SIMalliance LTE UICC profile

This document is a collection of requirements for optimal support of LTE/EPS networks by UICC

Document History

Version	Date	Editor	Remarks
1.0	23/06/2013	LTE Work Group	Public release

Table of Contents

1. Introduction

1.1 Document Purpose

This document is the technical illustration of the SIMalliance UICC LTE whitepaper available here: http://www.simalliance.org/en/resources/white_papers/

Enclosed in the following pages readers will find a collection of requirements for optimal UICC support for LTE/EPS networks. The document uses ETSI SCP and 3GPP standards as its baseline and aims to clarify which parts are mandatory and which are optional, in addition to addressing key implementation issues.

This document also refers to relevant specifications provided by OMA, OMTP, Global Platform and GSMA SmartSIM.

Since publication in 2012, the previous version of this document has been downloaded many thousands of times, demonstrating the interest that LTE players have in ensuring that their strategic card deployment takes full advantage of the technical recommendations contained herein. Selecting the right UICC technologies at the outset will guarantee a smooth transition to LTE and optimize the deployment of value added services, both for the Mobile Network Operator (MNO) and the end user.

The document defines two main sets of requirements:

SIMalliance UICC1: Recommended profile
This profile defines the fundamental set of features recommended by the SIMalliance that are required for users to realize the optimum benefit from the UICC and also to take full advantage of the services provided by high capacity networks.

It addresses the main use cases, including:
- Seamless management of the end user connectivity over multiple types of network
- Convenient and secure access to IMS multimedia services
- Efficient remote administration of the UICC over data networks via HTTPs

SIMalliance UICC2: Premium profile
This profile defines the enhanced features which are required in order to develop the fullest experience for the end user.

1.2 Terminology

Readers should note that SIMalliance is not a technical standards body. It is therefore only appropriate for this document to provide recommendations regarding how the technical standards should be implemented. In order to impart the significance of each, however, this document also classifies its recommendations, using the following terms and meanings:

- Mandatory
- Optional

1.3 Document scope

Feature	UICC1 (Recommended)	UICC2 (Premium)
EPS network authentication	X	X
Backward compatibility on UMTS / GSM authentication	X	X
Access to IMS network & services	X	X
i-WLAN access		X
3GPP / 3GPP2 interworking (*)	X	X
USIM Toolkit enhancement	X	X
Over The Air UICC administration	X	X
Generic bootstrapping architecture (GBA)		X
Extended Authentication Protocol (EAP)	X	X
NFC		X
Femtocell HeNB provisioning information	X	X
LTE roaming optimization	X	X
Others features	-	X

(*) Apply to 3GPP2 Operators

2. EPS Network Authentication

The UICC is a mandatory secure element of the LTE environment, ensuring safe and protected access to EPS networks.

The standard TS 22.278 clearly specifies "*Release 99 or later Releases' USIM application on the UICC is required to authenticate a user in an Evolved Packet System".* As a consequence **2G only SIMs are forbidden** to access to LTE network.

Two alternative solutions are proposed:

A Legacy USIM. This is a USIM used for UTRAN technology, where the EMM parameter storage and EPS location information files are not present in the file structure.

A Release 8 USIM (or LTE USIM). This is a USIM which includes LTE files specified in the Release 8 of the 3GPP 31.102 specification. The USIM files system supports:

- EMM parameters storage
- And EPS location information

SIMalliance recommends using a Release 8 USIM to store EPS security context instead of ME storage because from a security point of view, the storage of the UICC security context on the card is safer (it is protected by a PIN). This allows fast reconnection to the LTE network at switch on thus providing a quality end user experience. Moreover, storing LTE location information on the card enables the development of advanced roaming UICC based applications.

2.1 LTE Authentication with a LTE USIM

The TS 31.102 Release 8 and TS 33.401 specifications describe a new set of files dedicated for LTE authentication.

UICC usage requirements	Parameter/Comment	Support	
Features		Optional	Mandatory
USIM Service Table Service N°85	Informs the ME that the UICC is able to store the E-UTRAN Security Context.		X
ADF USIM /EF EPSNSC	Contains EPS NAS Security Context information. K_ASME (Access Security Management Entity) is master key derived from CK IK, and used to derive subsequent keys		X
ADF USIM/ EF EPSLOCI	Contains EPS location information: Globally Unique Temporary Identifier (GUTI) Last visited registered Tracking Area Identity (TAI) EPS update status.		X

EPS AKA	Authentication and key agreement procedure that shall be used for E-UTRAN network access. 3GPP TS 33.401 release 8 minimum		**X**

3. GSM/UMTS Authentication

Because UMTS provides a solution for the weaknesses of GSM security and also adds security features for new 3G radio access networks and services, it is possible to have GSM and UMTS authenticated access to an LTE USIM. This maximizes the compatibility between GSM and UMTS for LTE subscribers roaming across GSM and UMTS networks.

The full backward compatibility feature of the LTE UICC offers GSM secure access to subscribers. Since it also allows authentication to UMTS networks, the USIM is a mandatory secure element in the LTE environment, ensuring safe and protected access to mobile LTE and IMS networks.

USIM commands for authentication can be used in contexts such as:

- 3G security, when 3G authentication vectors (RAND, XRES, CK, IK, AUTN) are available (i.e. the UE is located in the UTRAN, or in a GSM radio access network which is connected to a 3G or 3G capable VLR/SGSN).
- GSM security, when only GSM authentication data is available (i.e. the UE is located in the GSM radio access network which is connected to a non-3G capable VLR/SGSN).

3.1 GSM and UMTS Authentication within the LTE USIM

In the 3GPP TS 31.102 specifications, the EFs regarding the GSM Access level are required for the USIM application to be able to access service through a GSM network.

To gain GSM access, the USIM provides GSM c2 and c3 conversion functions. These functions derive the required GSM parameters (SRES, cipher key Kc) from available 3G parameters.

UICC usage requirements	Parameter/Comment	Support	
Features		Optional	Mandatory
ADF USIM	Stores USIM file system		X
GSM Access	Service N° 27 of the USIM Service Table. This service indicates the presence of this DF and thus the support of a GSM access.		X
GSM Security Context	Service N° 38 of the USIM Service Table. USIM calculates the GSM response parameters SRES and KC, using the defined conversion functions.		X
Location Information: EF_{LOCI}	Containing: - TMSI: Temporary Mobile Subscriber Identity; - LAI: Location Area Information; - Location update status.		X
UMTS AKA	Authentication and Key Agreement TS 31.102 release 6.		X

4. Access to IMS network & services

Voice over LTE is performed over IMS (IP Multimedia Subsystem). This is a recommendation from the One Voice initiative, detailed in a document cosigned by AT&T, Orange, Telefonica, TeliaSonera, Verizon, Vodafone, Alcatel-Lucent, Ericsson, Nokia Siemens Networks, Nokia, Samsung and Sony Ericsson.

Now that voice is over IMS, a secure way to authenticate to the IMS layer is required. For voice services, user name and password authentication is insufficient. One Voice recommends utilizing the ISIM application on the UICC for this purpose: "The IMS core network shall support the procedures for ISIM based authentication. Support for ISIM based authentication in the UE is mandatory." This one Voice Initiative has now been renamed Voice over LTE (VoLTE) and integrated within the GSMA group.

Once the IMS network is deployed over LTE other services can then be offered to the end user. This is the case with Rich Communication Services (RCS) that enable users to perform video calls, for example, share their desktop while on a call, or share a dash board. The Generic Bootstrapping Architecture (GBA, see section 10) enables these third party IMS based services to be deployed securely. Here, the MNO can act as the identity and authorization manager for the service provider. Moreover, the GBA can offer an extra and applicative level of authentication to the service itself, in addition to the authentication already applied to the access gateway for the overall IMS infrastructure. This model makes a lot of sense when considering how to manage secure authentication most effectively for these applications.

There is clear momentum for carriers supporting voice over LTE and the RCS. In January 2013 many operators are actually deploying Voice over LTE, with a host of others also deploying RCS under different names, such as 'joyn', for example.

