Securing **mobility**
and **beyond**

idemia.com/**solution/connectivity**

Join us on

www.idemia.com

WHITE PAPER

IP Multimedia Services Identity Module. What role does it play in IP Multimedia Subsystem (IMS)?

IP Multimedia Subsystem (IMS) is a way for mobile operators to aggregate all multimedia Internet services in a standard way and offer those services to end users. It was originally standardized by the wireless standards body 3rd Generation Partnership Project (3GPP) to ease this fixed-mobile convergence. However, the real take-off of this technology comes with the migration of mobile operators to Long Term Evolution (LTE) networks. There is no longer a Circuit Switch (CS) to carry voice as was the case in 2G or 3G networks because LTE networks are becoming all-IP networks. Voice is instead sent using IMS over LTE. Therefore, if cell operators are switching to LTE and wish to provide voice services over LTE, they must introduce IMS networks over LTE.

With IMS, end users can receive many more services than just voice. For instance, Rich Communication Services (RCS) give end users the ability to communicate with anyone listed in their mobile address book via instant messaging, chat, file transfer, and more across any device and network. Many mobile operators are now implementing this RCS.

So, what is the most effective way to register subscribers for this IMS layer? Access to voice services via LTE needs to be secured and mobile network operators (MNOs) must keep public and private identities that are no longer necessarily connected to the IMSI. Doing this registration through the IMS Subscriber Identity Module (ISIM) program on the SIM card has a number of benefits. Since it recycles all the Universal Subscriber Identity Module (USIM's) security components, it may share security features with USIM and supports storing both public and private identities.

When IMS applications are offered by third parties, MNOs can share the users' authentication information with third-party applications. This information is stored in o the ISIM thanks to GBA (Generic Bootstrapping Architecture) and includes secrets that help to verify the identity of the user.

The bottom line is that the ISIM application has been designed for IMS authentication and has been adopted by several operators deploying worldwide Voice over LTE. It is the best way to authenticate subscribers to the IMS layer.

Contents

1 What is an IP Multimedia System (IMS)?

A service integrator

In and of itself, IMS is neither a service, an application, or even a use case. In fact, IMS offers service integration, enabling the standard integration of numerous basic services from different suppliers into new applications and services (for example aggregating voice plus video, plus file sharing to create a new service composed of elementary services). IMS manages Quality of Service (QoS) for a variety of networks or services, such as IP networks and CS networks (voice or video for example). IMS offers proper billing as well, with each service potentially having a distinct price (e.g. fixed rate per unit, or based on duration, or on the amount of information).

To achieve this, IMS provides standard interfaces that can be used by service developers.

Its smooth service, interworking between data and circuit-switched networks, takes care of synchronizing session establishment with QoS provision, even in roaming mode.

Let us see now the architecture of the IMS network.

IMS architecture

The IMS architecture is a collection of functions linked by standardized interfaces.

The calls are controlled by the Session Initiation Protocol (SIP), which eases the creation of new services and inherits most of its characteristics from SMTP and HTTP.

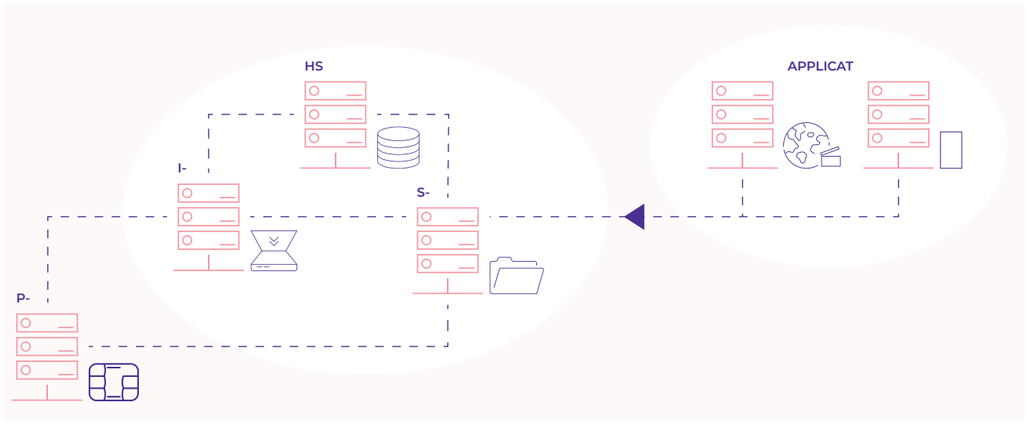


Figure 1: IMS Architecture

2 Why IMS?

Voice over LTE

Most MNOs are now migrating their network to LTE or even 5G. On the figure “3G to LTE to 5G architecture evolution” you will see above: the 3G architecture with the Core Network split into two parts:

- The Packet Switch (PS) part with the Gateway General Packet Radio Service (GGSN) and the Serving General Packet Radio Service (SGSN).
- The Circuit Switch (CS) part with the Mobile Switching Center (MSC).

In the radio access network (UTRAN in UMTS) there are still two links (CS and PS) through the Radio Network Controller (RNC).

In the middle, the LTE architecture has only one Core Network named the evolved Packet Core (EPC) including the Serving Gateway (SGW) and Packet Data Network Gateway (PGW). Gateway (PGW) and servers like the Mobility Management Entity (MME) and the Policy and Charging Rules Function (PCRF).

VoLte

VoNR 5G

Regarding 5G, there are certain similarities and variations between the two designs that can be seen when comparing the various functional entities in the EPC and the 5GC. With 5G, the roles of the EPC entities are either integrated into a single Network Function (NF) or divided into two NFs. In 5G, the Session Management Function (SMF) manages the user plane functions, while the User Plane Fuvnction (UPF) manages the control plane functions of the SGW and PGW.

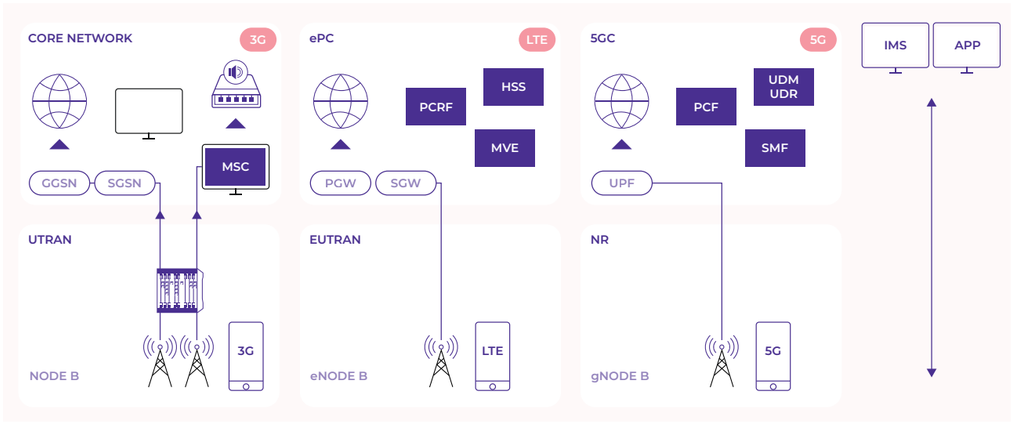


Figure 2: 3G to LTE to 5G architecture evolution

Policy and Charging Rules Function (PCRF) in EPC is equivalent to the Policy ControlFunction (PCF) in 5G. Similar to PCRF, PCF manages user plane resources and supplies pertinent charging-related information throughout a session. To apply a policy or rule, the PCRF depends on Application Function (AF) or subscriber data. Many other entities in the 5GC, including the Access and Mobility Management Function (AMF), Session Management Function (SMF), Application Function (AF), Unified Data Repository (UDR), Charging Function (CHF), and many others, provide input to the PCF. Whereas the PCF is connected to the SMF, which is then connected to the UPF, the PCRF is directly connected to the P-GW. As a result, SMF will apply the policies and rules on the user plane by corresponding with the UPF when PCF develops them.

The PCRF mainly manages the QoS and charging for each session. In addition to the function carried out by the PCRF, PCF can also verify the right to access of a particular service depending on the geographical area of the subscriber.

4G	5G
Radio Access Network	
E-ULTRA	NR
eNB	qNB
Core Network Elements	
MME	AMF SMF
SGW-C PGW-C	SMF
SGW-U PGW-U	UPF
HSS AuC	UDM, UDR AUSF
PCRF	PCF

Figure 3: One to One Mapping of 4G and 5G entities

IMS Services

IMS is a standard that can aggregate services; it is not a service as is. As described in the previous paragraph, voice can be one of those services. However, some other services, such as gaming services or even broadcasting services, can be offered through an IMS network. Those services can be provided either by the MNOs or by third parties.

