(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
02 January 2025 (02.01.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/002794 A1

(51) International Patent Classification:
*H04W 12/48* (2021.01) *H04L 9/40* (2022.01)
*H04W 12/126* (2021.01) *H04W 12/069* (2021.01)
*H04W 12/60* (2021.01)

(21) International Application Number:
PCT/EP2024/066109

(22) International Filing Date:
11 June 2024 (11.06.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
23315265.1 29 June 2023 (29.06.2023) EP

(71) Applicant: **THALES DIS FRANCE SAS** [FR/FR]; 6, rue de La Verrerie, 92190 Meudon (FR).

(72) Inventors: **RAGUENET, Alain**; C/O THALES DIS FRANCE SAS, Intellectual Property Department, Avenue du Jujubier, ZI Athelia IV, 13705 La Ciotat (FR). **PHAN, Ly Thanh**; C/O THALES DIS FRANCE SAS, Intellectual Property Department, Avenue du Jujubier, ZI Athelia IV, 13705 La Ciotat (FR). **PAULIAC, Mireille**; C/O THALES DIS FRANCE SAS, Intellectual Property Department, Avenue du Jujubier, ZI Athelia IV, 13705 La Ciotat (FR). **COLLET, Hervé**; C/O THALES DIS FRANCE SAS, Intellectual Property Department, Avenue du Jujubier, ZI Athelia IV, 13705 La Ciotat (FR). **DANY, Vincent**; C/O THALES DIS FRANCE SAS, Intellectual Property Department, Avenue du Jujubier, ZI Athelia IV, 13705 La Ciotat (FR). **GALIMARD, Alexandra**; C/O THALES DIS FRANCE SAS, Intellectual Property Department, Avenue du Jujubier, ZI Athelia IV, 13705 La Ciotat (FR).

(74) Agent: **THOMAS, Christine**; C/O THALES DIS FRANCE SAS, Intellectual Property Department, Avenue du Jujubier, ZI Athelia IV, 13705 La Ciotat (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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).

**Declarations under Rule 4.17:**
— *of inventorship (Rule 4.17(iv))*

**Published:**
— *with international search report (Art. 21(3))*

(54) **Title:** REMOVABLE SECURE ELEMENT HAVING IMPERSONATION PROTECTION

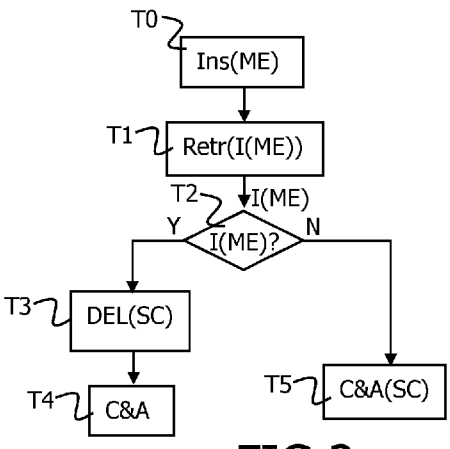



FIG.2

(57) **Abstract:** The present invention relates to a removable secure element having a memory to store at least a universal user identifier, a security context, a list of mobile equipment identifiers in which the removable secure element was previously inserted, said removable secure element being dedicated to be inserted in a mobile equipment compliant with plastic roaming connecting and authenticating automatically the mobile equipment to a serving network using the security context stored in the removable secure element as soon as the universal user identifier stored in the removable secure element is the same as the one associated to the security context on the serving network side, said removable secure element further having an application to monitor an identifier of a mobile equipment in which the removable secure element is inserted, said application implementing a retrieval of the identifier of the mobile equipment in which the removable secure element is inserted, a check of the presence of the retrieved identifier in the stored list of mobile equipment identifiers as stored, and, if the retrieved identifier is present in the list, a deletion of the security context as stored.

WO 2025/002794 A1

# REMOVABLE SECURE ELEMENT HAVING IMPERSONATION PROTECTION

## FIELD OF THE INVENTION

The present invention relates to a removable secure element having protection against impersonation.

The invention also pertains to method to protect a removable secure element against impersonation of a universal identifier of a user of the removable secure element. It relates at last to an application dedicated to be installed and run in a removable secure element to implement the method of the invention.

## BACKGROUND OF THE INVENTION

Researchers revealed a potential vulnerability to impersonate someone else identity on the 3GPP network. Such attacks already appeared on the field and Mobile Network Operators are concerned.