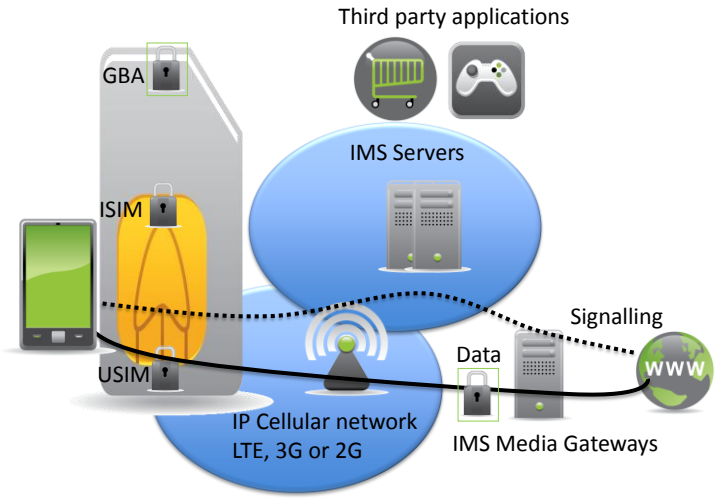

Figure 1: An access model for IMS applications and services

The ISIM application has several advantages:

- It reuses all the security aspects of the USIM

- It can eventually share the security functions with the USIM
- It enables the storage of public and private identities that are not necessarily linked to the IMSI. The TS 31.103 & TS 31.101 defines the ISIM application on the UICC for access to IMS services. A UICC can hold several ISIMs.
- IMS connection parameters are the property of the MNO, IMS Domain for example. The UICC offers the possibility to embed the settings for IMS.

4.1 IP Multimedia Services Identity Module (ISIM)

The more recent ISIM standard specifications implement features that are relevant for LTE. With this in mind, a UICC embedding an ISIM release 6 should be the minimum requirement.

UICC usage requirements	Parameter/Comment	Support	
Features		Optional	Mandatory
ISIM Release 5			X
ADF ISIM	Stores ISIM file system		X
ADF ISIM\EF IMPI	(IMS private user identity) Contains the private user identity of the user.		X
ADF ISIM\EF Domain	(Home Network Domain Name) Contains the home operator's network domain name		X
ADF ISIM\EF IMPU	(IMS public user identity) Contains one or more public user identity of the user		X
ADF ISIM\EF AD	Mode of operation (normal, type approval …)		X
ADF ISIM\EF ARR	Contains the access rules for files located under the ISIM ADF		X
Mutual Authenticate 3G in IMS context	ISIM performs an AKA scheme to access IMS services		X
ISIM Release 6			X
ADF ISIM\EF IST	(ISIM Service Table) Table of ISIM related services		X
ADF ISIM\ EFP-CSCF	(P-CSCF Address) For non 3GPP devices, not able to get the IMS proxy address from the access network procedures (GRPS PDP context activation or DHCP)		X
ADF ISIM\ EF GBABP	(GBA Bootstrapping Parameters) Contains the AKA Random challenge (RAND) and Bootstrapping Transaction Identifier (B-TID) associated with a GBA bootstrapping procedure		X
ADF ISIM\ EF GBANL	(GBA NAF list) Contains the list of NAF_ID (Network Application Function – i.e: web service) and B-TID associated to a GBA NAF derivation procedure		X
Mutual Authenticate in GBA (Bootstrapping mode) security context	ISIM performs a dedicated AKA for GBA.		X
Mutual Authenticate in GBA (NAF derivation) security context	ISIM derives results of the bootstrap using IMPI value.		X
Mutual Authentication HTTP Digest security context	ISIM furnishes response/session key to a realm/nonce/cnonce challenge according RFC2617	X	
ISIM Release 7		X	
ADF ISIM\EF IST	(ISIM Service Table) Service n°4: GBA-based Local Key Establishment Mechanism	X	

UICC usage requirements	Parameter/Comment	Support	
ADF ISIM\EF NAFKCA	(NAF Key Center Address) Contains one or more NAF Key Center Addresses.	X	
Mutual Authenticate	Security context Local Key Establishment (Key derivation mode)" and "(Key availability check mode)" for GBA new key establishment procedure.	**X**	
ISIM Release 8		X	
ADF ISIM\EF IST	(ISIM Service Table) Service n°5: Support of P-CSCF discovery for IMS Local Break Out. *A 3GPP device can now use EFP-CSCF in case of IMS local break Out*	**X**	

5. I-WLAN Access

Thanks to its unlicensed spectrum and low-cost hardware, WiFi can play an important role in relieving the pressure on the cellular networks, complementing them with fast data connections that are capable of delivering an excellent customer experience, resulting in strong user satisfaction.

By turning WiFi networks into seamless extensions of the LTE network, the Interworking Wireless LAN (I-WLAN) technique achieves this objective. I-WLAN enables the integration of WiFi technology with LTE networks providing subscribers a secure WiFi connection into the core network of the mobile operator so that they can "roam" onto unlicensed and untrusted IP access networks.

The UICC-based approach towards the integration of WiFi technology with LTE networks has a twofold advantage. On the one hand it allows MNOs to quickly re-use their existing network infrastructure and securely authenticate users with their UICC credentials, which reduces CAPEX in infrastructure and increases service availability and ARPU. On the other hand, it enables MNOs to offer an elegantly simple and portable solution, after the selection of the access point, users are automatically connected to the WiFi hotspot, uninhibited by the need to enter a username and password.

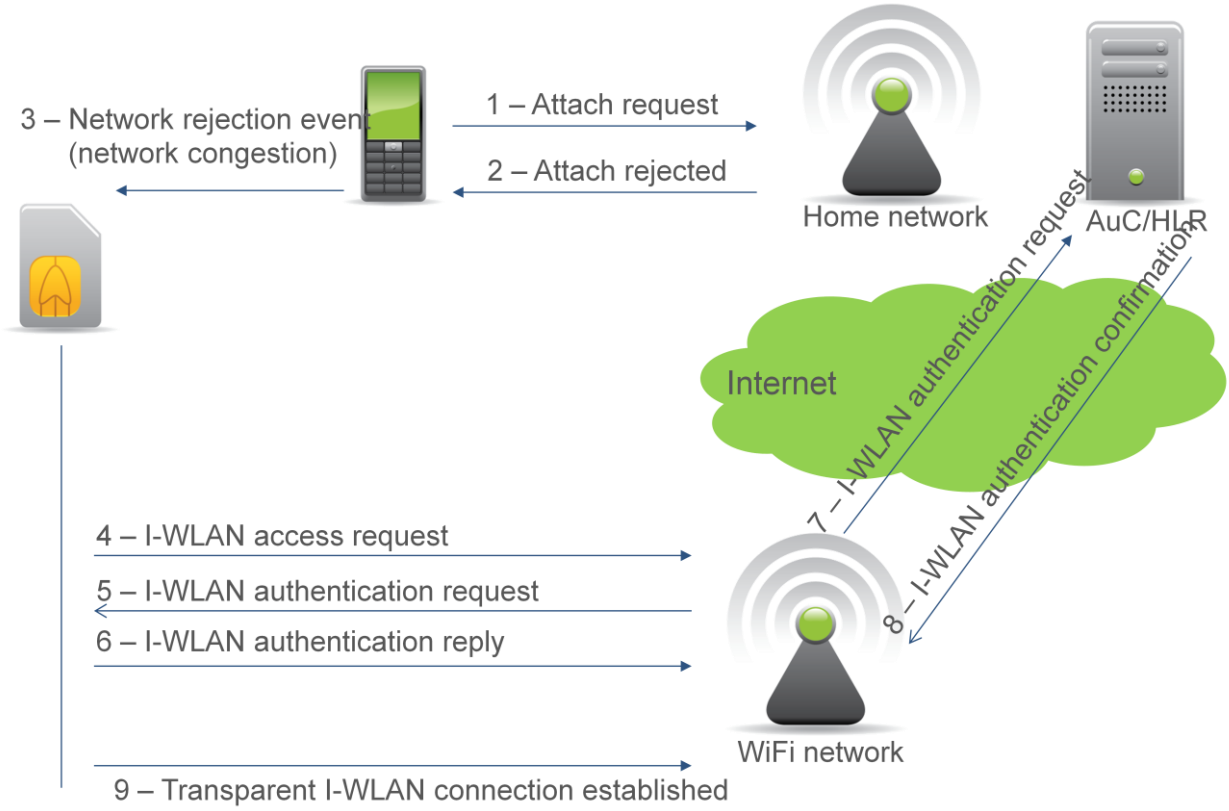

Figure 2: The I-WLAN model for LTE and WiFi integration

5.1 I-WLAN file system

The TS 31.102 Release 8 specification describes the set of files dedicated for I-WLAN authentication.

