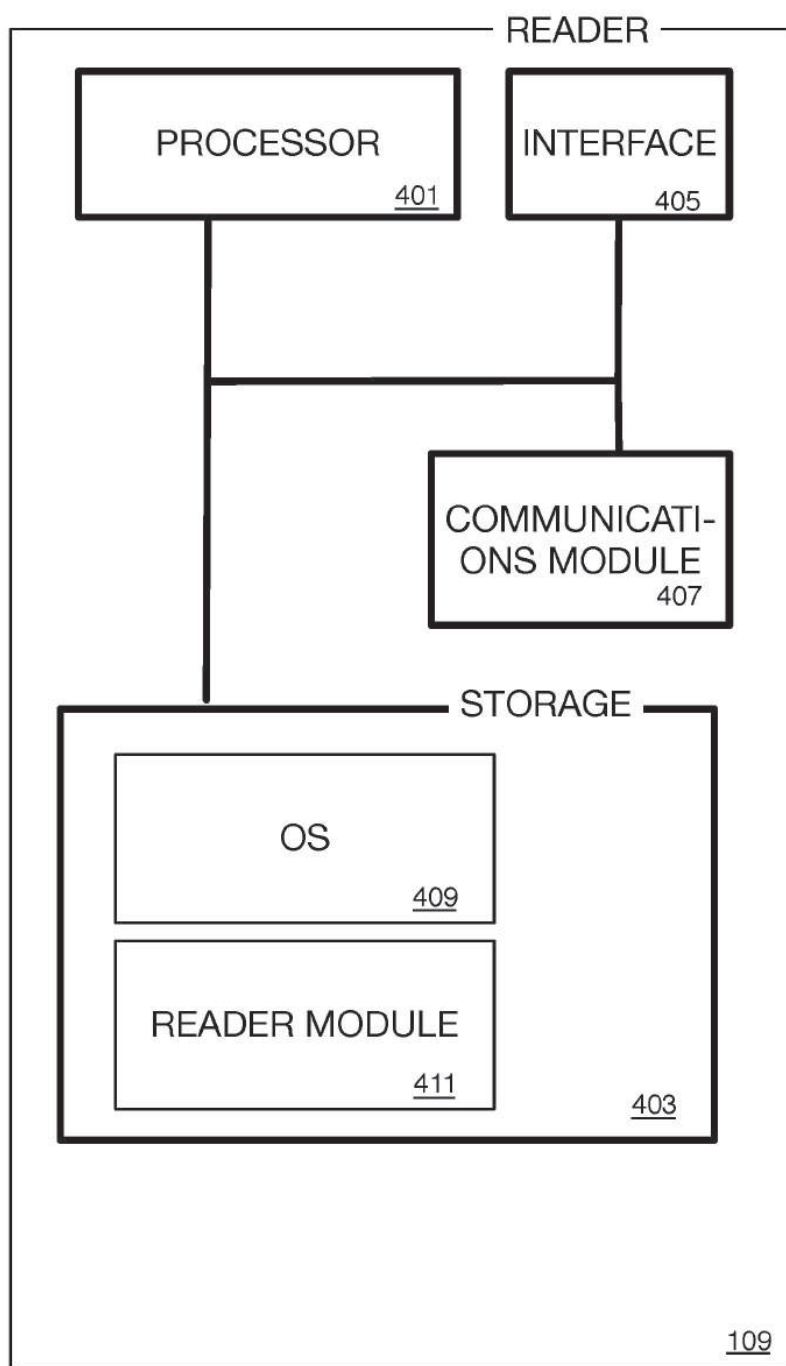
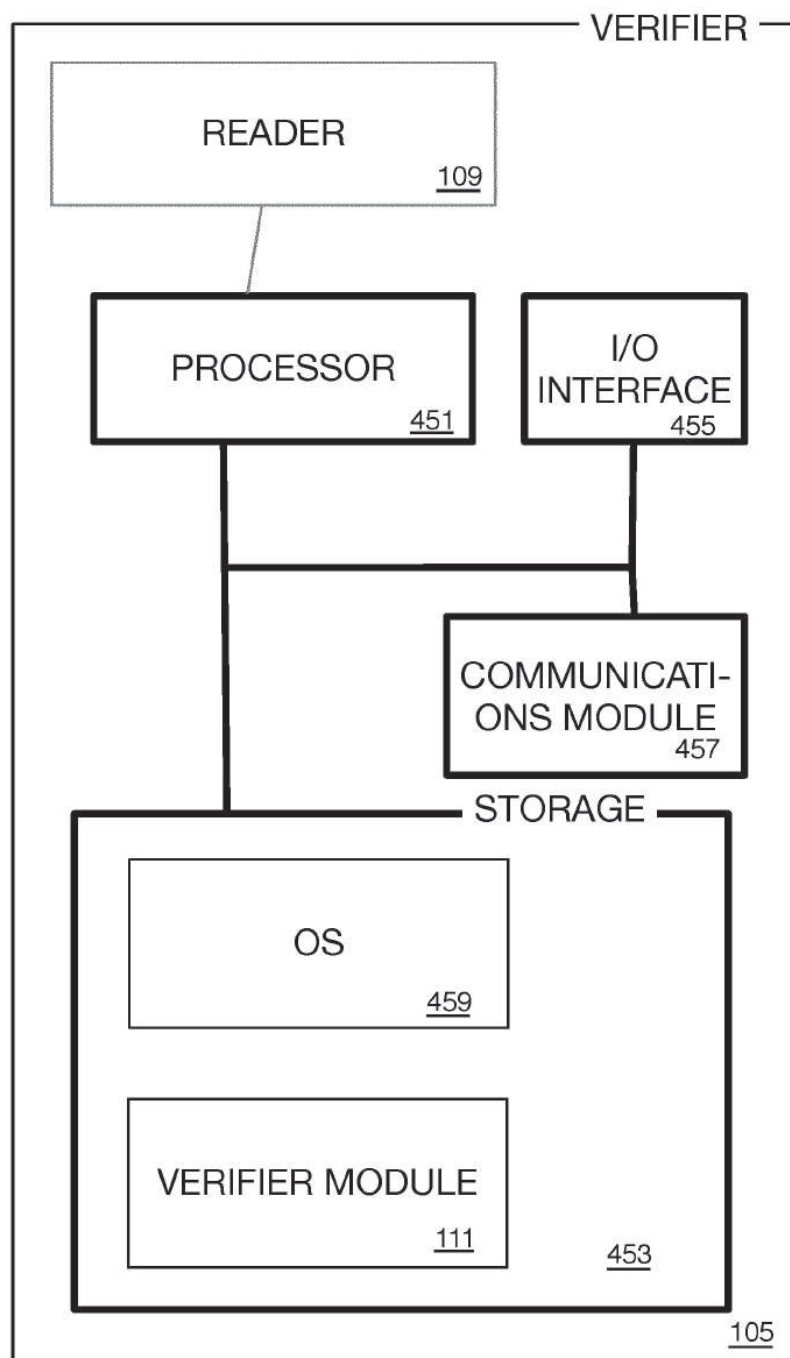


