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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 August 2020 (13.08.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/160804 A1

(51) International Patent Classification:
H04W 12/00 (2009.01)

(21) International Application Number:
PCT/EP2019/081215

(22) International Filing Date:
13 November 2019 (13.11.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
19155419.5 05 February 2019 (05.02.2019) EP
19195307.4 04 September 2019 (04.09.2019) EP

(71) Applicant: **SHENZHEN GOODIX TECHNOLOGY CO., LTD.** [CN/CN]; Floor 13, Phase B, Tengfei Industrial Building, Futian Free Trade Zone, Shenzhen, Guangdong 518045 (CN).

(72) Inventor: **FRÖHLICH, Martin**; Paulstr. 15, 01099 Dresden (DE).

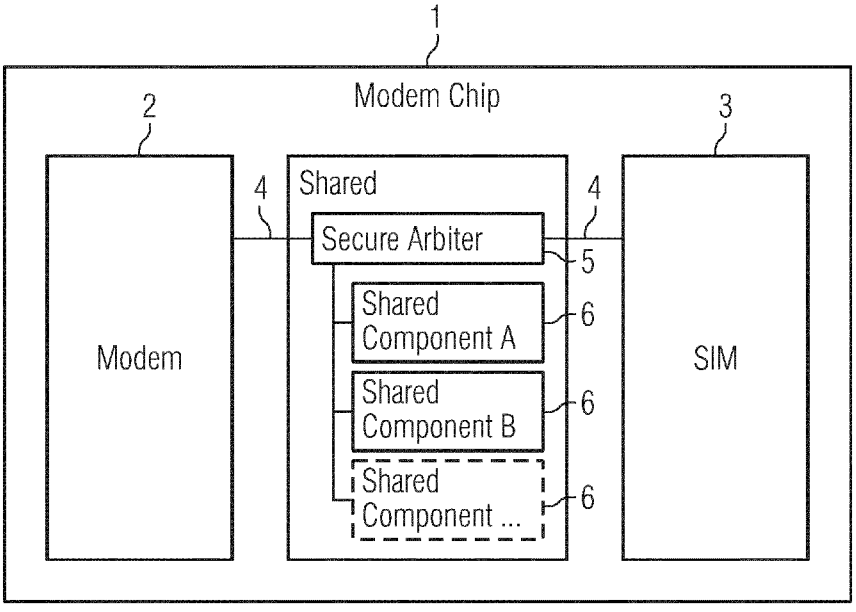
(74) Agent: **ADLER, Peter**; Lippert Stachow Patentanwälte Rechtsanwälte Partnerschaft mbB, Krenkelstraße 3, 01309 Dresden (DE).

(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, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

(54) Title: IMPROVED UE WITH AN INTEGRATED SUBSCRIBER IDENTITY MODULES (ISIM) BY RESOURCE SHARING

FIG 2



(57) Abstract: The invention discloses an improved Narrowband Internet of Things device (UE) supporting resource sharing for integrated Subscriber Identity Modules (iSIM). The object of the invention to further reduce the cost per UE by reducing the chip area and energy consumption of an integrated UICC chip will be solved therein that identical components of the modem and the iSIM are designed as shared components, whereas a secure hardware arbiter securely manages any access to said shared components by the modem or the iSIM and prevents any kind of information leaking.

WO 2020/160804 A1

[Continued on next page]

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))*

Improved UE with an integrated Subscriber Identity Modules (iSIM) by resource sharing

The invention relates to an improved Narrowband Internet of Things device (UE) supporting resource sharing for integrated Subscriber Identity Modules (iSIM).

There are standards describing the "classical" SIM/UICC or the embedded version eSIM, see: https://www.gsma.com/esim/. Consumer benefits of such eSIMs include, that a simpler device setup is possible without the need to insert or replace a SIM card; devices can operate independently of a tethered smartphone, with their own subscriptions; and a range of new, enhanced mobile-connected devices benefit from the standardized eSIM.

So far, integrated SIMs (iSIMs) are not yet standardized.

All 3GPP based cellular user equipments (UE), also known as Narrowband Internet of Things devices, such as mobile phone, require a mechanism to prove their identity against the cellular network and to exchange keys for a secure connection.