UICC usage requirements	Parameter/Comment	Support	
Features		Optional	Mandatory
USIM Service Table	Services nº59, nº60, nº61, nº62, nº63, nº66, n°81, n°82, n°83, n°84 or n°88 inform the ME that the UICC is able to manage the I-WLAN authentication		X
ADF USIM\DF WLAN			X
ADF USIM\DF WLAN\EF Pseudo	Temporary user identifier for subscriber authentication		X
ADF USIM\DF WLAN\EF UPLMNWLAN	User preferred PLMNs to be used for WLAN PLMN selection		X
ADF USIM DF WLAN\EF OPLMNWLAN	Operator preferred PLMNs to be used for WLAN PLMN selection		X
ADF USIM\DF WLAN\EF UWSIDL	User preferred list of WLAN specific identifier (WSID) for WLAN selection in priority order		X
ADF USIM\DF WLAN\EF OWSIDL	Operator preferred list of WLAN specific identifier (WSID) for WLAN selection in priority order		X
ADF USIM\DF WLAN\EF WRI	Parameters linked to a re-authentication identity to be used in fast re-authentication		X
ADF USIM\DF WLAN\EF HWSIDL	Home I-WLAN specific identifier list (WSID list) for I-WLAN selection in priority order		X
ADF USIM\DF WLAN\EF WEHPLMNPI	Indication to the ME for the presentation of the available EHPLMN(s) during I-WLAN selection procedures		X
ADF USIM\DF WLAN\EF WHPI	Indication to the ME for the selection of the I-WLAN EHPLMN or the I-WLAN last Registered PLMN		X
ADF USIM\DF WLAN\EF WLRPLMN	I-WLAN Last Registered PLMN to be used in fast re-selection of a WLAN network		X
ADF USIM\DF WLAN\EF HPLMNDAI	Identifies if the WLAN UE may attempt to select the HPLMN via WLANs that support non IEEE 801.1x authentication mechanisms		X

6. 3GPP/3GPP2 interworking

Some 3GPP2 MNOs require a UICC capable of supporting both LTE and CDMA. In these instances, the below requirements shall be adhered to.

In order to manage the interworking between 3GPP (2G, 3G, 4G …) and 3GPP2 (CDMA2000, HRPD, WiMAX) networks the 3GPP2 C.S0074-A V1.0 and 3GPP TS31.102 R9 specifications define a set of files that allow the UICC to store MNO preferences about the selection of the radio access technology. This is known as Multi Mode System Selection (MMSS).

Indeed, according to MNO business rules, the device has to select the most appropriate type of radio network; either 3GPP or 3GPP2. Once 3GPP or 3GPP2 has been selected, the UE follows the standard network selection procedure for the corresponding system in order to acquire a network attachment.

Operators may differentiate between voice only networks and networks that allow both voice and data depending on end user location.

The main benefit for the MNO here is the ability to manage roaming agreements between 3GPP and 3GPP2 partner networks. It also enables the MNO to deliver the utmost end user experience.

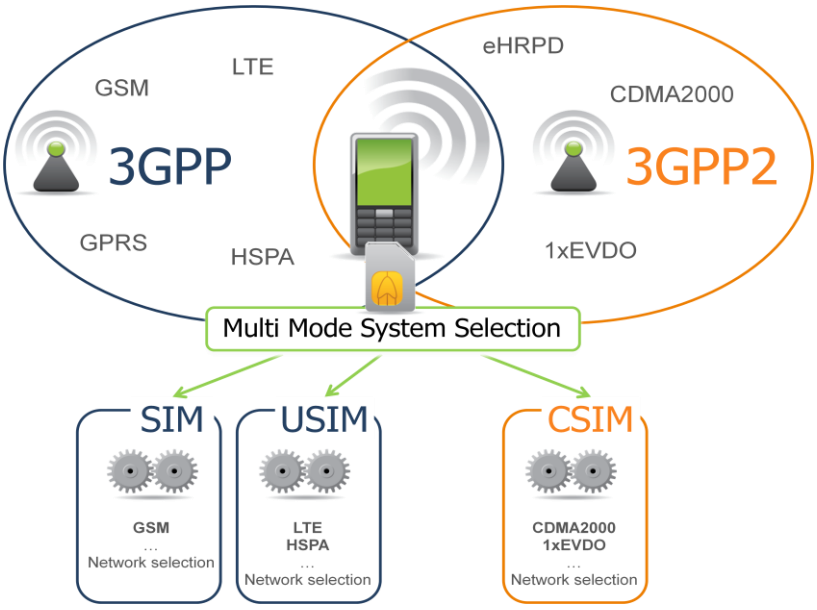

Figure 3: The versatility of the Multi Mode System Selection

The UICC shall be CSIM compatible, as described in 3GPP2 C.S0065-B, and support OTASP/PA stack to interact with CSIM for PRL and NAM parameters download, as described in 3GPP2 C.S0016-D.

The CSIM application is a Network Access Application coexisting with the USIM and hosted by the UICC providing access to CDMA2000/EVDO networks. The CSIM application supplies an extensive list of features and functionalities required to operate independently on legacy CDMA and EVDO networks.

6.1 Multi Mode Device Detection and 3GPP/3GPP2 System Selection

The following UICC parameters take precedence over those present in the terminal. When multiple systems are available, the multi mode device shall be able to automatically select the most preferred system.

UICC usage requirements	Parameter/Comment	Support	
Features		**Optional**	**Mandatory**
DF MMSS			X
EF MLPL	(MMSS Location Associated Priority List) List of grouping based on location specific information. Defines regions where system selection priorities are needed		**X**
EF MSPL	(MMSS System Priority List) List of prioritized cellular systems that assist the device in its selection. MSPL Parameters: SYS_TYP: CDMA, UMTS, LTE … PRI_CLASS: Allows for selection priority based on operator preference while roaming SYS_PRI: Indicates relative priority of technologies within the MSPL record HIGHER_PRI_SRCH_TIME: Set to the time between searches of higher priority systems of other radio access technologies NETWORK_CAP: Allows operators to specify the preference for "voice + data" network		**X**
EF MMSSMODE	(MMSS Mode Settings) Defines the selection mode: Automatic, Semi-Automatic or Manual		**X**

7. USIM Toolkit enhancement

USIM Application Toolkit (USAT) is a major Value Added Service (VAS) enabler since it helps mobile carriers to develop new revenue streams, differentiate from competitors, enhance their customers' experience and reduce churn. With the introduction of LTE, the communication protocol between the card and the handset has been enhanced with the introduction of proactive commands and events:

- Providing full management of the LTE access technology
- Allowing the integration of WiFi and femtocell offload strategies
- Enabling the deployment of GPS-based services with monitored Quality of Service (QoS)

By relying on standard capabilities which are available on all mobile handsets, the UICC allows the same application to run on any mobile device, regardless of manufacturer, and be used on every available network (2G, 3G and LTE). The LTE UICC capabilities include (but are not limited to):

- Getting the location data from a GPS-enabled handset in order to enhance the information of menu-based browsers, enabling the definition of "geo fences" for location-based advertising, etc.
- Enabling sophisticated "femtozone" services when the end user enters or leaves a defined femtocell.
- Proactively detecting, diagnosing and solving issues caused by connection problems or unsubscribed services.

Ensuring a high quality of service has become a real challenge for MNOs seeking to acquire and retain customers who are increasingly accustomed to anytime, anywhere, seamless and transparent access to mobile services.

The LTE UICC can be utilized as a tool to provide tailored, real-time solutions to the issues that affect the customer experience when accessing LTE networks and services. For example, if a subscriber hasn't activated their mobile data option when roaming, the LTE UICC could detect this and, upon user confirmation, activate it to ensure mobile internet remains available to the subscriber.