Fig. 3

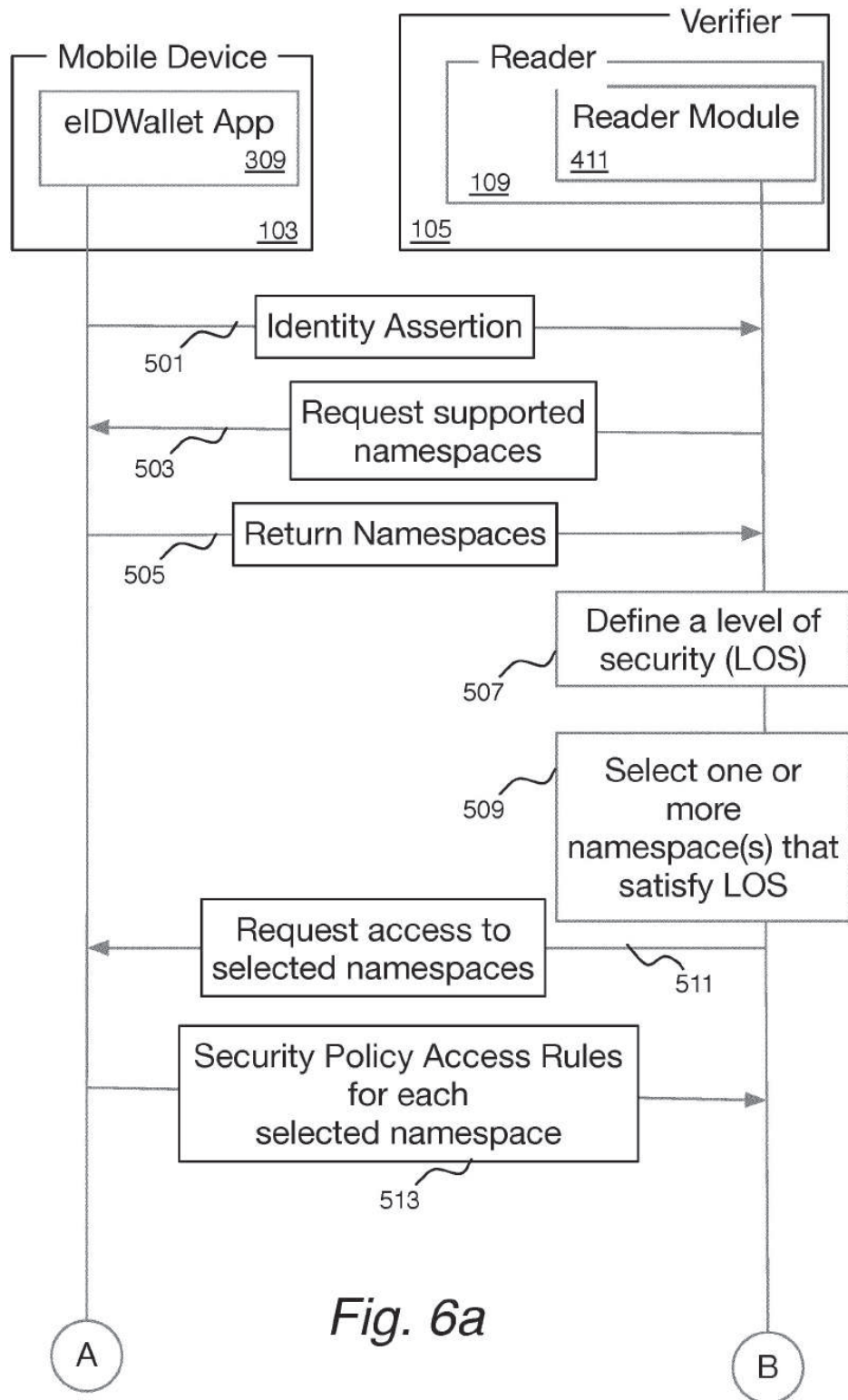
3/9

*Fig. 4*

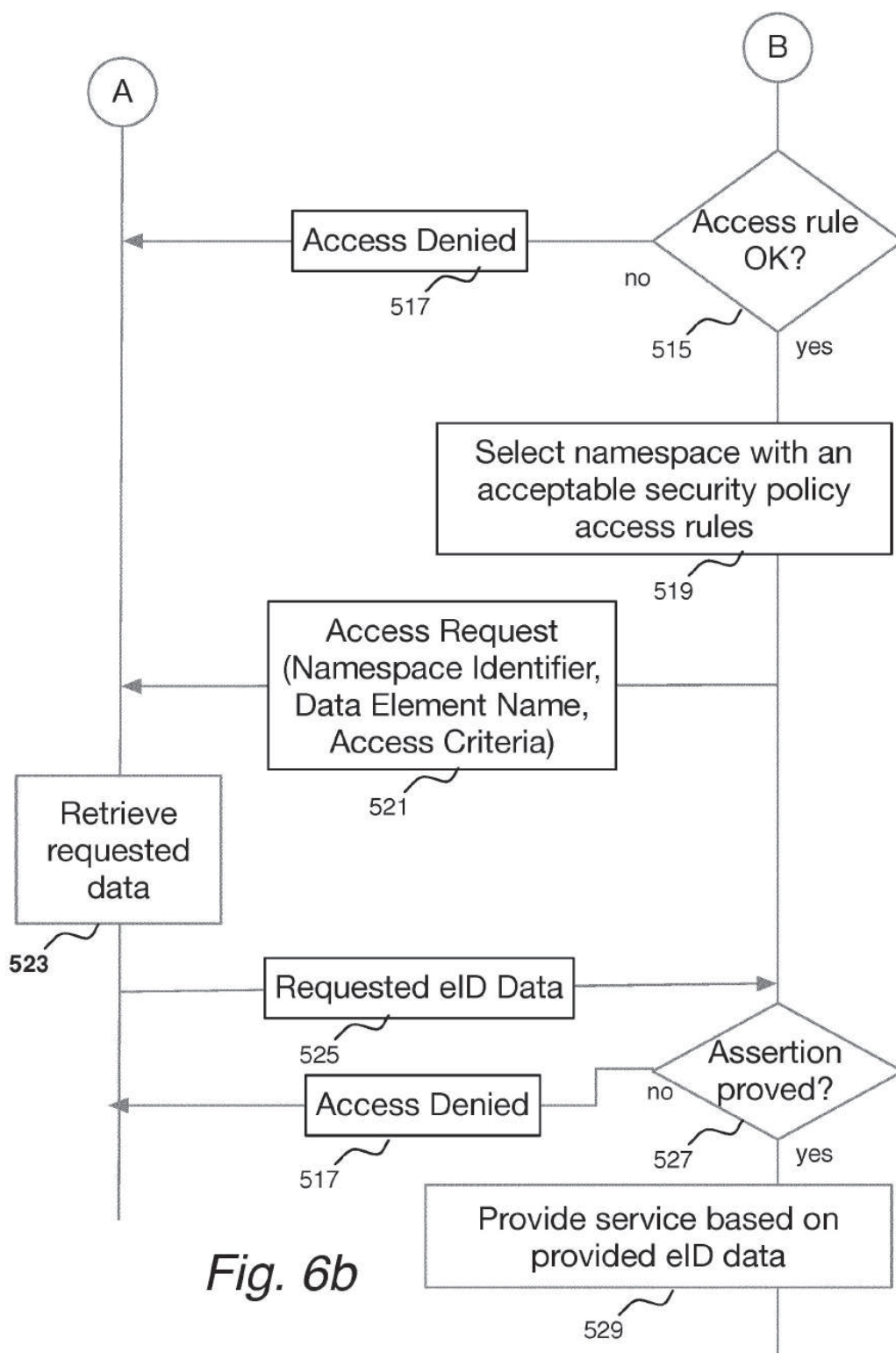
4/9

*Fig. 5*

5/9



6/9



7/9

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

601

Fig. 7

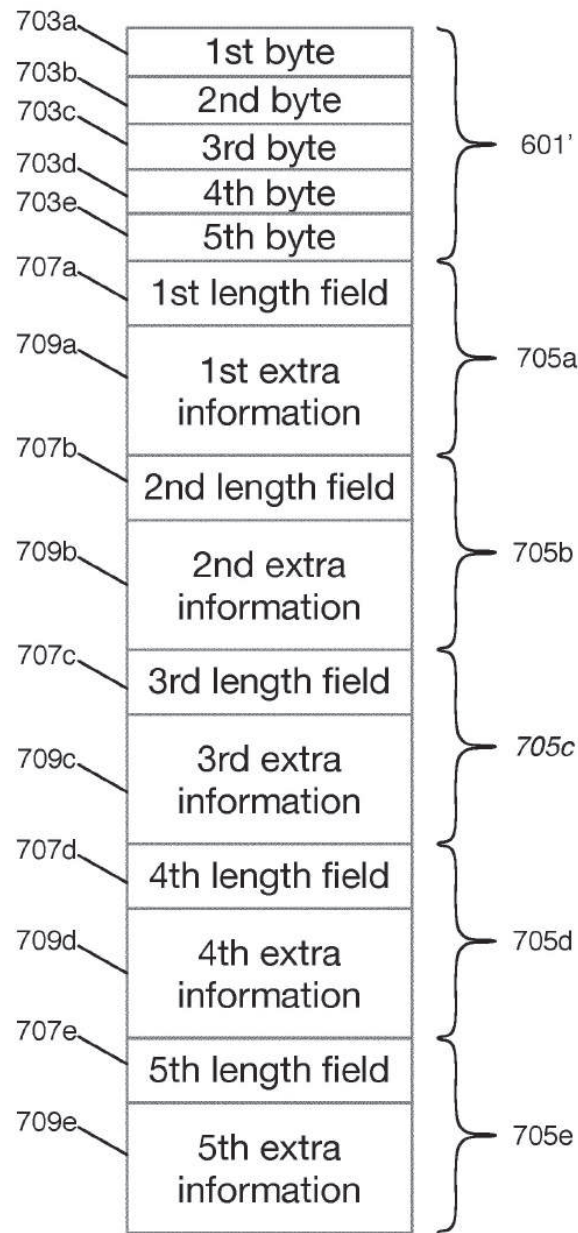
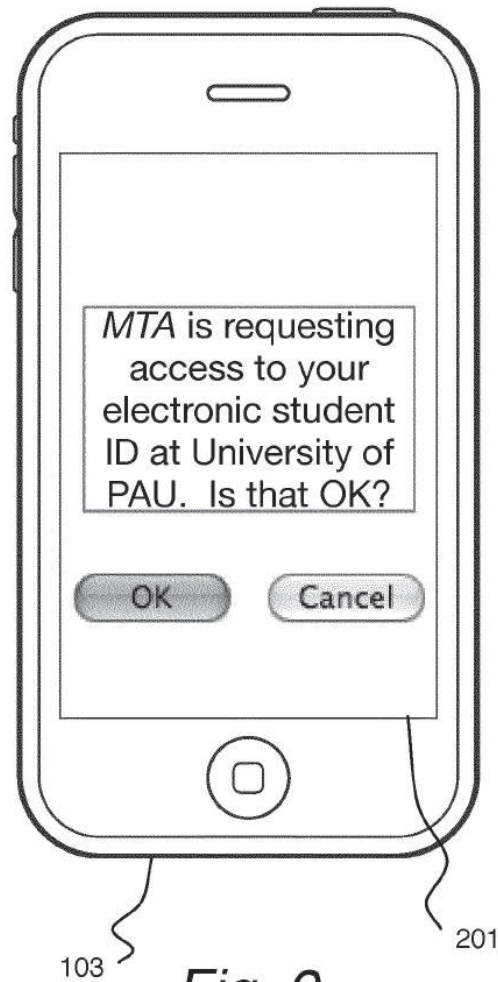


Fig. 8

9/9

*Fig. 9*

PATENT COOPERATION TREATY

From the RECEIVING OFFICE

PCT

To:

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

NOTIFICATION OF THE INTERNATIONAL
APPLICATION NUMBER AND OF THE
INTERNATIONAL FILING DATE

(PCT Rule 20.2(c))

Date of mailing
(day/month/year)

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)

Priority date (day/month/year)

18 October 2019 (18-10-2019)

Applicant

THALES DIS FRANCE SA

Title of the invention

1. The applicant is hereby notified that the international application has been accorded the international application number and the international filing date indicated above.

2. The applicant is further notified that the record copy of the international application:



was transmitted to the International Bureau on see above date of mailing



has not yet been transmitted to the International Bureau for the reason indicated below and a copy of this notification has been sent to the International Bureau*:



because the necessary national security clearance has not yet been obtained



because (reason to be specified)

* The International Bureau monitors the transmittal of the record copy by the receiving Office and will notify the applicant (with Form PCT/IB/301) of its receipt. Should the record copy not have been received by the expiration of 14 months from the priority date, the International Bureau will notify the applicant (Rule 22.1(c)).

Name and mailing address of the Receiving Office



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

Authorized officer

Koestel, Gilbert
00 31 70 340 3544
2288 EE Rijswijk NL

PCT REQUEST

(Original in Electronic Form)

0	For receiving Office use only	
0-1	International Application No.	PCT/EP2020/076906
0-2	International Filing Date	25 SEP 2020 (25.09.2020)
0-3	Name of receiving Office and "PCT International Application"	RO/EP
0-4	Form PCT/RO/101 PCT Request	
0-4-1	Prepared Using	PCT Online Filing Version 3.51.000.268e MT/FOP 20141031/0.20.5.24
0-5	Petition The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	Receiving Office (specified by the applicant)	European Patent Office (EPO) (RO/EP)
0-7	Applicant's or agent's file reference	GMT4110 WO/YL
I	Title of Invention	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
II	Applicant	
II-1	This person is	Applicant only
II-2	Applicant for	All designated States
II-4	Name	THALES DIS FRANCE SA