In 5G, each subscriber receives a Subscription Permanent Identifier SUPI. It is a globally unique identifier that is assigned to each subscriber in the 5G system and that is provisioned in an Unified Data Repository UDR. In legacy technologies 3G/4G, similar identifiers exist and are known under the term IMSI.

Figure 1 illustrates the identified vulnerability. It occurs when, in a step S1, an attacker temporarily takes a victim's secure element VSE from a victim's Mobile Equipment VME, previously connected and authenticated and inserts it, in a step S2, into an attacker's Mobile Equipment AME. This situation corresponds to a "plastic roaming" situation which enables a subscriber to use a same removable secure element in a new ME.

Such a plastic roaming uses a "security context" SC which is a state that is established locally at the ME and a serving network domain. It is represented by the "security context data" stored at the ME and a serving network. For example, security context in 5G is explained in TS33.501 – Paragraph 3.1 Definitions. Similar definitions are given in legacy 3G/4G standards.

Thanks to the rules as determined in the standards to enable the plastic roaming, the attacker indeed uses the security context SC stored in the victim's VSE and avoid re-authentication to the network. Thus, at step S2, the attacker's ME is connected and authenticated. This corresponds to a plastic roaming situation.

The attack then consists in powering off the attacker's ME in a step S3. During the attacker's ME power-off procedure, an attacker's security context SC' is stored in the USIM and in the attacker's AME. The serving network domain also has knowledge of this new security context SC'.

Besides this process, the attacker retrieves the SUPI of the victim from the USIM in a step S4.

The attacker then uses a programmable secure element USIM PSE and copies the victim's SUPI into the attacker's programmable USIM PSE, typically using a computer PC, in a step S5. Here it is noted that no removable property is necessary for the programmable secure element to implement the attack.

Steps S4 and S5 define the fraudulent manipulation addressed by the invention. This may occur while victim's secure element is stolen (e.g. from a locker or at work). The attacker can then temporarily substitute the victim's phone, recover the SIM and copies the victim's SUPI into the attacker's programmable USIM PSE before reinserting the USIM in the victim's mobile VME in a step S6, the mobile being then returned.

If USIM is not back to the victim, the victim will alert the MNO and thus the usage of the USIM will be blocked. This is the reason why USIM must be given back. The VME is thus again authenticated and connected as for a classical plastic roaming.

The attacker then inserts, in a step S7, the attacker's programmable USIM PSE including the SUPI of the victim's secure element into the attacker's AME.It is here noted that the programmable USIM PSE may also be a secure element already integrated/embedded in an attacker's AME. However it is necessary for this AME to have a slot where to introduce the removable victim secure element VSE in order to perform the attack.

As the SUPI stored in the attacker's USIM PSE is the same as the one stored in the attacker's AME, the security context SC' as locally stored in the AME is automatically used to reconnect the attacker's AME to the network without re-authentication.

The reason for such a situation is that mobile equipments do not reset security contexts SC until the SUPI is changed according to 23.501. With such a process, an attacker could pretend to be someone else. As a consequence, the attacker's mobile equipment AME uses the Security Context SC', locally stored in the AME memory, as long as the SUPI associated to that security context SC' and the SUPI of the USIM PSE are the same.

Some approaches can solve this issue like increasing the frequency and the number of Authentication and Key Agreement mechanism. However this increases the network load and the energy consumption.

The use of the USIM PIN can also be made mandatory. In addition not to be practical for the user, this solution will not provide more security as fewer and fewer people use or overwrite the default MNO's PIN code.

Another possibility would be to erase the security context stored in the USIM when a new ME is detected but this solution is not acceptable as it would prevent "plastic roaming", which is besides a requirement.

Further alternative and advantageous solutions would, accordingly, be desirable in the art.

## SUMMARY OF THE INVENTION

The present invention aims at avoiding the above-mentioned malicious attacks.

The present invention is defined, in its broadest sense, as a removable secure element having a memory to store at least a universal user identifier, a security context, a list of mobile equipment identifiers in which the removable secure element was previously inserted, said removable secure element being dedicated to be inserted in a mobile equipment compliant with plastic roaming connecting and authenticating automatically the mobile equipment to a serving network using the security context stored in the removable secure element as

soon as the universal user identifier stored in the removable secure element is the same as the one associated to the security context on the serving network side, said removable secure element further having an application to monitor an identifier of a mobile equipment in which the removable secure element is inserted, said application implementing:

- a retrieval of the identifier of the mobile equipment in which the removable secure element is inserted,

- a check of the presence of the retrieved identifier in the stored list of mobile equipment identifiers as stored,

- if the retrieved identifier is present in the list, a deletion of the security context as stored.