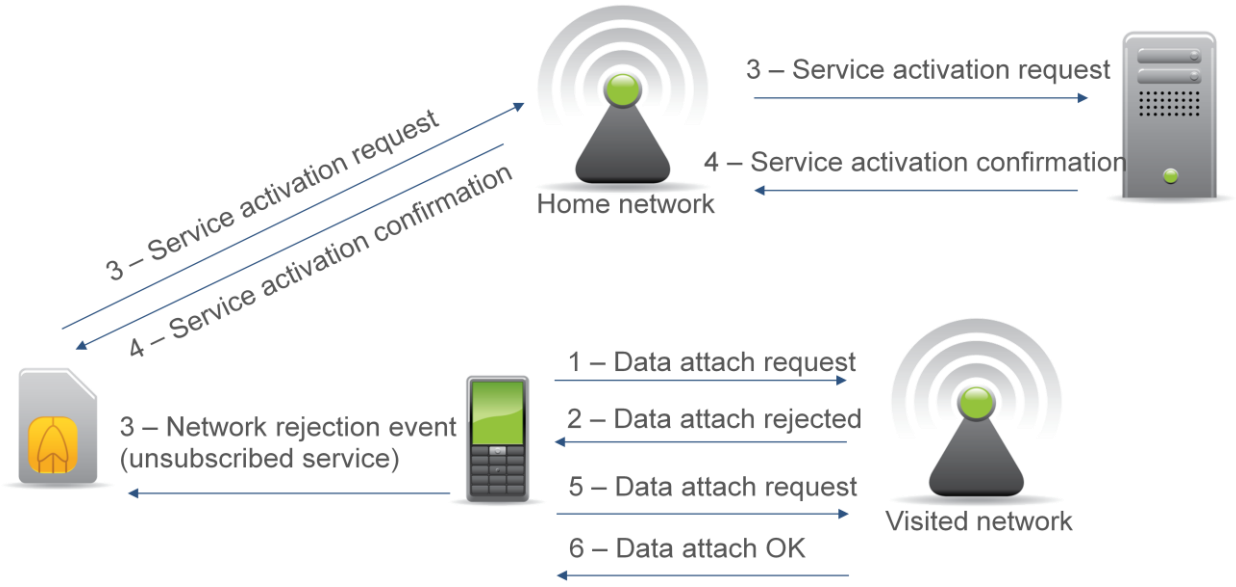

Figure 4: The LTE UICC can intelligently detect and activate services to enhance the user's experience

Femtocells offer an efficient and cost-effective way of offloading the traffic from the macro-cellular networks and therefore improve the experience of users in terms of high-quality coverage. In addition to carrying the femtocell access control parameters, the LTE UICC could also give MNOs the ability to manage subscriber devices remotely by triggering a device management session when entering a defined femtocell. This service would give subscribers the possibility to regularly and automatically backup their phonebook, receive appropriate new services, etc.

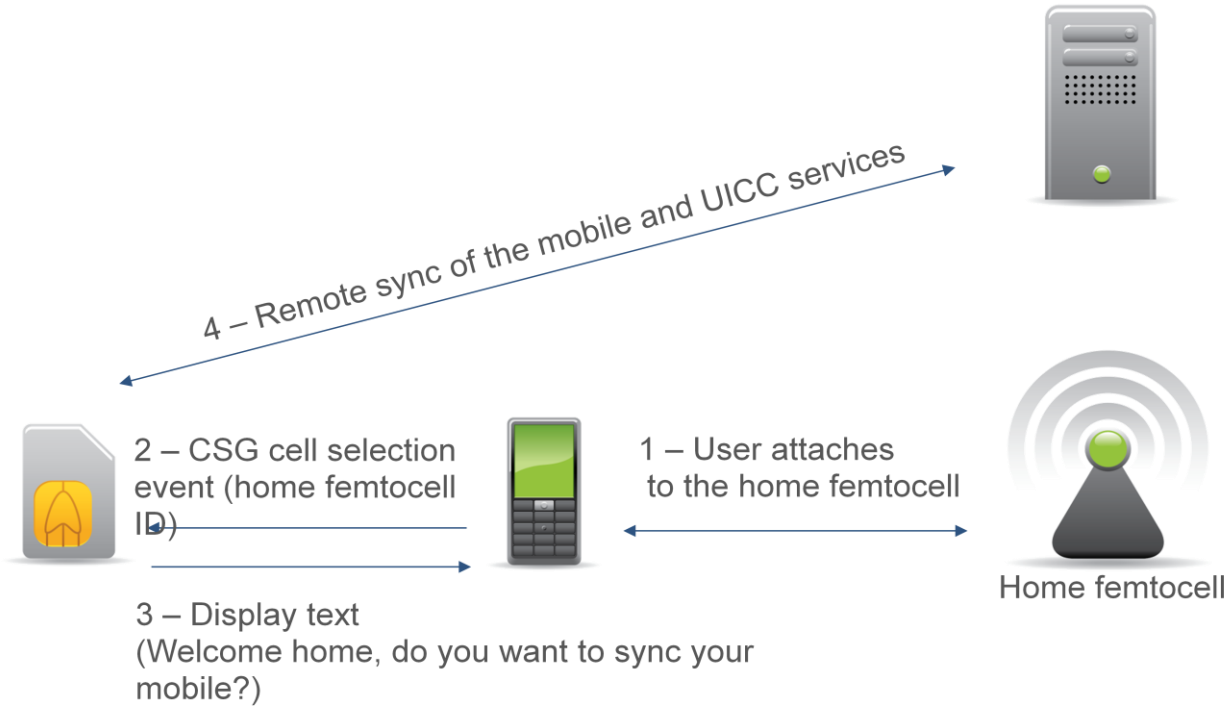

Figure 5: How MNO's could use the LTE UICC to trigger device management sessions via a femtocell

7.1 Enhanced event and proactive command

The ETSI TS 102 223 Release 8, the 3GPP TS 31.111 Release 8 and the 3GPP2 C.S0035 specifications describe the enhancements to the USIM Application Toolkit (USAT).

UICC usage requirements	Parameter/Comment	Support	
Features		Optional	Mandatory
CSG Cell Selection Event	From Release 9, CSG Cell Selection Event to inform the UICC on leaving or entering into CSG cell coverage or detecting a change in its current CSG cell selection status.		X
Discovery of surrounding CSG cells in Provide Local Information	From Release 9, the discovery of surrounding CSG cells in Provide Local Information allows the same list of CSG cells as is displayed during manual CSG selection to be obtained.		X

Call control on EPS PDN connection by USIM	From Release 8, the call control on EPS PDN connection by USIM forces the ME to first pass the corresponding data to USIM before any EPS PDN connection activation.		X
Service n°87 in the EF UST	Informs the ME that the UICC is able to manage all the related procedures and commands for Call control on EPS PDN connection by USIM.		X
Network Rejection Event	From Release 8, Network Rejection Event UTRAN allows the UICC to retrieve the network rejection codes when network issues prevent connection.		X
Steering of Roaming for I-WLAN	From Release 8, this extension of the Refresh command allows the MNO to remotely "force" a handset to run a I-WLAN network selection procedure with appropriate parameters.		X
Geographical Location Request	From Release 8 Geographical Location Request provides a solution to acquire GPS localization information from the device.		X
EPS support for OPEN CHANNEL BIP command	Bearer Type eUTRAN must be supported in addition to legacy modes (GPRS, UTRAN, etc…)		X
Provide Local information extended to support LTE.	Location Information : ME provides to UICC information on MNC, MCC, LAC/TAC, Cell ID, extended cell ID E-UTRAN cell ID Network measurement result: extended to E-UTRAN Current access technology: extended to E-UTRAN		X

8. Over The Air UICC administration

LTE will multiply the range of services offered to end users and will therefore also increase the number of applications on the UICC that require OTA administration.

At the same time, LTE introduces an all-IP environment suitable for OTA exchanges for administration between the UICC and Server which can be done through HTTP (as it is described in Global Platform 2.2 Amendment B: "Remote Application Management over HTTP"). Each card acts as an HTTP client and the OTA platform as an HTTP server.

LTE networks provide increased bandwidth, downloading success rates and low latency for transmissions.

Consequently, MNOs can reap a number of benefits from these improvements:

- Reliability: success on massive application updates.
- Performance: OTA servers can access and upgrade contents and applications faster than before.
- Secured administration: highest level of security in IP environments is attained due to the addition of secure HTTP or HTTPS (HTTP over TLS) as GP 2.2 Amendment B describes. NFC and IMS services can also be secured in this way.

End-users benefit from:

- Faster and seamless activation of new services.
- Secured administration: highest level of security in IP environments is attained due to the addition of secure HTTP or HTTPS (HTTP over TLS) as GP 2.2 Amendment B describes.

The addition of the polling mechanism, which allows applications to connect periodically to OTA server and check for updates, is another benefit provided by this kind of advanced OTA platform.