II-5	Address	6, rue de la Verrerie 92190 MEUDON France
II-6	State of nationality	FR
II-7	State of residence	FR
III-1	Applicant and/or inventor	
III-1-1	This person is	Inventor only
III-1-3	Inventor for	All designated States
III-1-4	Name (LAST, First)	FAHER, Mourad
III-1-5	Address	THALES DIS FRANCE SA Intellectual Property Department 6 Rue de la Verrerie 92190 MEUDON France

PCT REQUEST

(Original in Electronic Form)

III-2	Applicant and/or inventor	
III-2-1	This person is	Inventor only
III-2-3	Inventor for	All designated States
III-2-4	Name (LAST, First)	BAYLE, Carole
III-2-5	Address	THALES DIS FRANCE SA Intellectual Property Department 6 Rue de la Verrerie 92190 MEUDON France
IV-1	Agent or common representative; or address for correspondence	
	The person identified below is hereby/ has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	Agent
IV-1-1	Name (LAST, First)	LOTAUT, Yacine
IV-1-2	Address	THALES DIS FRANCE SA Intellectual Property Department 6 Rue de la Verrerie 92190 MEUDON France
IV-1-3	Telephone No.	+33 1 55 01 63 98
IV-1-5	e-mail	intellectual.property@thalesgroup.com
IV-1-5(a)	E-mail authorization The receiving Office, the International Searching Authority, the International Bureau and the International Preliminary Examining Authority are authorized to use this e-mail address, if the Office or Authority so wishes, to send notifications issued in respect of this international application:	exclusively in electronic form (no paper notifications will be sent)
V	DESIGNATIONS	
V-1	The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.	
VI-1	Priority claim of earlier regional application	
VI-1-1	Filing date	18 October 2019 (18.10.2019)
VI-1-2	Number	19306357.5
VI-1-3	Regional Office	EP
VI-2	Priority document request	
	The International Bureau is requested to obtain from a digital library a certified copy of the earlier application(s) identified above as item(s), using, where applicable, the access code(s) indicated:	VI-1 Access code: 3977
VI-3	Incorporation by reference : where an element of the international application referred to in Article 11(1)(iii)(d) or (e) or a part of the description, claims or drawings referred to in Rule 20.5(a), or an element or part of the description, claims or drawings referred to in Rule 20.5bis(a) is not otherwise contained in this international application but is completely contained in an earlier application whose priority is claimed on the date on which one or more elements referred to in Article 11(1)(iii) were first received by the receiving Office, that element or part is, subject to confirmation under Rule 20.6, incorporated by reference in this international application for the purposes of Rule 20.6.	

