USIM in 5G Era

Mireille Pauliac

Department of Standardization and Technology, Thales, France
E-mail: mireille.pauliac@thalesgroup.com

Received 01 November 2019; Accepted 28 November 2019;
Publication 04 January 2020

Abstract

If you ask anybody what is the name of the card inside his mobile phone, he will for sure answer SIM card, without knowing it is an acronym for Subscriber Identity Module. But, what about the USIM (Universal Subscriber Identity Module)? The USIM plays a key role in the mobile telecommunication services since it brings a host of fundamental features that are now perfected for 5G.

This paper gives an overview of the new functionalities offered by the USIM in 5G system including new authentication schemes, subscriber privacy, Steering of Roaming, UE Parameters Update over NAS, and Long Term Key Update Procedure.

Keywords: 5G USIM, UICC, smart card, OTA, authentication, AKA, 5G-AKA, EAP-AKA′, primary authentication, secondary authentication, network slice authentication, privacy, subscriber privacy, IMSI, SUPI, SUCI, key update, long term key update, LTKUP, steering of roaming, SoR, UE parameters update.

1 Introduction

In mobile telecommunications systems specified by the 3rd Generation Partnership Project (3GPP), the User Equipment consists of a Mobile Equipment (ME) and a Universal Integrated Circuit Card (UICC), where the UICC is a

Journal of ICT, Vol. 8_1, 29–40. *River Publishers*
doi: 10.13052/jicts2245-800X.813

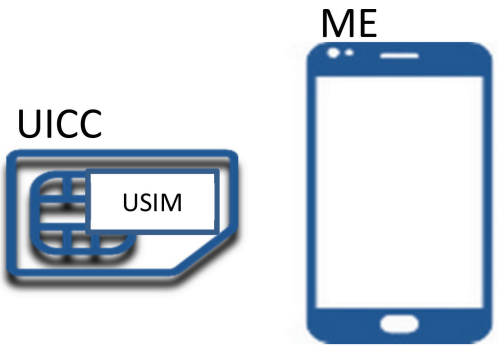

Figure 1 User equipment in 3GPP.

tamper-resistant entity designed to resist software and hardware attacks. The UICC can contain several applications and one of this application is the USIM.

The USIM securely stores and handles all the sensitive data related to the subscriber and the home network. The USIM is under the control of the home network operator: the home network operator chooses the data to be provisioned in the USIM before the issuance of the UICC and administrates remotely the USIM in the user equipment thanks to Over-The-Air (OTA) mechanisms. The USIM is a trust anchor in the user equipment.

This paper describes the new functionalities offered by the USIM for 5G system.

2 New Authentication Schemes in 5G System

In 5G Phase 1 (Rel-15), primary authentication has been defined to be used over both 3GPP-access and non-3GPP access, while the secondary authentication has been defined to allow a user equipment to access an external data network.

The introduction of network slicing in 5G made necessary the definition of a network slice-specific authentication. It is done in 5G Phase-2 (Rel-16).

These authentications are described below. They are specified in 3GPP TS 33.501 [1].

Primary authentication

A detailed overview of primary authentications is given in "3GPP 5G security" paper [2].

The primary authentication is a mandatory procedure to allow a user equipment to access 3GPP networks or non-3GPP networks. EAP-AKA′ or 5G-AKA are the only authentication methods allowed for primary authentication, and the subscription credentials are always stored in the USIM when the terminal supports 3GPP access capabilities.

For AKA-based primary authentication, the mutual authentication performed in the USIM and the generation of key material (the integrity key IK and the confidentiality key CK) sent by the USIM to the ME remain unchanged compared to 3G, 4G and fulfil 3GPP TS 33.102 specification [3].

The changes in the USIM for 5G primary authentication consist of the storage of new security contexts and additional key materials in the USIM depending on the configuration of the USIM. If the USIM supports the storage of 5G parameters, then the ME stores in the USIM the new 5G security context and new keys defined for 5G key hierarchy (i.e. K_{AUSF}, K_{SEAF} and K_{AMF}). The USIM can store one 5G security context for 3GPP access networks and one 5G security context for non-3GPP access networks. The storage of security contexts and key material in the USIM guarantees faster reconnections in case of plastic roaming where the UICC is moved from one ME to another one.