Once the security context is deleted, there is no possibility for the mobile equipment to connect and authenticate automatically at the serving network. New authentication data will be required. The serving network will not accept the previously used security context. It leads to an impossibility for the attacker's mobile equipment to automatically connect and authenticate at the serving network. The invention thus protects the universal identifier of the user of the removable secure element from impersonation according to the above-described attack. The application in the USIM thus monitors in an original way the ME identifier in order to erase the USIM files and thus, as a consequence, to automatically reset the terminal to prevent a SIM swap attacker to use its illicit security context to connect to the network.

According to a specific feature, said application further implements a monitoring of a mobile equipment change timing, the deletion being triggered when the retrieved identifier is present in the list and when the change timing is below a predetermined threshold.

This enables to refine the detection of an attack avoiding to force the user to re-authenticate while the user has used another mobile equipment for a while and returning to a previously used mobile equipment.

The present invention also relates to a method to protect a removable secure element against impersonation of a universal identifier of a user of the removable secure element, the removable secure element having a memory

to store at least a universal user identifier, a security context, a list of mobile equipment identifiers in which the removable secure element was previously inserted, said method comprising the steps of, while the removable secure element is inserted in a mobile equipment:

- retrieving an identifier of the mobile equipment in which the removable secure element is inserted;
- checking the presence of the identifier in the list of mobile equipment identifiers as stored;
- if the identifier is present in the list, deleting the security context as stored.

This method, when implemented in a secure element, prevents the attack as described in the background of the invention part.

Optionally, the method further comprises the step of monitoring a mobile equipment change timing, the deletion being triggered when the retrieved identifier is present in the list and when the change timing is below a preconfigured threshold.

Advantageously, it further comprises the step of sending a request to authenticate with the serving network to the mobile equipment.

This step enables to speed up the start of the authentication of the user that will otherwise be inherent to the absence of the security context. It will thus invalidate the attacker's mobile equipment security context as soon as possible.

The invention then relates to an application dedicated to be installed and run in a removable secure element to monitor an identifier of a mobile equipment in which the removable secure element is inserted, the removable secure element having further a memory to store at least a universal user identifier, a security context, a list of mobile equipment identifiers in which the removable secure element was previously inserted, said application having instructions for the secure element to:

- retrieve an identifier of the mobile equipment in which the removable secure element is inserted;

- check the presence of the identifier in the list of mobile equipment identifiers as stored;
- if the identifier is present in the list, delete the security context as stored.

Optionally, the application further has instructions to monitor a mobile equipment change timing, the deletion being triggered when the retrieved identifier is present in the list and when the change timing is below a preconfigured threshold.

Advantageously, the application further has instructions to send a request to authenticate with the serving network to the mobile equipment.

To the accomplishment of the foregoing and related ends, one or more embodiments comprise the features hereinafter fully described and particularly pointed out in the claims.

## BRIEF DESCRIPTION OF THE DRAWINGS

The following description and the annexed drawings set forth in detail certain illustrative aspects and are indicative of but a few of the various ways in which the principles of the embodiments may be employed. Other advantages and novel features will become apparent from the following detailed description when considered in conjunction with the drawings and the disclosed embodiments are intended to include all such aspects and their equivalents.

- Figure 1 illustrates the attack as prevented with the invention;
- Figure 2 shows a flowchart of the anti-impersonate method of the invention implemented in a mobile equipment ME;
- Figure 3 illustrates the prevention of the attack thanks to the invention.

## DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

For a more complete understanding of the invention, the invention will now be described in detail with reference to the accompanying drawing. The detailed description will illustrate and describe what is considered as a

preferred embodiment of the invention. It should of course be understood that various modifications and changes in form or detail could readily be made without departing from the scope of the invention. It is therefore intended that the invention may not be limited to the exact form and detail shown and described herein, nor to anything less than the whole of the invention disclosed herein and as claimed hereinafter. The same elements have been designated with the same references in the different drawings. For clarity, only those elements and steps which are useful to the understanding of the present invention have been shown in the drawings and will be described.