PCT REQUEST

(Original in Electronic Form)

VII-1	International Searching Authority Chosen	European Patent Office (EPO) (ISA/EP)	
VII-2	Request to use results of earlier search; reference to that search		
VII-2-1	Filing date	18 October 2019 (18.10.2019)	
VII-2-2	Application Number	19306357.5	
VII-2-3	Country (or regional Office)	EP	
VII-2-4	Statement (Rule 4.12(iii)):	This international application is the same, or substantially the same, as the application in respect of which the earlier search was carried out except, where applicable, that it is filed in a different language.	
VII-2-6	The applicant requests the receiving Office to prepare and transmit to the ISA a copy of the earlier search results (Rule 12bis.1(b) and (d)).		
VIII	Declarations	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	—	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	—	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	—	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	—	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	—	
IX	Check list	Number of sheets	Electronic file(s) attached
IX-1	Request (including declaration sheets)	4	✓
IX-2	Description	17	✓
IX-3	Claims	4	✓
IX-4	Abstract	1	✓
IX-5	Drawings	9	✓
IX-6a	Sequence listing part of the description (also to be used for the purposes of international search)	—	—
IX-7	TOTAL	35	
	Accompanying Items	Paper document(s) attached	Electronic file(s) attached
IX-8	Fee calculation sheet	—	✓
IX-20	Figure of the drawings which should accompany the abstract	6a	
IX-21	Language of filing of the international application	English	

PCT REQUEST

(Original in Electronic Form)

X-1	Signature of applicant, agent or common representative	(PKCS7 Digital Signature)
X-1-1	Name (LAST, First)	LOTAUT, Yacine
X-1-3	Capacity (if such capacity is not obvious from reading the request)	(Representative)

FOR RECEIVING OFFICE USE ONLY

10-1	Date of actual receipt of the purported international application	25 SEP 2020 (25.09.2020)
10-2	Drawings:	✓
10-2-1	Received	
10-2-2	No received	
10-3	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application	
10-4	Date of timely receipt of the required corrections under PCT Article 11(2)	
10-5	International Searching Authority	ISA/EP
10-6	Transmittal of search copy delayed until search fee is paid	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	Date of receipt of the record copy by the International Bureau	
-------------	--	--



Acknowledgement of receipt

We hereby acknowledge receipt of your request for the processing of an international application according to the Patent Cooperation Treaty as follows:

Submission number	9054602	
PCT application number	PCT/EP2020/076906	
Date of receipt	25 September 2020	
Receiving Office	European Patent Office, The Hague	
Your reference	GMT4110 WO/YL	
Applicant	THALES DIS FRANCE SA	
Number of applicants	1	
Country	FR	
Title	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES	
Documents submitted	eolf-pkda.xml eolf-appb.xml eolf-vlog.xml eolf-appb-P000001.pdf (9 p.)	eolf-requ.xml eolf-fees.xml eolf-othd-000001.pdf (22 p.)
Submitted by	CN=Yacine Lotaut 34912	
Method of submission	Online	
Date and time receipt generated	25 September 2020, 12:14 (CEST)	
Message Digest	31:DC:2D:94:F7:E3:E2:30:6E:F7:97:A7:D4:96:49:07:53:6A:89:0E	

/European Patent Office/

DAS access code

The access code generated for this application and used to retrieve the priority documents from WIPO's Digital Access Service (DAS) is indicated in the document appended to this acknowledgement of receipt. Please note that the appended document is non-public and will not be published.

/European Patent Office/

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

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.

SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES

BACKGROUND OF THE INVENTION

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

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

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

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

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

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

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

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

SUMMARY

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Another aspect of the invention is a mobile device comprising:

a processor; and

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

receive a list of selected namespaces from a reader;

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

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

receive a request for supported namespaces from a reader;

transmit a list of supported name spaces to the reader.

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

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

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

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

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

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

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

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

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

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

- operating the reader to:

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

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

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

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

BRIEF DESCRIPTION OF THE DRAWINGS

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

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

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

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

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

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

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

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

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

DETAILED DESCRIPTION OF THE INVENTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

where

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

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

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

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

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

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

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

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

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

[0076] We Claim:

PCT (ANNEX - FEE CALCULATION SHEET)

(Original in Electronic Form)

(This sheet is not part of and does not count as a sheet of the international application)

0	For receiving Office use only			
0-1	International Application No.	PCT/EP2020/076906		
0-2	Date stamp of the receiving Office	25 SEP 2020 (25.09.2020)		
0-4	Form PCT/RO/101 (Annex)			
0-4-1	PCT Fee Calculation Sheet Prepared Using	PCT Online Filing Version 3.51.000.268e MT/FOP 20141031/0.20.5.24		
0-9	Applicant's or agent's file reference		GMT4110 WO/YL	
2	Applicant		THALES DIS FRANCE SA	
12	Calculation of prescribed fees	Fee amount/multiplier	Total amounts (EUR)	
12-1	Transmittal fee T	↔	135	
12-2-1	Search fee S	↔	1775	
12-2-2	International search to be carried out by	EP		
12-3	International filing fee (first 30 sheets) i1	1217		
12-4	Remaining sheets	5		
12-5	Additional amount (X)	14		
12-6	Total additional amount i2	70		
12-7	i1 + i2 = i	1287		
12-12	Electronic Filing reduction (Image) R	-183		
12-13	Total International filing fee (i-R) I	↔	1104	
12-14	Fee for priority document Number of priority documents requested	0		
12-15	Fee per document (X)	105		
12-16	Total priority document fee: P	↔		
12-17	Fee for restoration of priority rights RP Number of requests for restoration of priority rights	0		
	Total amount of fees for restoration of priority rights			
12-19	TOTAL FEES PAYABLE (T+S+I+P+RP)	↔	3014	
12-21	Mode of payment	Authorization to charge deposit or current account		
12-22	Deposit or current account instructions			
	The receiving Office	European Patent Office (EPO) (RO/EP)		
12-22-1	Authorization to charge the total fees indicated above	✓		
12-22-2	Authorization to charge any deficiency or credit any overpayment in the total fees indicated above	✓		
12-22-3	Authorization to charge the fee for priority document	✓		

PCT (ANNEX - FEE CALCULATION SHEET)

(Original in Electronic Form)

(This sheet is not part of and does not count as a sheet of the international application)

12-23	Deposit or current account No.	28040183
12-24	Date	25 September 2020 (25.09.2020)
12-25	Name and signature	THALES DIS FRANCE SA, /Yacine Lotaut/