In case of private networks (named standalone non-public networks), the authentication can rely on the EAP framework supported by 5G system. The user equipment and the serving network may support 5G AKA, EAP-AKA′, or any other key-generating EAP authentication method:

- When an AKA-based authentication method is used, clause 6.1 of 3PP TS 33501 [1] applies.
- When an EAP authentication method other than EAP-AKA′ is selected, the chosen method determines the credentials needed in the UE and in the network. How these credentials for EAP methods other than EAP AKA′ are stored and processed within the UE is out of the scope. But to ensure a high level of security in accessing the private network, the private network operator can decide to require the presence and the use of a UICC containing a USIM application in order to securely store and handle the subscription credentials for EAP methods such as EAP-AKA′ or EAP-TLS.

Secondary authentication

A detailed overview of secondary authentications is given in “3GPP 5G security” paper [2].

The secondary authentication is an optional authentication based on EAP and takes place between the user equipment and an external data network (DN). The choice of the EAP authentication method and the credentials is out of the scope of 3GPP. Nevertheless, an external Data Network can take the decision to secure the access to its DN by performing strong authentication thanks to EAP-AKA′ or EAP-TLS authentication methods with the presence of a USIM on a UICC in the user equipment to securely store and handle the credentials used to access the DN.

Network slice-specific authentication

The use of a network slice-specific authentication between a user equipment and an AAA (Authentication, Authorization and Accounting) server to access a network slice is optional. The network slice-specific authentication is based on EAP framework with a User ID and credentials distinct from the 3GPP subscription credentials. It takes place after the mandatory primary authentication. The stakeholder deploying a slice can decide to have a USIM on a UICC in the user equipment to ensure a high level of security to access his slices and prevent presence of unauthorized users.

3 Subscriber Privacy

A major evolution in 5G system is the protection of the subscriber privacy.

With subscriber privacy mechanism, it is now possible to never send in clear the Subscription Permanent Identity (SUPI) on the radio interface. The SUPI in 5G is the equivalent of the IMSI (International Mobile Subscriber Identity) in 4G. The SUPI takes the format of an IMSI or a NAI (Network Access Identifier). To counteract privacy-related attacks such as false base station attack, the user equipment computes and sends the SUCI: a privacy preserving identifier containing the concealed SUPI. However, the sending of the SUCI instead of the SUPI is not mandatory, the use of the subscriber privacy mechanism depends on the home network operator decision taking into national regulations. Thanks to the USIM configuration chosen by the home network operator, the ME knows whether a SUCI has to be sent rather than the SUPI and whether the computation of the SUCI takes place in the USIM or in the ME. The Home Network Public Key used to conceal the SUPI is always provisioned and stored only in the USIM.

- If the operator's decision is that ME has to calculate the SUCI, then the home network operator provisions in the USIM an ordered priority list of the protection scheme identifiers that the operator allows. The priority

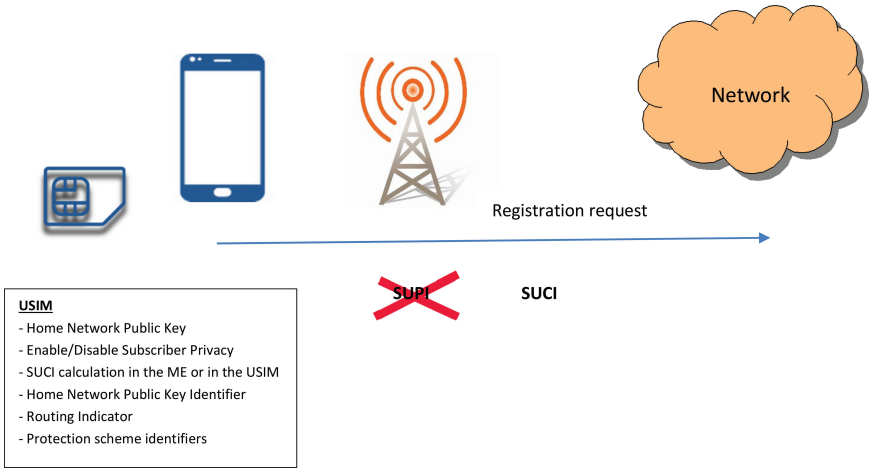

Figure 2 Subscriber privacy.