Therefore, the Universal Integrated Circuit Card (UICC - the hardware), with a USIM application (the software) running on it, is used. The UICC is a high secure hardware module that is connected (wired) to the UE. The USIM application contains all secret keys and provider specific information. The USIM application is provisioned by the cellular operator.

The secret keys inside the USIM application stored on the UICC must not be read out. The keys are used to authenticate the UE against the core network with the help of a cryptographic algorithm. Furthermore, the USIM application generates the secret session keys for the UE.

Thus, each UE requires a USIM application (running on the UICC) to attach to a core network successfully.

The modem to UICC communication is done via wired serial interface which is standardized in ISO/IEC 7816-3.

The disadvantage of a separate UICC is it's embodiment as a separated secure hardware element, a SIM card, which is required in a UE. This causes additional system costs. Cost sensitive systems require a solution where the UICC becomes part of the modem inside the UE. Thus, the integration of the UICC (with the USIM application) is called for integrated Subscriber Identity Modules (iSIM).

A quite simple solution for an iSIM is just to put the UICC chip and the modem chip in one package (SIP - System in Package) or to have the UICC chip as part of the modem chip (figure 1).

The objective of the invention is to further reduce the cost per UE by reducing the chip area and energy consumption of an integrated UICC chip.

The objective of the invention will be solved by an improved Narrowband Internet of Things device (UE) comprising a modem and an integrated Subscriber Identity Module (iSIM) both combined on a modem chip, wherein identical components of the modem and the iSIM are designed as shared components,

whereas a secure hardware arbiter securely manages any access to said shared components by the modem or the iSIM and prevents any kind of information leaking.

Integrated Subscriber Identity Modules (iSIMs) require for network authentication and provisioning cryptographic functions like AES, HMAC, Elliptic Curve Cryptography or true random numbers. Secure hardware modules, including iSIMs, provide special hardware accelerator to support such functions. Those special hardware accelerators are also used in the modem, e. g. for secure boot, firmware encryption and integrity checking, for encryption of the network packets, or end-to-end data protection with DTLS-Datagram Transport Layer Security.

The usage of shared hardware components requires a secure hardware arbiter that prevents any access of a used component by the other module, either the modem or the iSIM and prevents any kind of information leaking.

In a preferred embodiment of the inventive UE, the hardware arbiter comprises a timer for preventing blocking of said shared components. If an attacker can execute code on a modem or an application processor, he allocates the resource or component and, in the worst case, never releases that resource or component again, thus blocking the entire system. With the timer, the arbiter can specify that a resource can only be used for a certain time. After the timer has expired, the resource is forced to be released again.

So, in a further preferred embodiment of the inventive UE, the hardware arbiter ensures real-time operating and hence

preventing the blocking of a shared component. A blocked component can be released either through a request of the modem for example or after the timer has expired. This prevents that the system fails entirely and ensures a real-time operating.

In another embodiment of the inventive UE, the hardware arbiter provides reset and/or RAM cryptography procedures for securely removing all information that remains after usage of said shared components by the modem or the iSIM.

In an embodiment of the inventive UE the shared components are cryptographic accelerators. Cryptographic accelerators are suitable because they can be reset easily to remove all remaining information. The securely removing of information in registers after usage can be done by a reset. These components are rarely. An access protection module will grand access only to one party – iSIM or modem. The other has to wait till the usage was finished.

If asymmetric cryptography is used, which is based on elliptic curves, one need RAM, which as such has no reset. For securely removing the information inside the RAM there is either the possibility to overwrite the RAM with random data by means of a routine. Or alternatively an XOR mask with a random value can be used. All data written to RAM will be XOR-ed with the XOR mask. The XOR mask, which is stored in a register, is then reset. Only if one knew the value of the XOR mask, a recovery of the RAM would be possible.

To summarize, the arbiter must prevent any kind of information leaking.

The invention will be explained in more detail using exemplary embodiments.

The appended drawings show

Fig. 1 Basic components of an iSIM (state-of-the-art);

Fig. 2 Secure component sharing via a secure arbiter.