LTE provides great potential for OTA applications to meet the new expectations of subscribers:

- Automatic and immediate access to LTE voice and multimedia services (ISIM personalization with end user public identities)
- SCWS services personalization and administration
- Traffic preferences
- Remote applet and file management (banking applications, NFC services, etc)

The OTA over HTTPS process starts by sending a PUSH SMS (step 1, figure 6, below) embedding the OTA server connection data. This information is needed by the UICC to open a BIP channel and then a TCP/IP connection with the OTA server (step 2, figure 6, below).

TLS is widely deployed in the IP world to establish secure TCP communications and, combined with HTTP protocol, makes HTTP secure (HTTPS). In fact, PSK TLS (Pre-Shared Key TLS) allows mutual authentication between the UICC (HTTPS Client) and OTA server (HTTP Server); both share a secret key. The authentication procedure is called PSK TLS Handshake (step 3).

After a successful authentication, step 4 consists of an administration stage. A HTTPS Request connection (POST command) with OTA HTTPS Server is started by the UICC. The OTA Server then

sends a HTTPS Response with an encapsulated remote command APDU to the UICC. RAM and RFM applications (ETSI 102 226) from UICC then process this command information and administrate or upgrade a corresponding file or application. The UICC will then inform the OTA server of the administration command success by sending a HTTPS Request (POST command) with an embedded R-APDU.

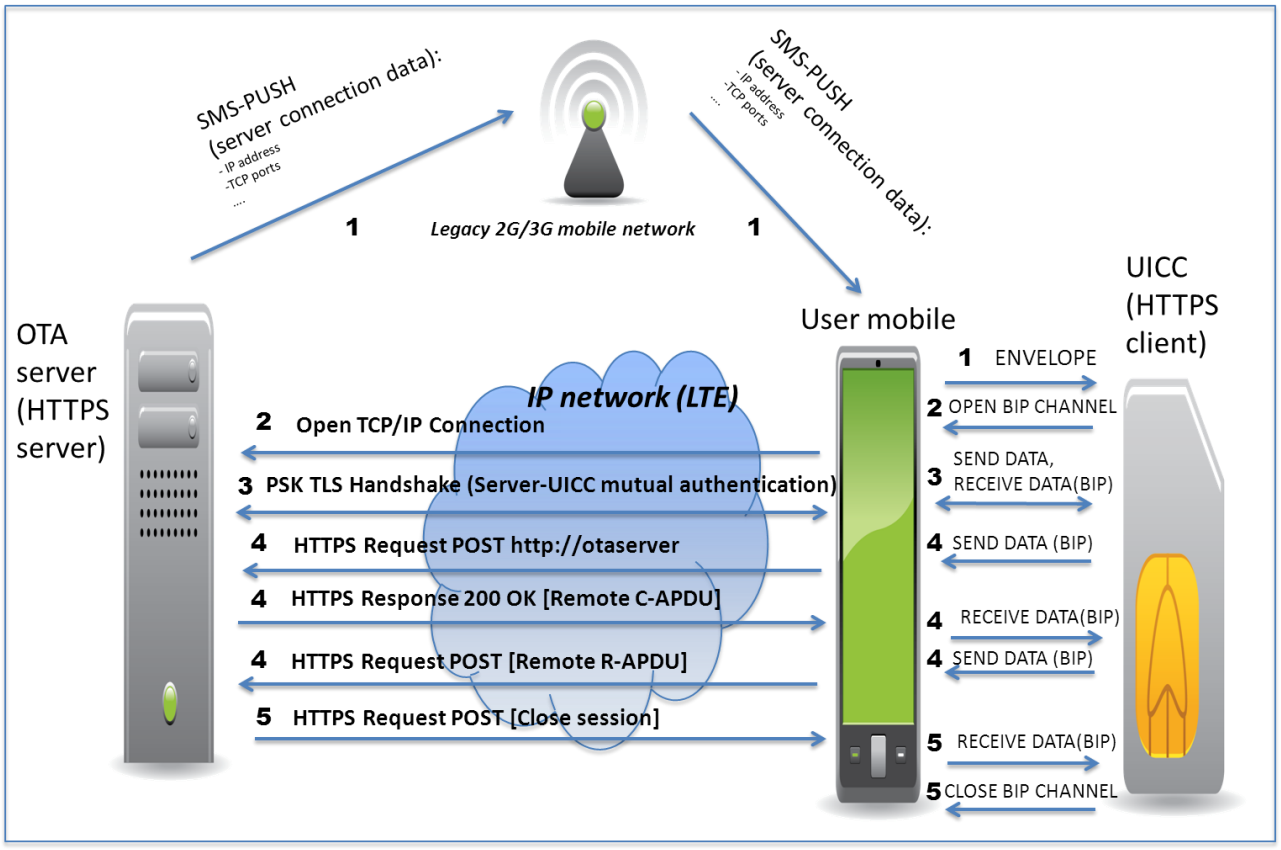

Figure 6: A model for OTA UICC administration

LTE UICC should comply with the following OTA features:

UICC usage requirements	Parameter/Comment	Support	
Features		**Optional**	**Mandatory**
OTA over HTTP(S)	The UICC shall support Global Platform 2.2, Amendment B: "Remote Application Management over HTTP"		X
RAM / RFM	The UICC shall support ETSI TS 102 225 (Secured Packet) and ETSI TS 102 226 (Remote File and Application Management), both for Release 9		X
Bearer interface transport level	The UICC shall support interface transport level: - '01' for UDP/CAT-TP for backward compatibility purpose. - '02' for TCP	X	X

9. Generic Bootstrapping Architecture (GBA)

As has been mentioned in previous chapters, the increase in both the number and sophistication of new mobile services inevitably gives rise to new technical challenges. One such challenge is mobile user credentials management. Subscribers are already known to struggle with the need to manage a large number of unique passwords, with many resorting to reusing the same password (or a close variant) across numerous services, thus compromising the effectiveness of the overall model.

Generic Bootstrapping Architecture (GBA) benefits users by authenticating them across several services by utilizing their valid user identity. This valid identity shall be also located in the Home Location Register (HLR) or a Home Subscriber Server (HSS), both in the MNO's infrastructure. In this way, operators can benefit by acting as an identity or authorization verifier to service providers over the internet or over IMS.

The user authentication is achieved by AKA authentication, i.e. a shared secret between the smart card inside the mobile phone and the HLR/HSS, by making a network component challenge to the SIM card and verifying that the answer is identical to the one expected by the HLR/HSS.

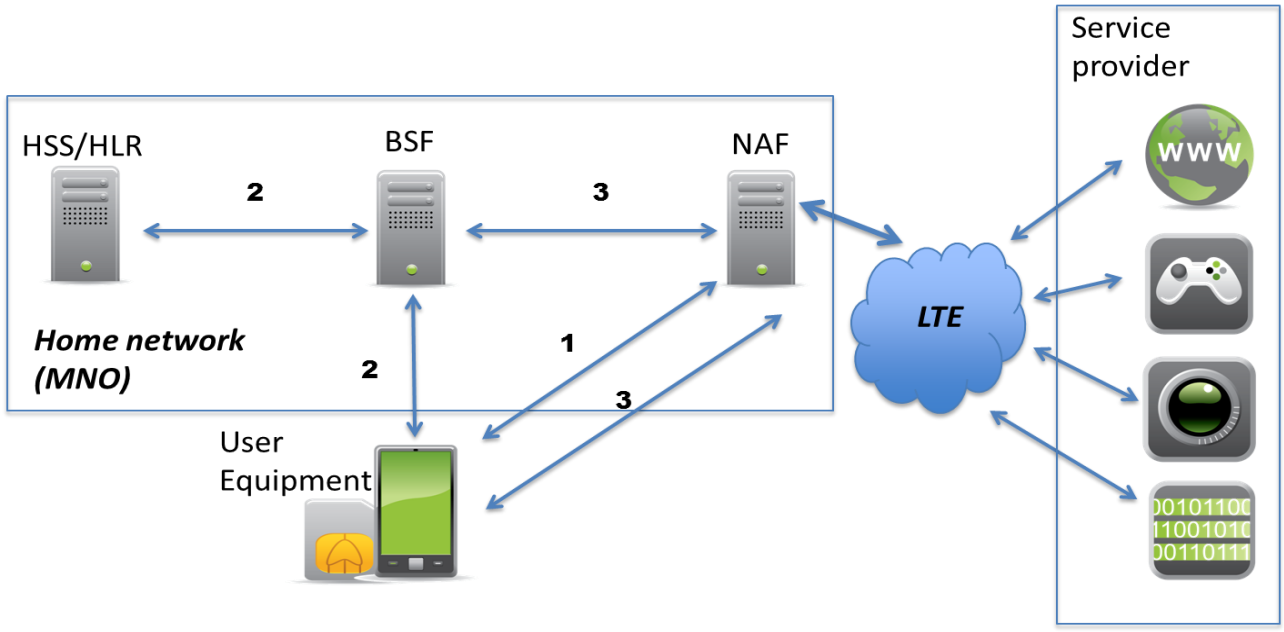

Figure 7: A model of Generic Bootstrapping Architecture

GBA refers to an architecture/network which implements several procedures and performs different methods of authentication. The network components required for GBA are:

- **User Equipment (UE):** The user is subscribed to a set of services (data traffic, IP multimedia services such as Mobile TV, streaming, VoLTE, etc.)
- **Bootstrapping Server Function (BSF) and HSS/HLR:** Both are responsible for the authenticating bootstrapping process; this means the authentication of the UE to the home network and the creation of session keys for the user.