list of protection scheme identifiers in the USIM only contains protection scheme identifiers as specified in Annex C of 3GPP TS 33.501 [1]. This list may contain one or more protection schemes identifiers. The ME reads the SUCI calculation information from the USIM, including the SUPI, the SUPI Type, the Routing Indicator, the Home Network Public Key Identifier, the Home Network Public Key and the list of protection scheme identifiers. The ME selects the protection scheme from its supported schemes that has the highest priority in the list obtained from the USIM.

- If the operator's decision, indicated by the USIM, is that the USIM has to calculate the SUCI, then the USIM does not provide any parameter to the ME related to the calculation of the SUCI. The operator has to choose one protection scheme to conceal the SUPI between those specified in Annex C of 3GPP TS 33.501 [1]; it could also be a customized protection scheme chosen by the home network operator. Consequently, the computation of the SUCI in the USIM offers more flexibility and control for the mobile network operator to protect the identities of his subscribers.
- In case that the Home Network Public Key or the priority list are not provisioned, the ME calculates the SUCI using the null-scheme, equivalent to no subscriber privacy mechanism.

4 Steering of Roaming

5G introduced the Steering of Roaming (SoR) enabling the home network to send a list of preferred PLMNs over NAS when the user equipment is in a visited network. The preferred PLMN list is dynamically built for the presence of the subscriber in this particular visited network. The target of the SOR list in the user equipment could the ME or the USIM:

- In case that the SoR list is sent to the ME, then the list is protected in integrity thanks to a MAC computed with the key K_{AUSF} derived from the primary authentication.
- If the USIM is the target, then the list is protected in integrity with the MAC but also in confidentiality since the home network sends to the USIM the SoR list encapsulated in a secured packet as defined in 3GPP TS 31.115 [4] for OTA services. Consequently, the use of secured packet prevents a visited network from knowing the content of the SoR list.

5 UE Parameters Update

In a 5G system the home network could decide to modify UE parameters over NAS (Non-Access Stratum) such as the routing indicator in the USIM. In order to secure the update of the data in the USIM over NAS, the home network operator encapsulates the routing information in secured packet as defined in 3GPP TS 31.115 [4].

6 Long Term Key Update Procedures

There are scenarios where the mobile network operator would have interest in replacing the long term key used in the USIM for subscriber authentication.

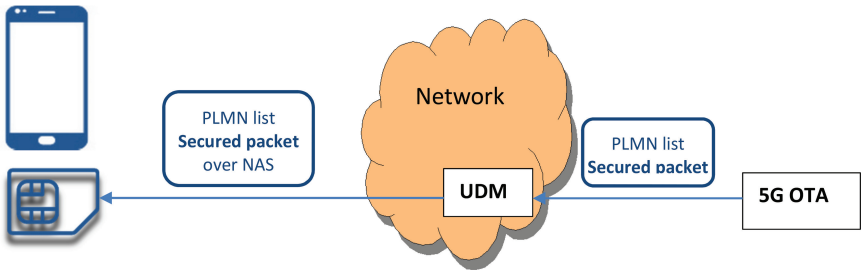

Figure 3 Steering of roaming with the USIM.