Figure 2 schematically shows a flowchart of a method of the invention as implemented in a secure element VSE of the invention. The secure element VSE has a memory to store the security context SC and other instructions and data necessary to the functioning of the VSE with the Mobile Equipment and the Networks. According to the method of the invention, once the secure element of the invention is inserted in a mobile equipment of a user ME in a step T0, an application/routine in the secure element VSE retrieves, in a step T1, an identifier I(ME) of the ME. In a step T2, the application/routine checks if the identifier I(ME) is included in an historic of Mobile Equipment Identifiers I(ME) where the VSE was previously inserted. Said historic is a list of Mobile Equipment identifiers stored in the memory of the secure element VSE.

If the identifier I(ME) is in the historic (case Y), the security context SC as stored in the memory of the secure element VSE is deleted by the application/routine in a step T3 and the connection and authentication routine is fully performed again by the secure element VSE in a step T4. If the identifier I(ME) is not in the historic (case N), this signs a plastic roaming and the connection and authentication is automatically re-established in a step T5.

The USIM VSE thus stores an historic of ME identities I(ME) where the USIM has been inserted into. When the USIM VSE detects that the same ME is used, i.e. if ME identity I(ME) is already in the history list, the security context stored in the USIM is cleared including the security context SC' and location information (LOCI) files. The deletion first occurs in the USIM, but it will also subsequently occur in the ME. It is the case as soon as the ME reads the

security context in the USIM according to an application/routine executed in the USIM.

The absence of security context thus forces the ME to reset and then to perform authentication to the network. This is automatic as soon as no security context is available from USIM. Optionally, the timing of change of ME could be used to determine if an attack was performed. Typically, a short period of time between change of ME will correspond to an attack.

According to the invention, the secure element USIM identifies the current mobile equipment in which it is inserted and checks if the ME identifier is in the history list. The invention advantageously uses an already existing list, i.e. the EFIPD which contains the IMEI(SV) of Pairing Device as defined in TS 23.003 where USAT Application Pairing is supported (point 4.2.102 of ETSI TS 131 102 V12.13.0).

If the identifier of the ME in which the SE is inserted is present, the invention triggers an erase of at least USIM security contexts and request ME to reset and to force authentication.

Figure 3 schematically shows how the invention prevents the vulnerability as described in figure 1.

The invention intervenes at step S6, when the attacker inserts back the SE in the victim's ME. If the identifier of the ME is in the list, it triggers a deletion of the security context SC' which is thus not anymore valid to serve with the previously serving network. The connection and authentication are not anymore possible using the security context SC' as besides present on the attacker's ME AME. The attacker's mobile equipment, even if having the SUPI of the victim's secure element, cannot anymore connect or authenticate.

The solution of the invention is fully compatible with Plastic Roaming. It only impacts the secure element and can thus be deployed independently of the mobile equipment. It enables a pre/post issuance deployment scheme. It solves the identified security issue from mobile behaviors.

In the above 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. The above 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.

## CLAIMS

1. Removable secure element having a memory to store at least a universal user identifier, a security context, a list of mobile equipment identifiers in which the removable secure element was previously inserted, said removable secure element being dedicated to be inserted in a mobile equipment compliant with plastic roaming connecting and authenticating automatically the mobile equipment to a serving network using the security context stored in the removable secure element as soon as the universal user identifier stored in the removable secure element is the same as the one associated to the security context on the serving network side, said removable secure element further having an application to monitor an identifier of a mobile equipment in which the removable secure element is inserted, said application implementing:

- a retrieval of the identifier of the mobile equipment in which the removable secure element is inserted,
- a check of the presence of the retrieved identifier in the stored list of mobile equipment identifiers as stored,
- if the retrieved identifier is present in the list, a deletion of the security context as stored.

2. Removable secure element according to claim 1, wherein said application further implements a monitoring of a mobile equipment change timing, the deletion being triggered when the retrieved identifier is present in the list and when the change timing is below a preconfigured threshold.

3. Method to protect a removable secure element against impersonation of a universal identifier of a user of the removable secure element, the removable secure element having a memory to store at least a universal user identifier, a security context, a list of mobile equipment identifiers in which the removable secure element was previously inserted,

said method comprising the steps of, while the removable secure element is inserted in a mobile equipment:

- retrieving an identifier of the mobile equipment in which the removable secure element is inserted;
- checking the presence of the identifier in the list of mobile equipment identifiers as stored;
- if the identifier is present in the list, deleting the security context as stored.