- **NAF (Network Application Functions):** Session keys derived from authenticating bootstrapping process allow users to communicate with NAF and enjoy subscribed services.

The usage of GBA can be divided in to three steps (see figure 7 above):

1) User Equipment wants to use a subscribed service but it does not know if the NAF requires GBA authentication for this. UE contacts NAF and the latter indicates a bootstrapping initiation is required.
2) User Equipment starts the **authentication bootstrapping procedure.**
3) User Equipment starts the **bootstrapping usage procedure.**

Authentication bootstrapping procedure:

The user starts introducing the identity. Then, secure communication between mobile web browser and BSF is achieved through HTTP Digest. A great advantage here is that usually Web servers and device browsers have already implemented HTTP Digest, making this solution easy to deploy for GBA infrastructures.

Figure 8, below, describes the procedure:

- The user introduces the identity in the browser and it is sent embedded in a HTTP Response to the BSF server.
- BSF requests to HSS/HLR the security information related to the user (i.e. shared secret key, random number, user security settings, etc.). Then BSF sends a HTTP Digest Response with the random number and a starting key session.
- UICC launches AKA authentication from received parameters and derives the expected response (RES). If RES matches with SRES in BSF, the user will be successfully authenticated.

BSF notifies UE of the authentication success by sending a B-TID and both parts derive the same key sessions (Ks) from Kc, expected responses SRES and the starting key session.

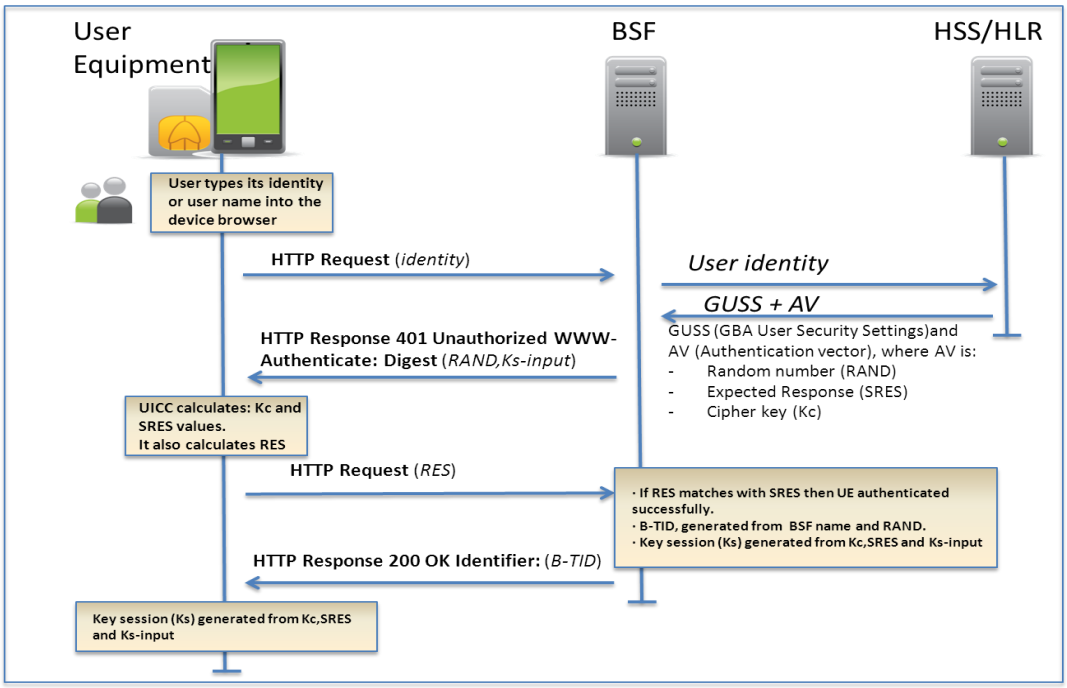

Figure 8: The authentication bootstrapping procedure

Bootstrapping usage procedure:

The usage of session keys (Ks_NAF derived from Ks) and received B-TID allow the mobile user to request an application NAF. After this NAF authenticates itself to BSF in order to purchase session keys. BSF will return derived Ks_NAF. Finally, UE and NAF are authenticated and subscribed services can be requested from UE to NAF.

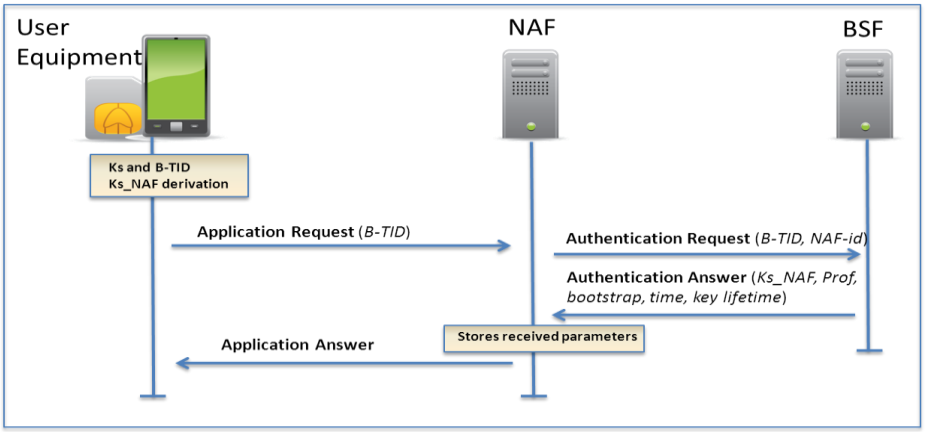

Figure 9: The bootstrapping usage procedure

9.1 Generic Bootstrapping Architecture within a LTE USIM

The 3GPP TS 33.220 (Release 8) specifications describe a set of features to enable Generic Bootstrapping Architecture in the UICC.

UICC usage requirements	Parameter/Comment	Support	
Features		Optional	Mandatory
USIM Service Table: Service N° 68	Generic Bootstrapping Architecture (GBA) activation		X
ISIM Service Table: Service N°2	Generic Bootstrapping Architecture (GBA) activation. GBA is managed by ISIM.		X
EF$_{GBABP}$: GBA Bootstrapping parameters	This EF contains the AKA Random challenge (RAND) and Bootstrapping Transaction Identifier (B-TID) associated with a GBA bootstrapping procedure.		X
EF$_{GBANL}$: GBA NAF List	This EF contains the list of NAF_ID and B-TID associated to a GBA NAF derivation procedure.		X

10. Extended Authentication Protocol (EAP)

Wi-Fi off load is becoming increasingly relevant as LTE is introduced. Indeed the more off load that is offered to the end user, the more they are likely to consume. This trend was evident during the migration from dial-up to DSL in the fixed line environment. So leveraging the Wi-Fi asset is key in an LTE environment, in order to off load the LTE layer or event to the 2G and 3G layers. Smooth and secure authentication to this Wi-Fi layer is key here. For a mobile network, the natural answer is to leverage the UICC. Then a connection between the Wi-Fi layer and the cellular layer is required to leverage the cellular credential stored in the HSS. With this link made, the Wi-Fi layer becomes a iWLAN. EAP SIM or AKA will then be available for use on the UICC, to leverage the HSS credentials and smoothly and securely authenticate the subscriber.