Figure 2 illustrates the inventive UE with a modem chip which comprises a modem and an iSIM. The modem and the iSIM share components which are used by both - the modem and the iSIM. A shared component can be typically cryptographic accelerators which is used e.g. for AES, HMAC, Elliptic Curve Cryptography or true random number generator. For example, an AES core is used by the iSIM for data-encryption or data-decryption or session key generation. After the network authentication and provisioning the iSIM releases the AES core. The secure hardware arbiter ensures that all information is removed after said usage. Afterwards, the modem uses the AES core for data (packet data) encryption or decryption. It is important, that the hardware arbiter prevents any access of the AES core by the respective other component (modem or iSIM) if it is used.

It is also important that the hardware arbiter obfuscate the access time to prevent side channel attacks, because the execution time of asymmetric crypto accelerators is key dependent. This is done by some hardware that generates randomly non operation cycles or stops the clock for some cycles.

The modem is booting and uses the AES for the firmware image decryption and the ECC module to verify the firmware

signature. Afterwards the modem starts the iSIM. The iSIM does the same with the firmware. The modem tries to connect to the network. The modem receives the authenticate data from the network and sends the data to the iSIM. The iSIM uses the AES to check the authentication data, generates the response and the session keys for the modem. The modem uses the session keys to encrypt and/or decrypt the network data.

Improved UE with an integrated Subscriber Identity Modules (iSIM) by resource sharing

List of Reference Signs

1 modem chip
2 modem
3 integrated Subsciber Identity Module
4 serial interface
5 secure hardware arbiter
6 shared component

Improved UE with an integrated Subscriber Identity Modules (iSIM) by resource sharing

Claims

1. An improved Narrowband Internet of Things device – UE – comprising a modem (2) and an integrated Subscriber Identity Module (3) – iSIM – both combined on a modem chip (1), wherein identical components of the modem (2) and the iSIM (3) are designed as shared components (6), whereas a secure hardware arbiter (5) securely manages any access to said shared components (6) by the modem (2) or the iSIM (3) and prevents any kind of information leaking.

2. The improved UE according to claim 1, wherein the hardware arbiter (5) comprises a timer for preventing blocking of said shared components (6).

3. The improved UE according to claim 2, wherein the hardware arbiter (5) ensures real-time operating.

4. The improved UE according to claim 1, wherein the hardware arbiter (5) provides reset and/or RAM cryptography procedures for securely removing all information that remains after usage of said shared components (6) by the modem (2) or the iSIM (2).