4. Method according to claim 3, further comprising the step of monitoring a mobile equipment change timing, the deletion being triggered when the retrieved identifier is present in the list and when the change timing is below a preconfigured threshold.

5. Method according to at least one of claims 3 and 4, further comprising the step of sending a request to authenticate with the serving network to the mobile equipment.

6. Application dedicated to be installed and run in a removable secure element to monitor an identifier of a mobile equipment in which the removable secure element is inserted, the removable secure element having further a memory to store at least a universal user identifier, a security context, a list of mobile equipment identifiers in which the removable secure element was previously inserted, said application having instructions for the secure element to:

- retrieve an identifier of the mobile equipment in which the removable secure element is inserted;
- check the presence of the identifier in the list of mobile equipment identifiers as stored;
- if the identifier is present in the list, delete the security context as stored.

7. Application according to claim 6, further having instructions to monitor a mobile equipment change timing, the deletion being triggered when the retrieved identifier is present in the list and when the change timing is below a preconfigured threshold.

8. Application according to at least one of claims 6 and 7, further having instructions to send a request to authenticate with the serving network to the mobile equipment.

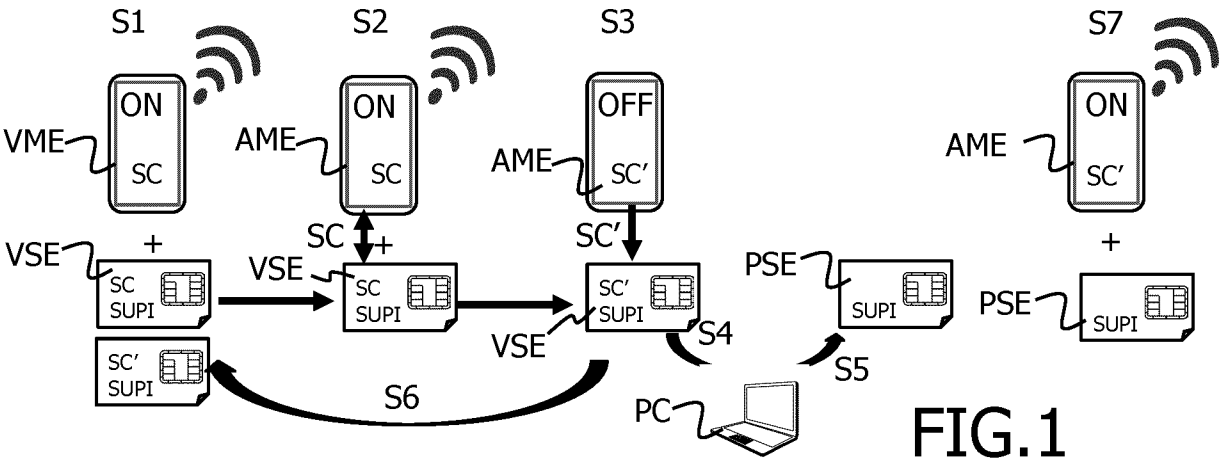



FIG.1

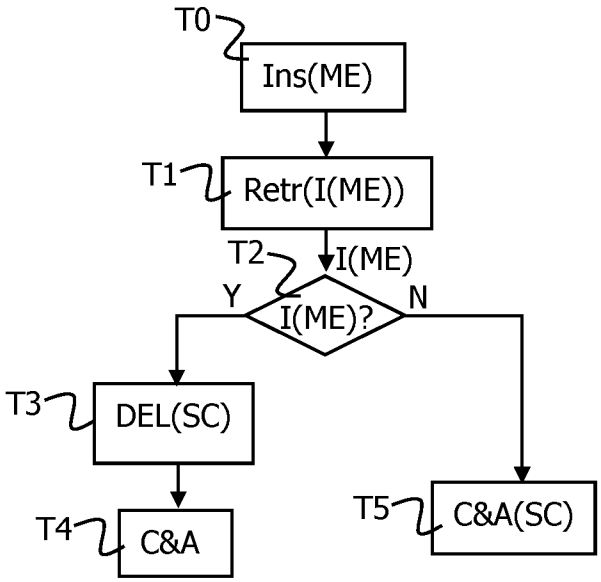



FIG.2

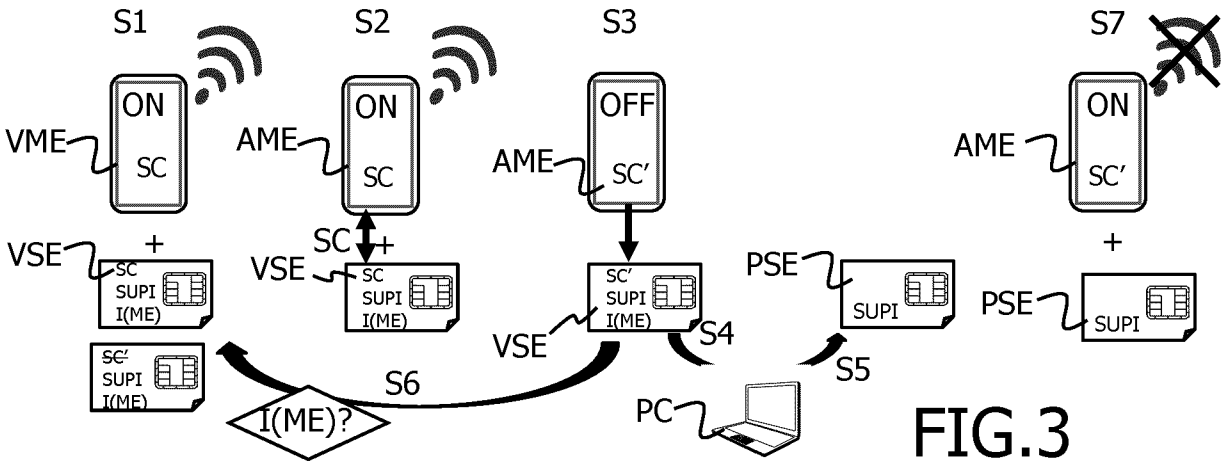



FIG.3

# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2024/066109

**A. CLASSIFICATION OF SUBJECT MATTER**

INV. H04W12/48 H04W12/126 H04W12/60 H04L9/40
ADD. H04W12/069

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)
H04W H04L

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. |
|---|---|---|