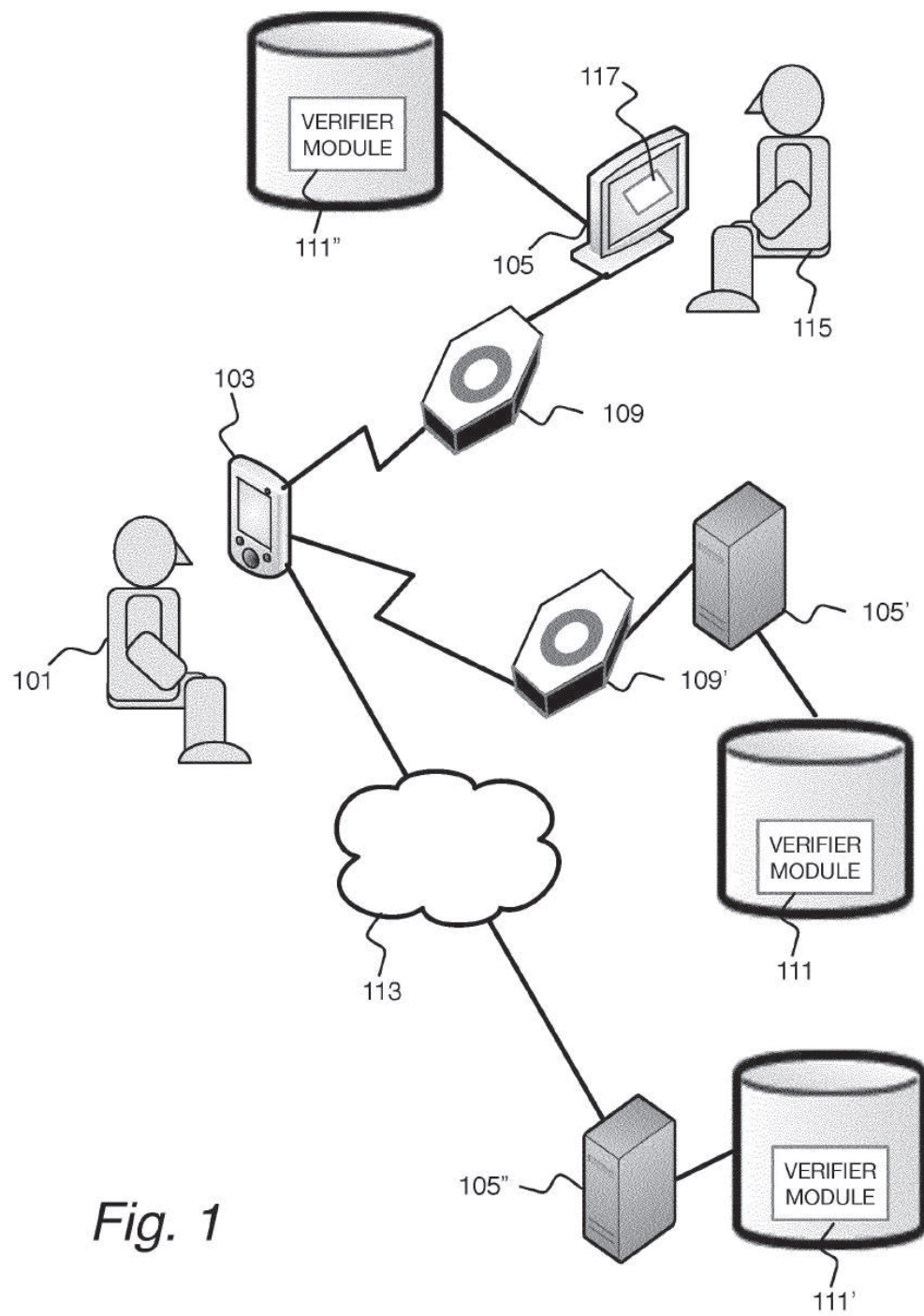


Fig. 1

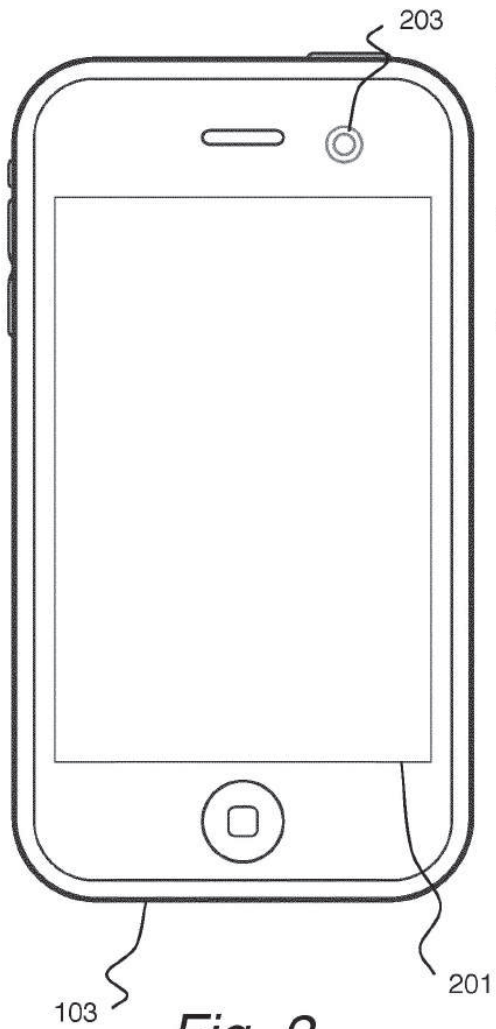


Fig. 2