This has several advantages:

- It secures the iWLAN access by leveraging the cellular credentials.
- It enhances the user experience because the end user is not required to engage in the process by entering a user-defined or other WPA password, for example.

It optimizes usage of iWLAN to off load 2G/3G/4G cellular networks according to MNO business rules
EAP (Extensible Authentication Protocol) is a framework for transporting authentication protocols suitable for identifying mobile subscribers over IP networks (ADSL and Wi-Fi).

The EAP structure is composed of several components:

- The UICC EAP Framework provides information to the terminal about the existing UICC applications that provide UICC EAP clients.
- A UICC application provides one or more UICC EAP clients.
- A UICC EAP client implements one specific EAP method, EAP AKA being the most secure version leveraging millenage cryptography.

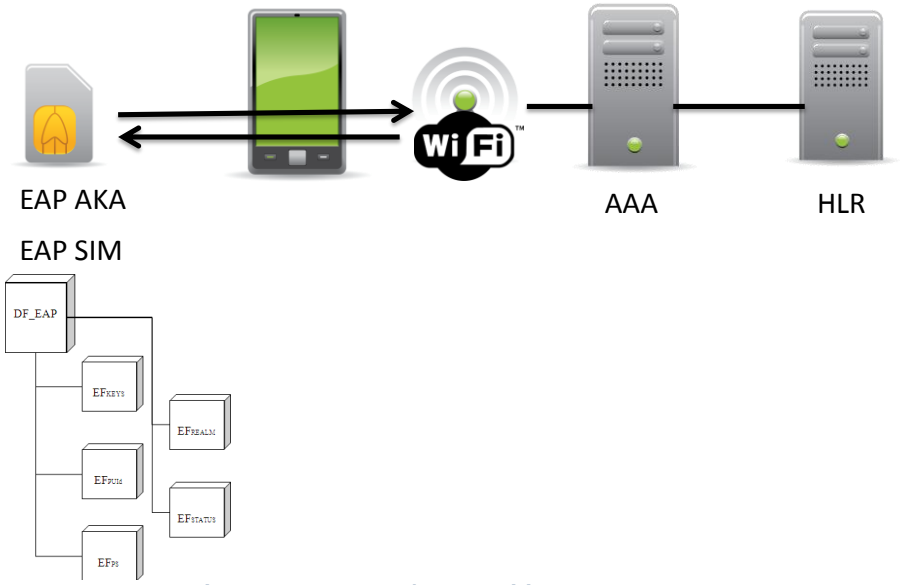

Figure 10: EAP SIM/AKA architecture

Having the EAP implemented on the UICC has several advantages compared to an implementation that is split between the device and the UICC:

- It becomes less device dependent and leverages one key benefit of the UICC: that it is removable and can be ported onto other devices with associated user credentials.
- EAP AKA cannot be implemented onto the device. This version of EAP leverages the USIM capabilities, offering better security.

10.1 EAP authentication capabilities in the LTE USIM

The ETSI TS 102 310 v9.0.0 specifications document defines additional features that shall be provided by the UICC to support EAP authentication capabilities.

The goal of these features is to adapt the UICC to provide support for different EAP methods, ensuring interoperability between the UICC and any terminal, independent of their respective manufacturers.

UICC usage requirements	Parameter/Comment	Support	
Features		**Optional**	**Mandatory**
EAP Clients Discovery	When a UICC application implements one or more EAP clients, EF$_{DIR}$ corresponding record shall contain EAP related Data Objects.		**X**
EAP-capable-application selection	The terminal shall use the information in EF$_{DIR}$ file if available to present the list of EAP-capable applications to the user or to any application that may request an EAP authentication.		**X**
EAP Derived Keys: EF$_{EAPKEYS}$	Containing the key material derived after a successful EAP authentication: - Master Session Key (MSK) - Extended Master Session Key (EMSK)		**X**
EAP Authentication STATUS: EF$_{EAPSTATUS}$	Authentication status related to the EAP client supported by the application.		**X**

EAP AKA shall be implemented according to 3GPPTS 33.234.

11. NFC

Near Field Communications (NFC) moves the game on yet further. Often running in tandem with LTE roll-outs, NFC's ability to allow a mobile device to securely 'talk' to a similarly connected neighbouring device held within a proximity of four or five centimeters has opened up a host of contactless payment opportunities that have already found their way onto the high street.

Also, by integrating NFC technologies in the UICC, the operator is able to offer its subscriber a seamless experience between the virtual and real worlds.

NFC technology transforms the mobile phone into a universal and secure remote control to access multiple localized and contextualized services. Without doubt, NFC will revolutionize the way we interact with our environment. And with LTE migration and NFC roll-outs coinciding in many markets, it makes sense to examine the possibilities of the technologies together.

12. Femtocell (HeNB) provisioning information

The 3GPP standard defines in the TS 31.102 that the UICC shall implement the storage of ***end user*** H(e)NB parameters (Release 8) and the ***operator*** H(e)NB parameters (Release 9).

The role of the UICC is to provide relevant information to the device in order to select and try to get access to the most appropriate Femtocell according to business rules defined either by the operator or by the end user's preferences. The UICC doesn't control the access; this is managed by the MNO's back end.

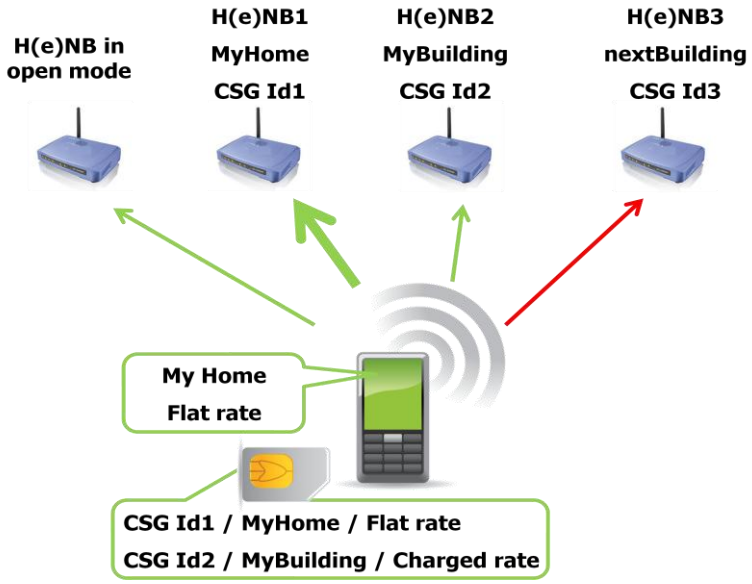

Figure 11: A model for Femtocell provisioning

The following UICC information takes precedence over that which is stored in the Mobile Equipment:

- **Allowed Closed Subscriber Group lists:** list of members, that are allowed to access to the Femtocell
- **Close Subscriber Group Type**: gives indication on billing type
- **Home eNodeB Name:** human readable name to be associated with CSG ID

Please also refer to the SIM Toolkit enhancement related to event and proactive commands for Femtocells in Chapter 7.

12.1 H(e)NodeB provisioning in TS 31.102 Release 8

UICC usage requirements	Parameter/Comment	Support	
Features		Optional	Mandatory

H(e)NB related files in USIM TS 31.102 Release 8	Definition of H(e)NB parameters		X
EF UST Service	N°86 Allowed CSG Lists and corresponding indications DF_HNB must be present under ADF USIM if the service is activated		X
ADF USIM/DF_HNB id 5F50	DF H(e)NB		X
EFACSGL id 4F81	Allowed CSG Lists		X
EFCSGT id 4F82	CSG Type		X
EFHNBN id 4F83	Home NodeB Name		X

12.2 H(e)NodeB provisioning in TS 31.102 Release 9

In addition to User H(e)B parameters the TS 31.102 Release 9 defines the same parameters for the MNO.

UICC usage requirements	Parameter/Comment	Support	
Features		Optional	Mandatory
H(e)NB related files in USIM TS 31.102 Release 9	Definition of Operator H(e)NB parameters		X
EF UST	Service N°90 Operator CSG List and corresponding indications DF_HNB must be present under ADF USIM if the service is activated		X
ADF USIM/DF_HNB id 5F50	DF H(e)NB		X
EFACSGL id 4F84	Operator CSG List		X
EFCSGT id 4F85	Operator CSG Type		X
EFHNBN id 4F86	Operator Home NodeB Name		X

13. LTE roaming optimization

Public Land Mobile Network (PLMN) identifies a specific network and its country of origin. MNOs need this information for roaming and billing purposes.