| Y | EP 0 993 747 B1 (ORANGE PERSONAL COMM SERV LTD [GB]) 16 March 2005 (2005-03-16) paragraph [0006] - paragraph [0009] paragraph [0021] - paragraph [0058] figures 1-6 | 1-8 |
| Y | EP 2 209 329 A1 (NTT DOCOMO INC [JP]) 21 July 2010 (2010-07-21) paragraph [0039] - paragraph [0056] figures 1-3 | 1-8 |
| A | US 2010/317320 A1 (SAKARGAYAN ANUPAM [IN]) 16 December 2010 (2010-12-16) paragraph [0003] | 1-8 |

-/--

[x] Further documents are listed in the continuation of Box C.

[x] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 26 August 2024 | 17/09/2024 |

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

2

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

# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2024/066109

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | GEMALTO ET AL: "Storage of the EPS NAS security context in non-volatile memory of the UE", 3GPP DRAFT; S3-090246, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, no. Florence; 20090123, 23 January 2009 (2009-01-23), XP050334864, [retrieved on 2009-01-23] the whole document<br>----- | 1-8 |

2

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2024/066109

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 0993747 B1 | 16-03-2005 | AT E291334 T1 | 15-04-2005 |
| | | AU 750203 B2 | 11-07-2002 |
| | | CN 1264524 A | 23-08-2000 |
| | | DE 69829375 T2 | 13-04-2006 |
| | | EP 0993747 A1 | 19-04-2000 |
| | | EP 1441552 A1 | 28-07-2004 |
| | | ES 2239807 T3 | 01-10-2005 |
| | | GB 2327570 A | 27-01-1999 |
| | | JP 4222722 B2 | 12-02-2009 |
| | | JP 2001510973 A | 07-08-2001 |
| | | TW 384449 B | 11-03-2000 |
| | | WO 9904587 A1 | 28-01-1999 |
| EP 2209329 A1 | 21-07-2010 | EP 2209329 A1 | 21-07-2010 |
| | | JP 4796190 B2 | 19-10-2011 |
| | | JP 2010166566 A | 29-07-2010 |
| US 2010317320 A1 | 16-12-2010 | CN 102460451 A | 16-05-2012 |
| | | EP 2441027 A2 | 18-04-2012 |
| | | JP 5404924 B2 | 05-02-2014 |
| | | JP 2012530290 A | 29-11-2012 |
| | | KR 101308334 B1 | 22-11-2013 |
| | | US 2010317320 A1 | 16-12-2010 |
| | | WO 2010144718 A2 | 16-12-2010 |