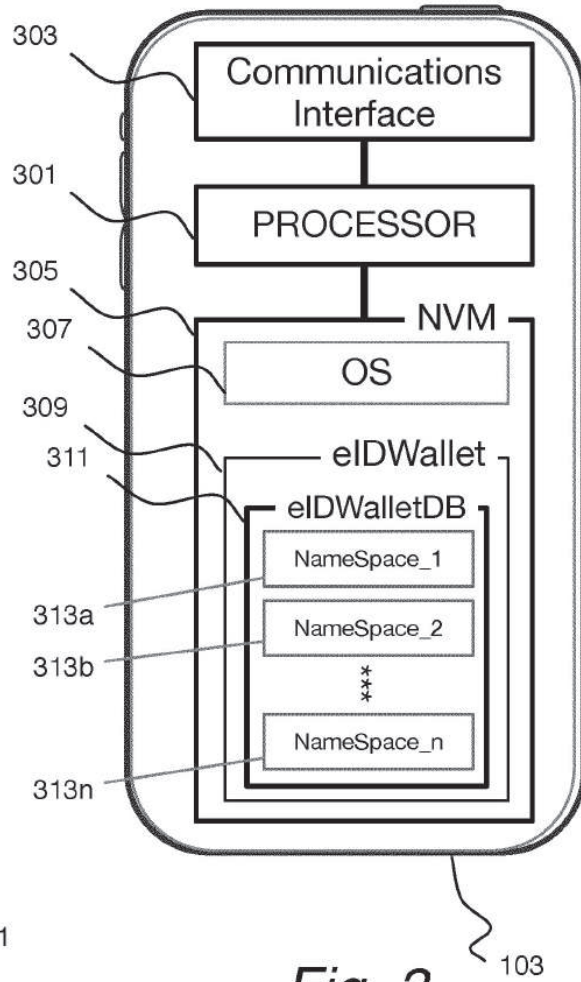
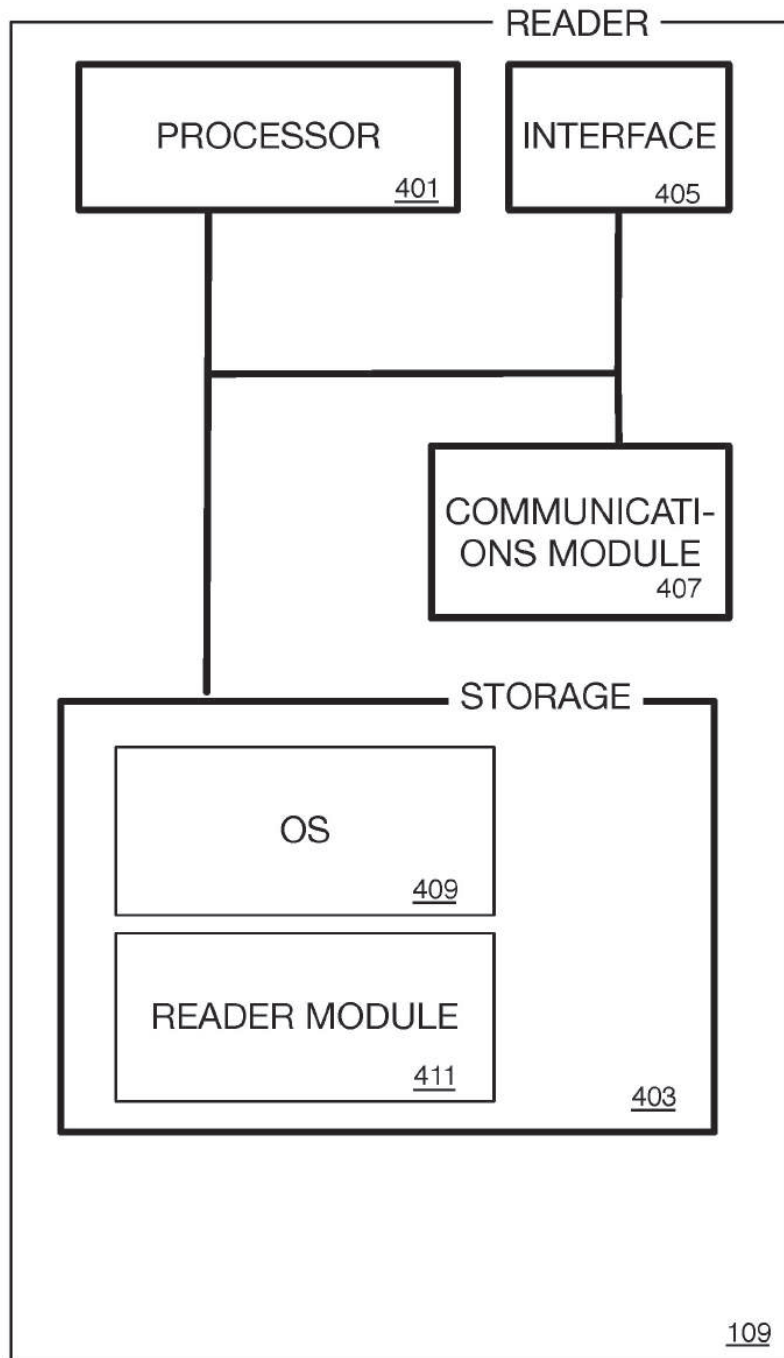
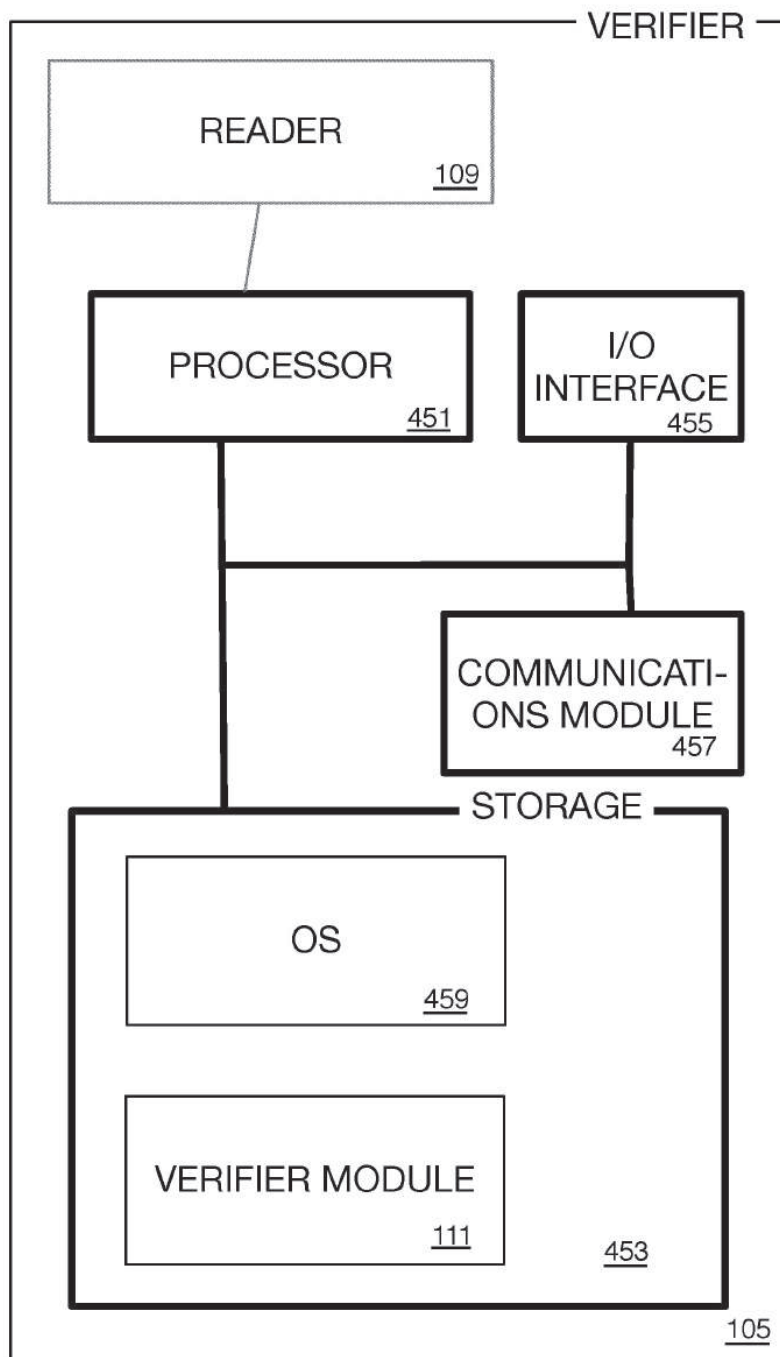