Another common IMS service is the so-called Rich Communication Services (RCS). This service provides Mobile Network Operators voice and messaging services with an all-IP network—LTE for example.

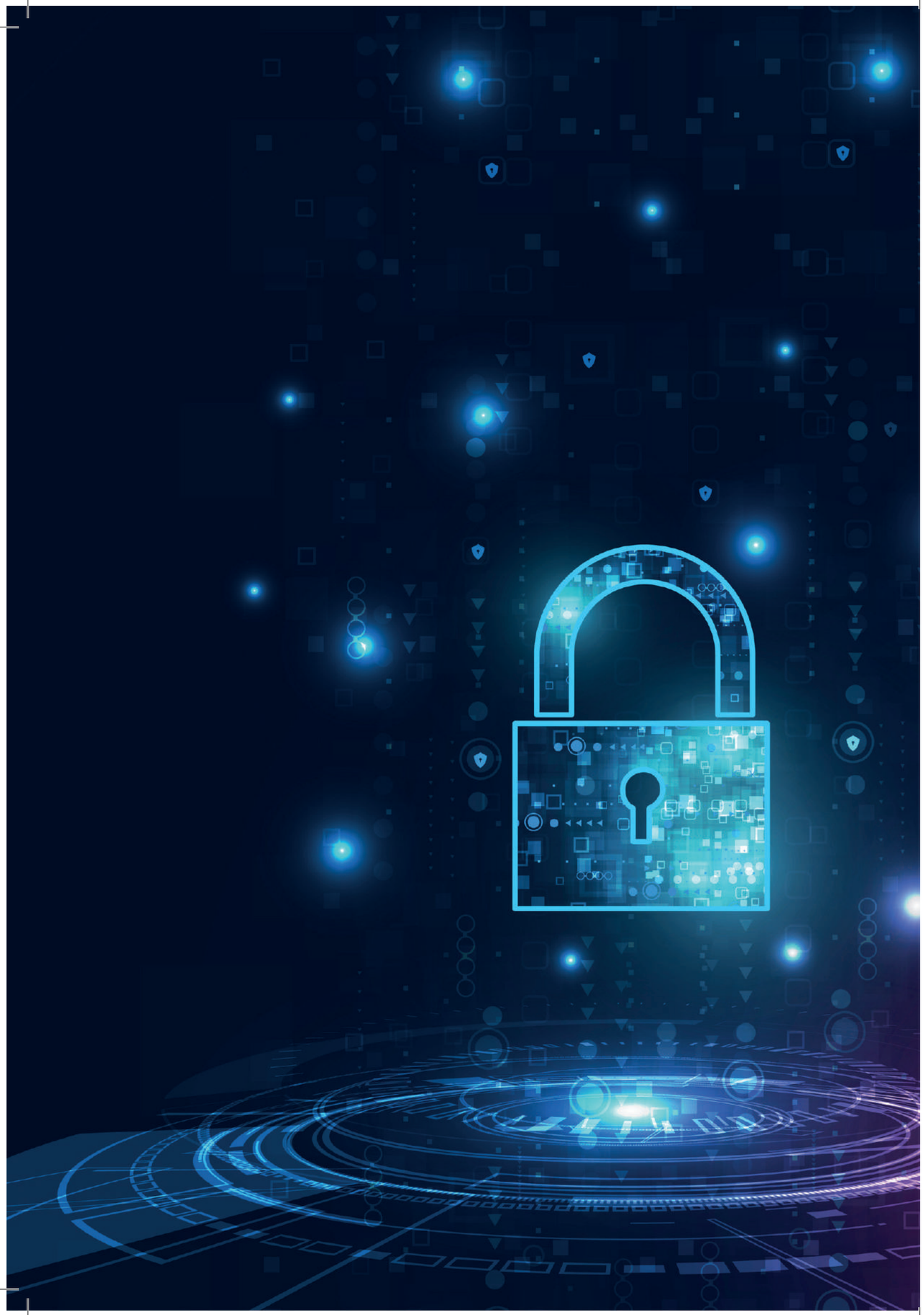
For subscribers, IMS opens up a whole new world of services. For operators, IMS is the guarantee of delivering cost-effective services quickly and efficiently while still providing quality and controlling ARPU.