5. The improved UE according to claim 1, wherein the shared components (6) are cryptographic accelerators.

FIG 1

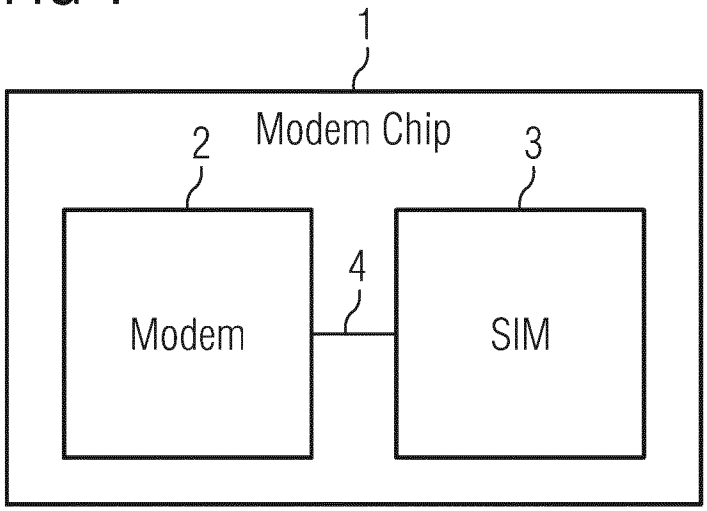
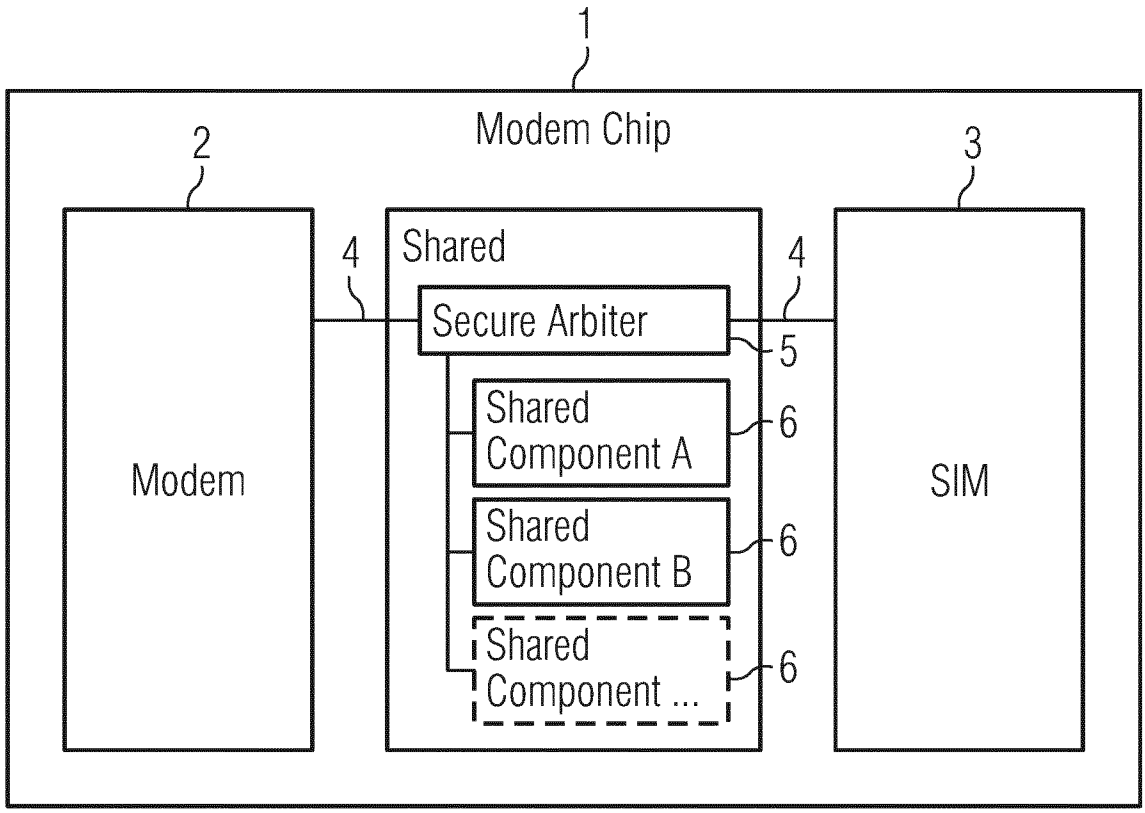

1
Modem Chip
2
3
4
Modem
SIM

FIG 2


1
Modem Chip
2
3
4
Shared
4
Secure Arbiter
5
Shared Component A
6
Shared Component B
6
Shared Component ...
6
Modem
SIM

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2019/081215

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/00
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)
H04W

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	WO 2017/082966 A1 (INTEL IP CORP [US]) 18 May 2017 (2017-05-18) figure 7 page 6, line 8 page 7, line 4 - line 30 page 10, line 1 - line 20 page 9, line 30 - line 35 page 39, line 21 - line 31 page 40, line 27 - page 41, line 13 page 45, line 1 - line 24 -----	1-5
A	WO 2016/075622 A1 (SIMLESS INC [US]) 19 May 2016 (2016-05-19) page 2, line 10 - line 11; figure 3 page 15, line 18 - line 20 -----	1-5

-/--

[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
19 February 2020	28/02/2020

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

1

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

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Arm: "Unlocking the cellular IoT potential for chipset makers Whitepaper", , 1 February 2019 (2019-02-01), pages 1-7, XP055666839, Retrieved from the Internet: URL:https://learn.arm.com/rs/714-XIJ-402/images/Kigen-Unlocking_whitepaper.pdf [retrieved on 2020-02-10] the whole document -----	1-5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2019/081215

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2017082966 A1	18-05-2017	NONE	
WO 2016075622 A1	19-05-2016	EP 3257281 A1	20-12-2017
		WO 2016075622 A1	19-05-2016