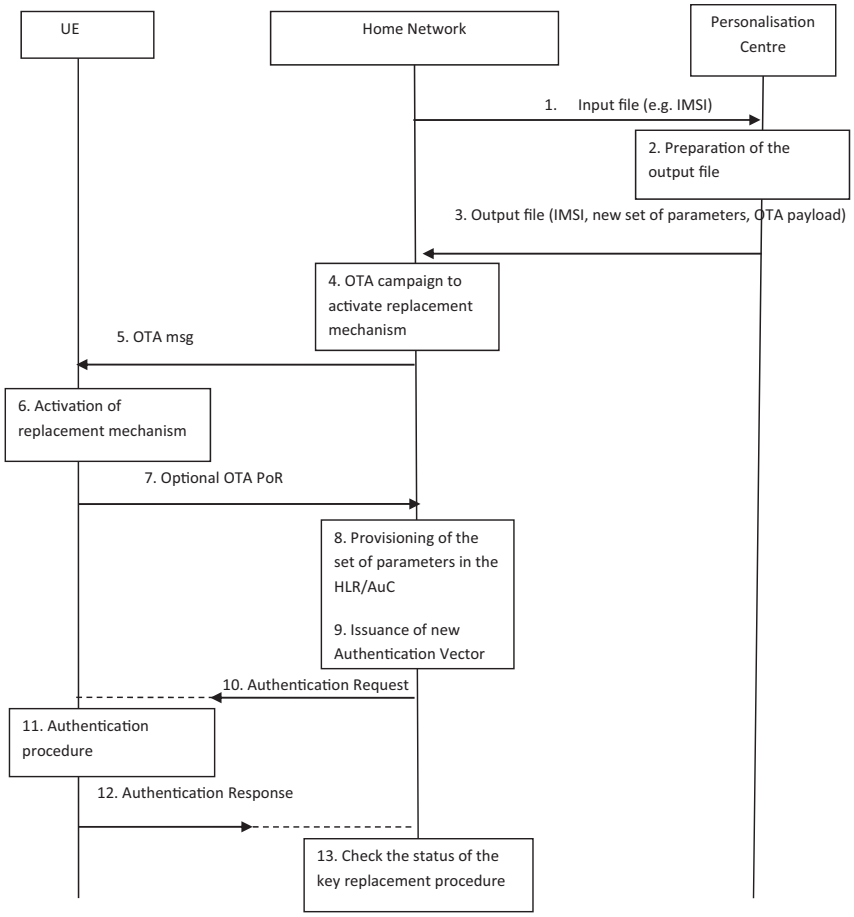

Figure 4 Key replacement procedure.

This is the Long Term Key Update Procedure (LTKUP) described in 3GPP TR 33.935 [5].

Multiple sets of parameters on the USIM

One of the solution for the LTKUP is to perform a key rotation in the USIM, as described in 3GPP TR 33.935 [5] with Solution #5 "Multiple sets of parameters on the USIM" The solution relies on the presence of several sets of parameters (K/OPc or K/TOPc) stored in the USIM. Only one set of parameters is active at a time in the USIM. The decision to launch the procedure to replace the long term key K in the USIM is taken by the

home network operator. The solution requires steps when the UICC is in the personalisation centre and then when the UICC is in the field.

UICC in personalisation centre

For each UICC, several sets of parameters (K/OPc or K/TOPc) are generated and provisioned in a USIM. But, only one set of parameters is active at a time in this USIM.

The personalisation centre sends to the network operator an output file, which contains only one single set of parameters (K and eventually OPc or TOPc). This set of parameters is provisioned in the network operator backend. The other sets of parameters generated may be retrieved on demand from the personalisation centre.

The OTA command sent to the USIM/UICC is secured thanks to secured packet mechanism specified in 3GPP TS 31.115 [4]. Optionally, a shared key called "replacement mechanism protection" key is provisioned in the UICC in order to protect in integrity the payload of the OTA command. This "replacement mechanism protection" key offers an additional level of security due to the sensitivity of the procedure. This "replacement mechanism protection" key, if present, is securely stored in the personalisation centre and never exits the personalisation centre.

UICC in the field

Once the UICC is in a User Equipment in the field, the network operator can launch when he wants the replacement procedure as follows:

The procedure to replace the long term key K works as follows:

1. When the network operator decides to update the long term key K of a given USIM within a UICC, the network operator sends an input file requesting the personalisation centre to deliver an output file containing a new set of parameters for a given USIM/UICC. The input file contains at least an identifier enabling the personalisation centre to retrieve new set of parameters (e.g. IMSI or ICCID).
2. The personalisation centre generates a new output file. This new output file contains the IMSI, a new set of parameters for this USIM (K and eventually OPc or TOPc), and the OTA payload that the network operator will have to send to the USIM. The OTA payload contains the request to activate the replacement mechanism, and an index identifying the corresponding set of parameters provisioned in the USIM.