Technically speaking IMS provides:

› Integrated services: which allows to merge a multiplicity of elementary Internet services from distinct providers into one or more “killer applications”, such as voice mail + text-to-speech conversion = text messages for blind users.

› With the best Quality of Service (QoS): including faster and continuous communications, with optimized bandwidth,

› and with appropriate charging: each service may possibly be charged independently e.g., fixed rate per unit, or based on duration, or based on the amount of information



3 IMS Security

Identification in IMS

Public user identities

An IMS user is allocated one or more Public User Identities used for routing SIP requests. These identities are typically used as contact information on business cards. A Public User Identity is to the IMS what an MSISDN is to GSM/UMTS. Technically, the Public User Identity is either a SIP URI (Uniform Resource Identifier) as defined in RFC 3261 (typically “sip:first.last@operator. com”) or a TEL URL (Uniform Resource Locator) as defined in RFC 2806 (typically “tel:phonenumber”) required to make a call from an IMS terminal to a PSTN phone.

IMS operators are likely to allocate at least one SIP URI and one TEL URL per user.

Private user identities

An IMS user is allocated one or more Private User Identities used for subscription identification and authentication. A Private User Identity is to the IMS what an IMSI is to GSM/ UMTS. It does not need to be known by the user, especially when it is stored in a smart card.

Technically, the Private User Identity takes the format of a Network Access Identifier (NAI, typically “username@ operator.com”), as specified in RFC 2486.

Public service identities

The concept of Public Service Identities (PSI) is introduced in Release 6 of the 3GPP specifications. A PSI is allocated to a service hosted in a Application Server (AS) and takes the format of either a SIP URI as defined in RFC 3261 (typically “sip:service@operator. com”) or a TEL URL as defined in RFC 2806 (typically tel:phonenumber).

Home network domain URL

The Home Network Domain URI is a SIP URI used when finding the address of the home network during the registration procedure.

Several possibilities for IMS service authentication

For mobile operators, securing access to IMS services is crucial, especially when this service is voice-based, as it is in LTE networks. This IMS layer can be authenticated in several ways:

- **Use of username and password**: This is unsecure as these parameters can be easily passed to several users. This authentication will not be discussed in this paper.
- **Use of a distinct ISIM (IMS SIM**) application on a UICC which:
  - Does not share security functions with the USIM; useful when IMS and network layers are not from the same provider.
  - Shares security functions with the USIM.
- **Use of a USIM applicatio**n on a UICC.

What authentication specifications are recommended?

IMS authentication keys and procedures on the user side are kept on a UICC, in accordance with 3GPP TS 33.203. There are two conceivable ADFs: ADF USIM without identity or ADF ISIM. Regardless of the ADF employed, this 3GPP TS 33.203 specification refers to ISIM as a security function.

ISIM is a term that indicates the collection of IMS security data and functions on a UICC.

The main difference between the ISIM application implementation and the USIM application implementation is that the user identity does not appear in the USIM implementation. This identity then could possibly be retrieved by another means from the network. The one voice initiative document3 and thus the GSMA recommends: “The IMS core network shall support the procedures for ISIM based authentication. Support for ISIM based authentication in the User Equipment is mandatory.”

The RCS GSMA specification4 recommends a strong authentication through the UICC, including the ISIM authentication: “IMS AKA with IPsec is the preferred long-term approach in IMS for access signaling security from a cellular PS network. Such access requires the IMS client device to possess an AKA based credential (e.g., Universal SIM (USIM)/IP Multimedia Services SIM (ISIM)) and support the “ipsec-3gpp” procedures specified in [3GPP TS 33.203] and [3GPP TS 24.229]. IMS AKA with IPsec is the access signaling approach specified for Voice over LTE (VoLTE).”

Clearly, the specifications recommend authentication through the UICC, including the ISIM application to authenticate to the IMS layer, especially for Voice over LTE services.