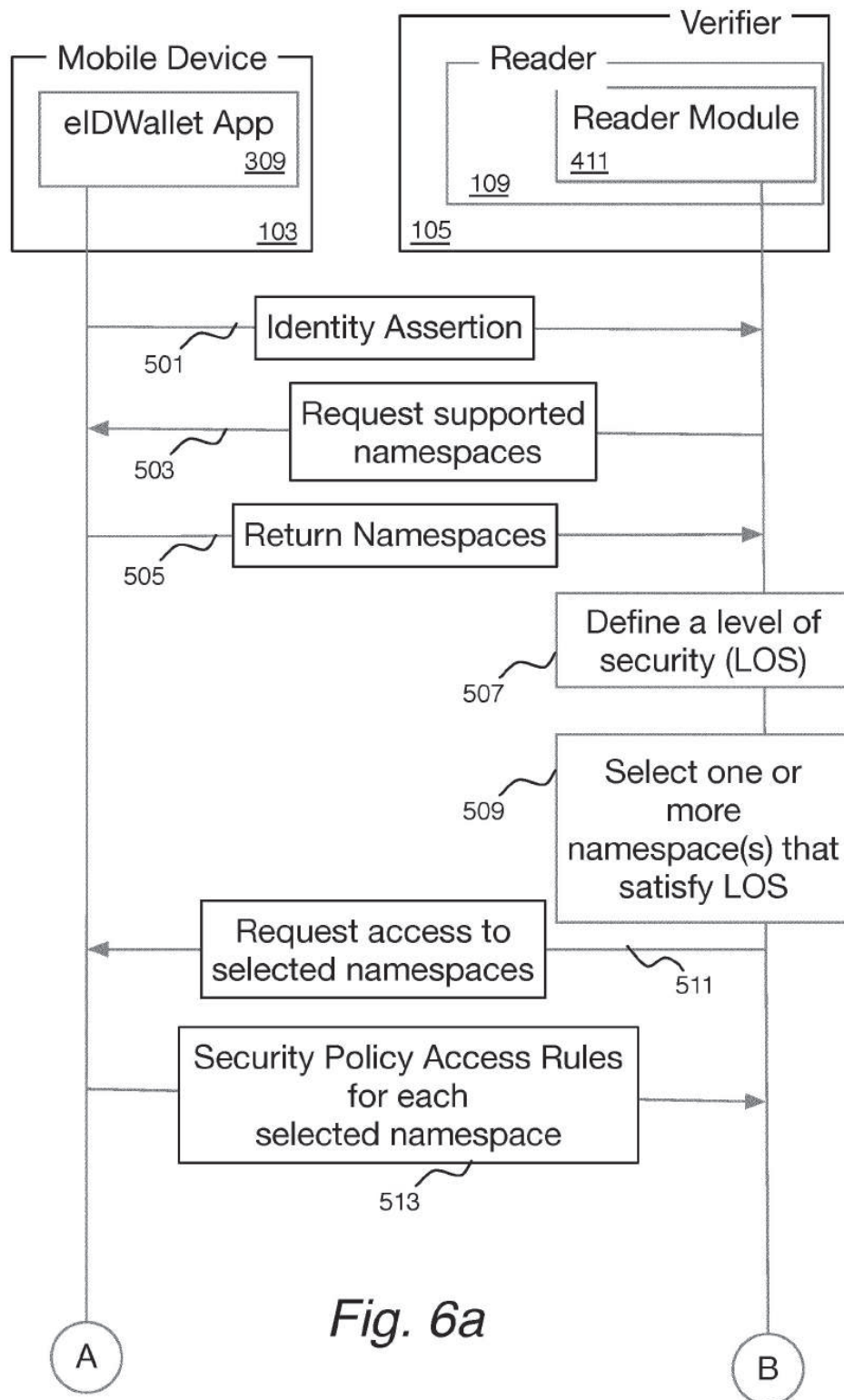
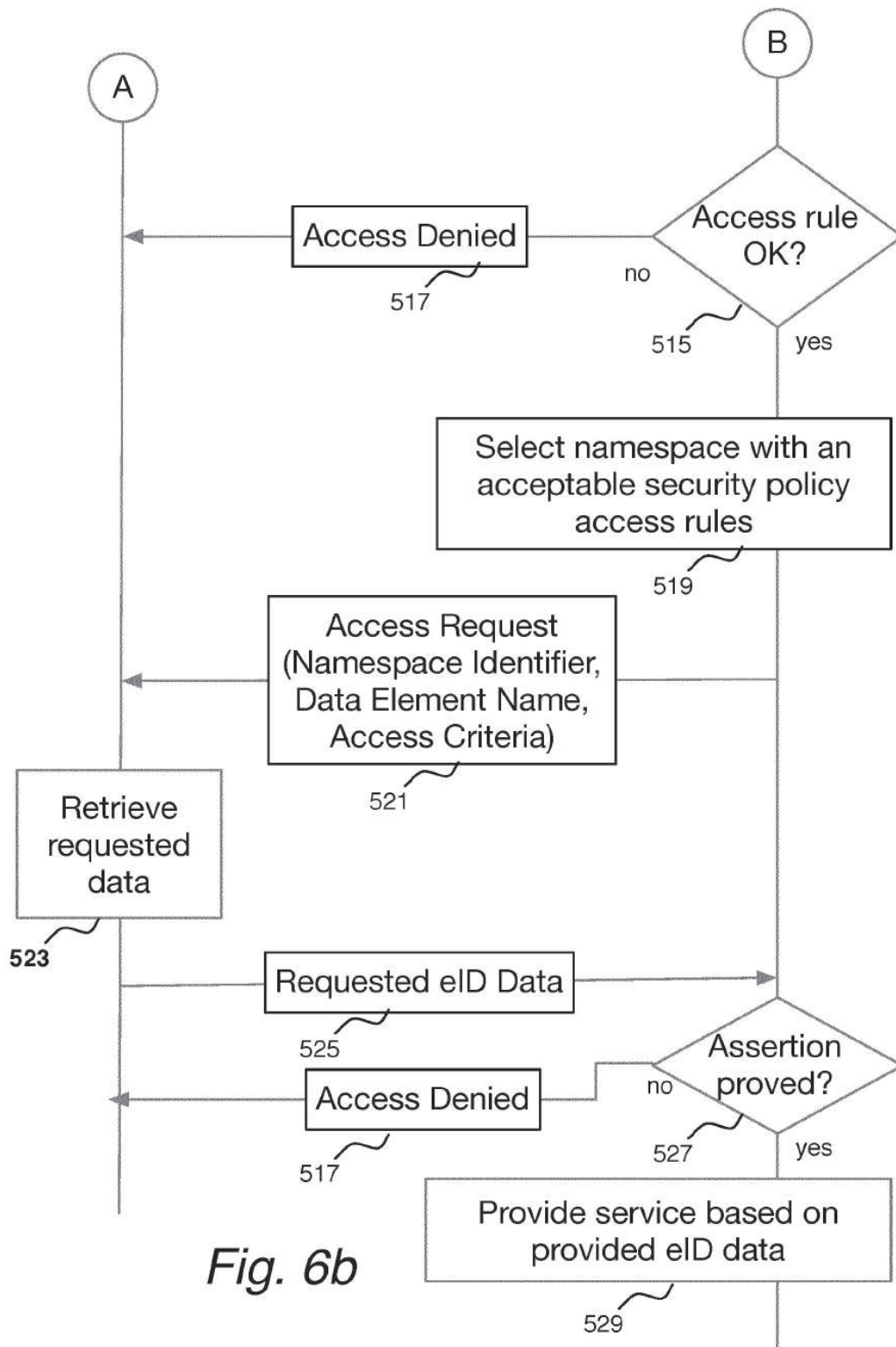