   Optionally, in case that the "replacement mechanism protection" key was generated and stored in the personalisation centre, the personalisation centre protects the OTA payload in integrity.

3. The personalisation centre sends securely the output file to the network operator.
4. At reception of the output file, the network operator launches an OTA campaign targeting the corresponding USIM/UICC. The OTA campaign does not intend to immediately update the parameters in the USIM; the OTA campaign only activates the replacement mechanism for the targeted USIM.
5. The network operator sends to the USIM/UICC the OTA command activating the replacement mechanism in the USIM and providing the index of the new set of parameters.
6. The USIM/UICC in the UE receives the OTA command activating the replacement mechanism.

   If the USIM is provisioned with the "replacement mechanism protection" key, then the USIM verifies the protection in integrity of the OTA payload. The replacement mechanism remains inactive if the OTA payload verification is unsuccessful.

   If the verification of the integrity of the OTA payload is successful, then the USIM activates the replacement mechanism and stores the index of the corresponding set of parameters.

   Once the replacement mechanism is active, the USIM is ready to proceed the change of parameters set, but waits for an event to do so. The change of key is not yet done.
7. The USIM sends OTA Proof of Receipt to the network operator, if requested by the operator in step 4.
8. The network operator provisions the received set of parameters (K and eventually OPc or TOPc) in the backend using usual mechanism. Only one single set of parameters (K and eventually OPc or TOPc) is active at a time in the network operator for a given USIM.
9. The network operator issues an authentication vector with the new set of parameters.
10. The network operator sends an authentication procedure request.
11. The USIM receives an AUTHENTICATE command and performs the authentication procedure. If the USIM detects an authentication failure due to wrong key K and if the replacement mechanism has been activated in the USIM, then the USIM tries to perform the MAC verification of the AUTHENTICATE command with the new set of parameters (K/OPc or K/TOPc) provisioned identified by the index received in step 6.

If the MAC verification with the new set of parameters is successful, then

- the new set of parameters becomes active and the previous set of parameters may be deleted,
- the USIM continues the authentication procedure with the new set of parameters,
- and the USIM deactivates the replacement mechanism.

Otherwise,

- the USIM increments a retry counter associated to the replacement mechanism,
- The USIM deactivates the replacement mechanism if the retry counter has reached its maximum value,
- And, the USIM abandons the authentication procedure with MAC failure error.

12. The UE sends the results of the authentication procedure.
13. The network operator knows the status of the key replacement procedure thanks to the results of the authentication procedure sent by the USIM. If the result of the authentication procedure sent by the USIM indicates a MAC failure, then the network operator knows that the replacement mechanism failed. In that case, the network operator can decide to perform a new replacement procedure starting from step 9, or to perform a full procedure starting from step 1, or to restore the existing set of parameters active in the USIM.

7 Conclusion

This paper describes the new functionalities of the USIM in 5G era. Due to the fact that the Rel-16 is not yet finished some other uses of the USIM are under discussion and will be available in the near future.

References

[1] 3GPP TS 33.501, “Security architecture and procedures for 5G System”, Rel-15.
[2] Anand R. Prasad, Sivabalan Arumugam, Sheeba B and Alf Zugenmaier, 3GPP 5G Security, River Publishers, May 2018.
[3] 3GPP TS 33.102, “3G security; Security architecture”, Rel-15.

[4] 3GPP TS 31.115, "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications", Rel-15.
[5] 3GPP TR 33.935, "Detailed long term key update solutions", Rel-16.

Biography

Mireille Pauliac is security expert at Thales (former Gemalto/Gemplus) and belongs to the Standardization and Technology Department. After an engineering degree in computer science from "Ecole Supérieure d'Ingénieurs en Génie Electrique" (ESIGELEC) in France, she started working in 1996 as smart card operating system developer and then joined the security experts team. She has participated in numerous projects in banking and telecommunications areas to design and review the security protocols, and leaded security evaluations for ITSEC and Common Criteria certifications. She has contributed to telecommunications standardization with active participation in security of 3GPP, TISPAN, ETSI M2M, oneM2M, LoRa Alliance, and ETSI ITS.