As 3GPP TS 31.102 and 3GPP TS 23.122 indicates, at mobile device and UICC initialization time, the USIM checks the content of listed PLMNs to be accessed. In addition, "PLMN Lists with Access Technology" files contains radio access technologies, i.e. the way the device shall connect (GSM, UTRAN, etc.) to the MNO network. LTE (E-UTRAN) has been introduced in the list of reachable radio technologies in those files.

PLMNs with Access Technologies are given in a preferred order (roaming preferences) and are selected in priority order (if the network is available). By setting up these files, MNOs can provide the same data connectivity or access technology to users on other visited networks as they do on their Home network.

Services for reading PLMN files execute at initialization time. Firstly Home PLMNs are checked (EF HPLMNwAct). Then, visited network may be selected (e.g. roaming). In Figure 12, below, an example of usage of EF HPLMNwAct and EF OPLMNwAct is shown when the user leaves the country of the Home Network ("Country1") and moves to another country ("Country2"). Once the user powers on the mobile and the UICC, USIM application checks that Home Network is not reachable and discovers E-UTRAN visited network called "Network1". Following the roaming agreement, if E-UTRAN is not reachable, the user can connect to another MNO ("Network3") by UTRAN.

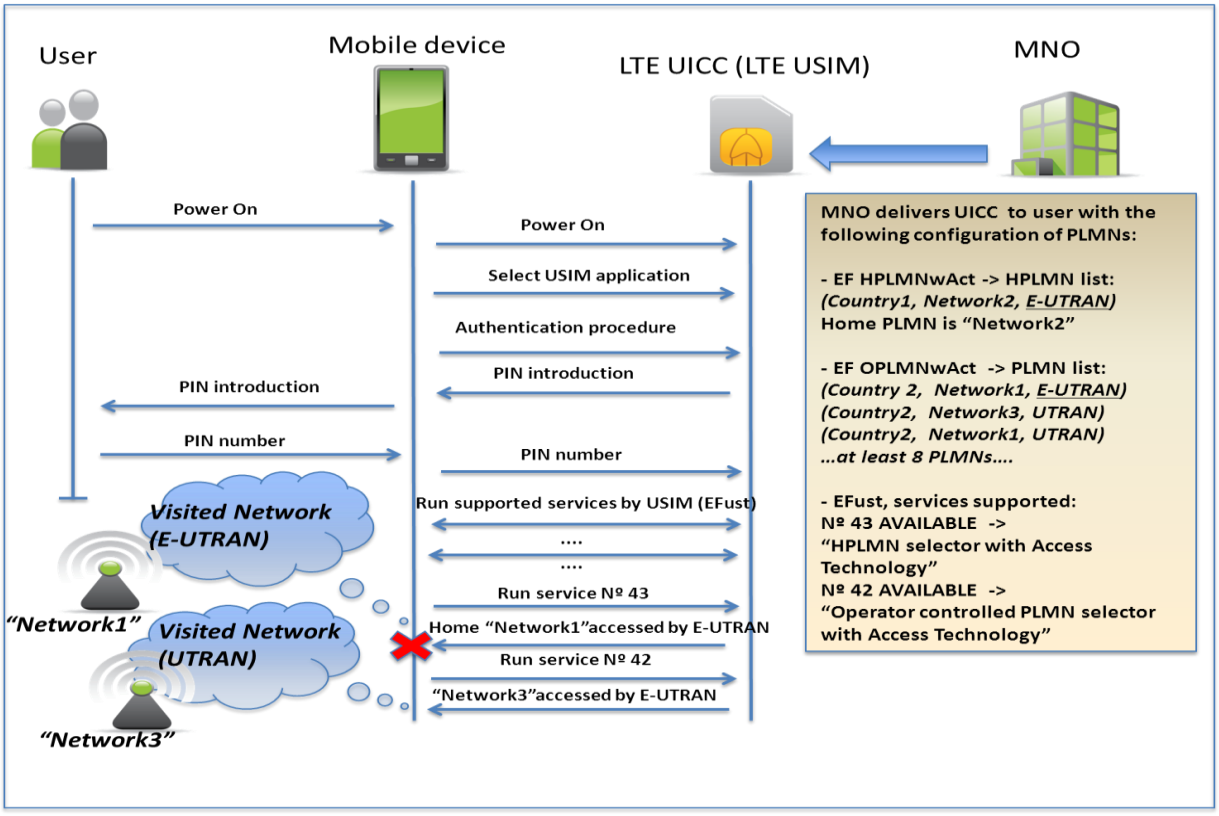

Figure 12: A model of LTE roaming optimization

If the operator delivers a UICC with EFPLMNwAct activated and service nº20 enabled, it lets the user to configure the list of preferred PLMNs. On the next initialization process PLMNs from this file will be read by the USIM again.

13.1 PLMN List with Access Technology

EF PLMNwAct, EF OPLMNwAct, EF HPLMNwAct are defined in the 3GPP TS 31.102 (USIM, Release 8). Access Technology Identifier in PLMN files is extended to support E-UTRAN radio access technology.

UICC usage requirements	Parameter/Comment	Support	
Features		**Optional**	**Mandatory**
ADF USIM/EFPLMNwAct	This information is determined by the user and defines the preferred PLMNs of the user in priority order *(See Note1)*		**X**
ADF USIM/EFOPLMNwAct	This information is determined by the operator and defines the preferred PLMNs in priority order *(See Note1)*		**X**
ADF USIM/EFHPLMNwAct	The HPLMN Selector with access technology data field contains the HPLMN code, or codes together with the respected access technology in priority order		**X**

Note 1: EFPLMNwAct and EFOPLMNwAct shall manage at least 80 networks and preferably 100 in their list of networks

14. Appendix

14.1 Other useful features

UICC usage requirements	Parameter/Comment	Support	
Features		**Optional**	**Mandatory**
DF Telecom \ $EF_{ICE\ DN}$	(In Case of Emergency – Dialing Number) This EF contains one or several call numbers (family, doctor, hospital, etc.)	X	
DF Telecom \ EF_{ICE_FF}	(In Case of Emergency – Free Format) This EF contains ICE information (for instance: blood type, specific medication, etc.)	X	
eCall support indicated in EF UST.	(Emergency Call) eCall mode. Described in TS 31.102 Release 8	X	
eCall procedures as described in TS 31.102 Release 8	UE in eCall only mode: - FDN service enabled (numbers are provided here) UE in eCall + normal mode: - 2 last entries of EF SDN (numbers are provided here)	X	

15. Abbreviations

For the purposes of the present document, the following abbreviations apply:

Abbreviation	Description
ADF	Application Dedicated File
APDU	Application Protocol Data Unit
ATR	Answer To Reset
BIP	Bearer Independent Protocol
CAT	Card Application Toolkit
CCA	CDMA Card Application Toolkit
CLK	Clock signal
CSFB	Circuit Switch Fallback
CSIM	CDMA Subscriber Identity Module
EAP	Extensible Authentication Protocol
EF	Elementary File
eMBMS	evolved Multicast Broadcast Multimedia Service
EPC	Evolved Packet Core
EPS	EPC + E-UTRAN
GND	Ground
GSM	Global System for Mobile communications
IMEI	International Mobile Station Equipment Identity
IMEISV	International Mobile Station Equipment Identity Software Version
IMS	IP Multimedia Subsystem
ISIM	IP Multimedia Services Identity Module
ISO	International Organization for Standardization
LAC	Location Area Code
LTE	Long Term Evolution
MCC	Mobile Country Code
ME	Mobile Equipment
MEID	Mobile Equipment Identifier
MNC	Mobile Network Code
MS	Mobile Station
NAA	Network Access Application
NAS	Non Access Stratum
NFC	Near Field Communication
NVM	Non Volatile Memory
OMH	Open Market Handset
PPS	Protocol and Parameter Selection
RAM	Remote Applet Management
RFM	Remote File Management
SAC	Secure Authenticated Channel
SCWS	Smart Card Web Server
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SMS-PP	Short Message Service – Point to Point
SWP	Single Wire Protocol
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
VCC	Voice Call Continuity