Fig. 3

*Fig. 4*

*Fig. 5*

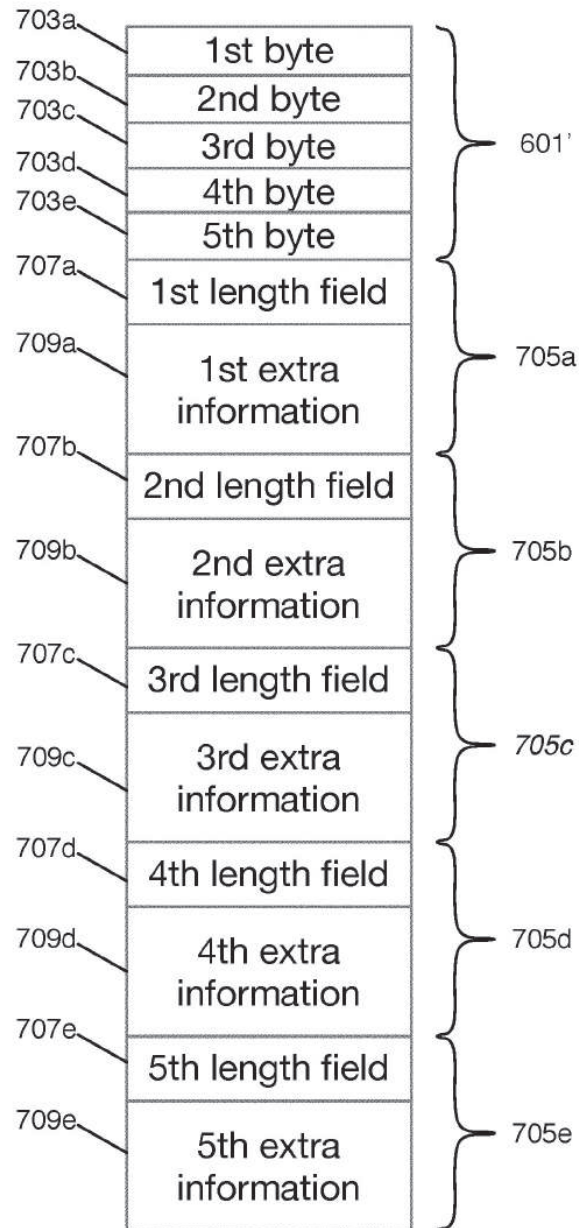


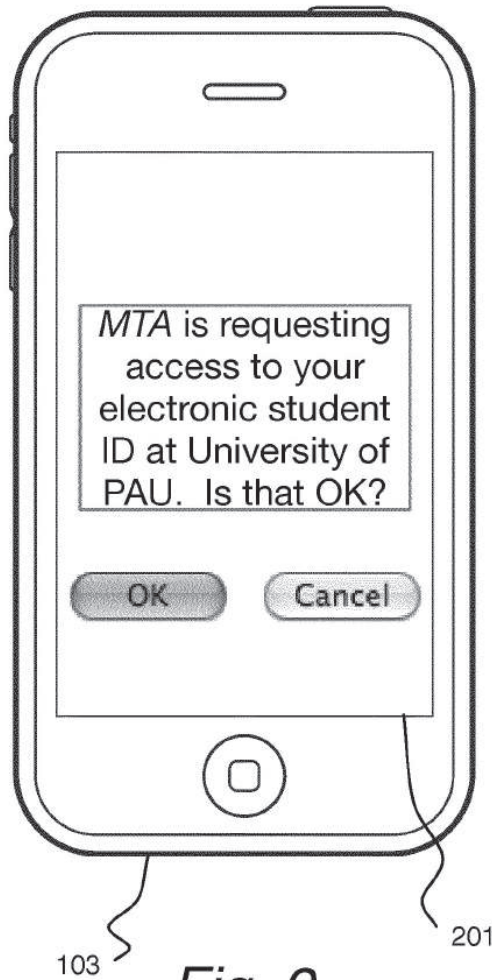
*Fig. 6b*

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

601

Fig. 7

*Fig. 8*

*Fig. 9*

PCT REQUEST

(Original in Electronic Form)

0	For receiving Office use only	
0-1	International Application No.	PCT/EP2020/076906
0-2	International Filing Date	25 SEP 2020 (25.09.2020)
0-3	Name of receiving Office and "PCT International Application"	RO/EP
0-4	Form PCT/RO/101 PCT Request	
0-4-1	Prepared Using	PCT Online Filing Version 3.51.000.268e MT/FOP 20141031/0.20.5.24
0-5	Petition The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	Receiving Office (specified by the applicant)	European Patent Office (EPO) (RO/EP)
0-7	Applicant's or agent's file reference	GMT4110 WO/YL
I	Title of Invention	SECURITY MECHANISM FOR NAMESPACES USED IN ELECTRONIC IDENTIFICATION ON MOBILE DEVICES
II	Applicant	
II-1	This person is	Applicant only
II-2	Applicant for	All designated States
II-4	Name	THALES DIS FRANCE SA
II-5	Address	6, rue de la Verrerie 92190 MEUDON France
II-6	State of nationality	FR
II-7	State of residence	FR
III-1	Applicant and/or inventor	
III-1-1	This person is	Inventor only
III-1-3	Inventor for	All designated States
III-1-4	Name (LAST, First)	FAHER, Mourad
III-1-5	Address	THALES DIS FRANCE SA Intellectual Property Department 6 Rue de la Verrerie 92190 MEUDON France

PCT REQUEST

(Original in Electronic Form)

III-2	Applicant and/or inventor	
III-2-1	This person is	Inventor only
III-2-3	Inventor for	All designated States
III-2-4	Name (LAST, First)	BAYLE, Carole
III-2-5	Address	THALES DIS FRANCE SA Intellectual Property Department 6 Rue de la Verrerie 92190 MEUDON France
IV-1	Agent or common representative; or address for correspondence	
	The person identified below is hereby/ has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	Agent
IV-1-1	Name (LAST, First)	LOTAUT, Yacine
IV-1-2	Address	THALES DIS FRANCE SA Intellectual Property Department 6 Rue de la Verrerie 92190 MEUDON France
IV-1-3	Telephone No.	+33 1 55 01 63 98
IV-1-5	e-mail	intellectual.property@thalesgroup.com
IV-1-5(a)	E-mail authorization The receiving Office, the International Searching Authority, the International Bureau and the International Preliminary Examining Authority are authorized to use this e-mail address, if the Office or Authority so wishes, to send notifications issued in respect of this international application:	exclusively in electronic form (no paper notifications will be sent)
V	DESIGNATIONS	
V-1	The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.	
VI-1	Priority claim of earlier regional application	
VI-1-1	Filing date	18 October 2019 (18.10.2019)
VI-1-2	Number	19306357.5
VI-1-3	Regional Office	EP
VI-2	Priority document request	
	The International Bureau is requested to obtain from a digital library a certified copy of the earlier application(s) identified above as item(s), using, where applicable, the access code(s) indicated:	VI-1 Access code: 3977
VI-3	Incorporation by reference : where an element of the international application referred to in Article 11(1)(iii)(d) or (e) or a part of the description, claims or drawings referred to in Rule 20.5(a), or an element or part of the description, claims or drawings referred to in Rule 20.5bis(a) is not otherwise contained in this international application but is completely contained in an earlier application whose priority is claimed on the date on which one or more elements referred to in Article 11(1)(iii) were first received by the receiving Office, that element or part is, subject to confirmation under Rule 20.6, incorporated by reference in this international application for the purposes of Rule 20.6.	

PCT REQUEST

(Original in Electronic Form)

VII-1	International Searching Authority Chosen	European Patent Office (EPO) (ISA/EP)	
VII-2	Request to use results of earlier search; reference to that search		
VII-2-1	Filing date	18 October 2019 (18.10.2019)	
VII-2-2	Application Number	19306357.5	
VII-2-3	Country (or regional Office)	EP	
VII-2-4	Statement (Rule 4.12(iii)):	This international application is the same, or substantially the same, as the application in respect of which the earlier search was carried out except, where applicable, that it is filed in a different language.	
VII-2-6	The applicant requests the receiving Office to prepare and transmit to the ISA a copy of the earlier search results (Rule 12bis.1(b) and (d)).		
VIII	Declarations	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	—	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	—	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	—	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	—	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	—	
IX	Check list	Number of sheets	Electronic file(s) attached
IX-1	Request (including declaration sheets)	4	✓
IX-2	Description	17	✓
IX-3	Claims	4	✓
IX-4	Abstract	1	✓
IX-5	Drawings	9	✓
IX-6a	Sequence listing part of the description (also to be used for the purposes of international search)	—	—
IX-7	TOTAL	35	
	Accompanying Items	Paper document(s) attached	Electronic file(s) attached
IX-8	Fee calculation sheet	—	✓
IX-20	Figure of the drawings which should accompany the abstract	6a	
IX-21	Language of filing of the international application	English	

PCT REQUEST

(Original in Electronic Form)

X-1	Signature of applicant, agent or common representative	(PKCS7 Digital Signature)
X-1-1	Name (LAST, First)	LOTAUT, Yacine
X-1-3	Capacity (if such capacity is not obvious from reading the request)	(Representative)

FOR RECEIVING OFFICE USE ONLY

10-1	Date of actual receipt of the purported international application	25 SEP 2020 (25.09.2020)
10-2	Drawings:	✓
10-2-1	Received	
10-2-2	No received	
10-3	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application	
10-4	Date of timely receipt of the required corrections under PCT Article 11(2)	
10-5	International Searching Authority	ISA/EP
10-6	Transmittal of search copy delayed until search fee is paid	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	Date of receipt of the record copy by the International Bureau	
-------------	--	--