ISIM application description

The ISIM is the application that may be invoked on a UICC to secure access to applications in the IMS, the ISIM being standardized in 3GPP TS 31.103 “Characteristics of the IP Multimedia Services Identity Module

(ISIM) application”. The ISIM contains parameters for identifying the home domain and the user:

› The Home Domain name

› One private user identity

› One or more public user identities

IMS security is composed of access security (3GPP TS 33.203 - Access security for IP-based services) and network security (3GPP TS 33.210, UICC not involved). For 3GPP, IMS authentication keys and functions on the user side are stored on a UICC. IMS access is protected by the IMS AKA as specified in 33.203. IMS AKA and UMTS AKA implement the same mechanisms:

› A long-term secret is used for mutual authentication of user and network, and establishment of a pair of cipher and integrity keys (CK, IK).

› The authentication mechanism includes sequence control (SQN management).

This ISIM application has several advantages:

› It reuses all the security aspects of the USIM and can share the security functions with USIM.

› It allows storing public and private identities that are not necessarily linked to the IMSI as described above.

› IMS connection parameters are the property of the MNO (IMS Domain for example). The UICC offers the possibility to embed the settings for IMS.

› It has been specifically designed for IMS authentication.

IMS applications are provided by third parties. MNOs have the possibility to derive ISIM keys to allow those third parties the authentication of the end user without disclosing to them their secrets.

Generic bootstrapping architecture

The ideal way to authenticate end users to the IMS layer of the network, as we saw in the previous paragraphs, was through the ISIM application. MNOs are not required to provide their secrets to third parties who supply IMS applications, such as video or gaming, when those services are delivered by a third party. The ISIM's GBA capabilities make it possible to deduce those secrets.

The ISIM also allows IMS applications (NAF) and the user equipment to establish shared secrets based on the GBA, defined in TS 33.220. Depending on the application, the shared secrets can be used for authentication, encryption, or integrity. The ISIM may also contain the address of the P-CSCF and of the NAF key center for GBA.

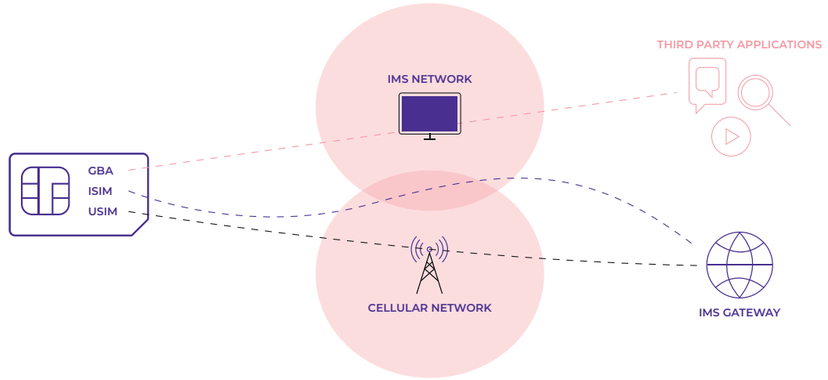


Figure 3: ISIM and GBA in cellular network

Conclusion

Voice over LTE requires IMS networks, which are becoming a reality in the cellular world. In this whitepaper, we demonstrated that the UICC's ISIM application was the most effective and secure method for performing an IMS layer authentication. In fact, ISIM was created with IMS authentication in mind.

Because of GBA, it is possible to infer the secrets from this application's secrets to reveal the authentication to third-party programs without revealing the secrets to them.

Acronyms

3GPP	3rd Generation Partnership Project
ADF	Application Data File ENODEB evolved Node B
EPC	Evolved Packet Core
eNB	Evolved Node B (radio base station in 4G LTE networks)
gNB	Next generation base station (5G radio base station that connects to 5G New Radio (NR) devices)
GBA	Generic Boostraping Architecture
GGSN	Gateway General Packet Radio Service
GSM	Global System for Mobile Communications
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISIM	IMS Subscriber Identity Module
LTE	Long Term Evolution
MME	Mobility Management Entity
MNO	Mobile Network Operator
MSC	Mobile Switching Center
NAF	Network Application Function
NFC	Near Field Communication
NODE B	Term used in UMTS to denote the base transceiver station
PCRF	Policy and Charging Rules Function
PGW	Packet Data Network Gateway
RCS	Rich Communication Services
SGSN	Serving General Packet Radio Service
SGW	Serving Gateway
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
UMTS	Universal Mobile Telecommunications System
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module