



Technical White Paper Smart Card in IMS

Feeling at home. Everywhere.

February 2007

BANKING & RETAIL

ENTREPRISE

INTERNET CONTENT PROVIDER

PUBLIC SECTOR & TRANSPORT

TELECOMMUNICATIONS > WHITE PAPER

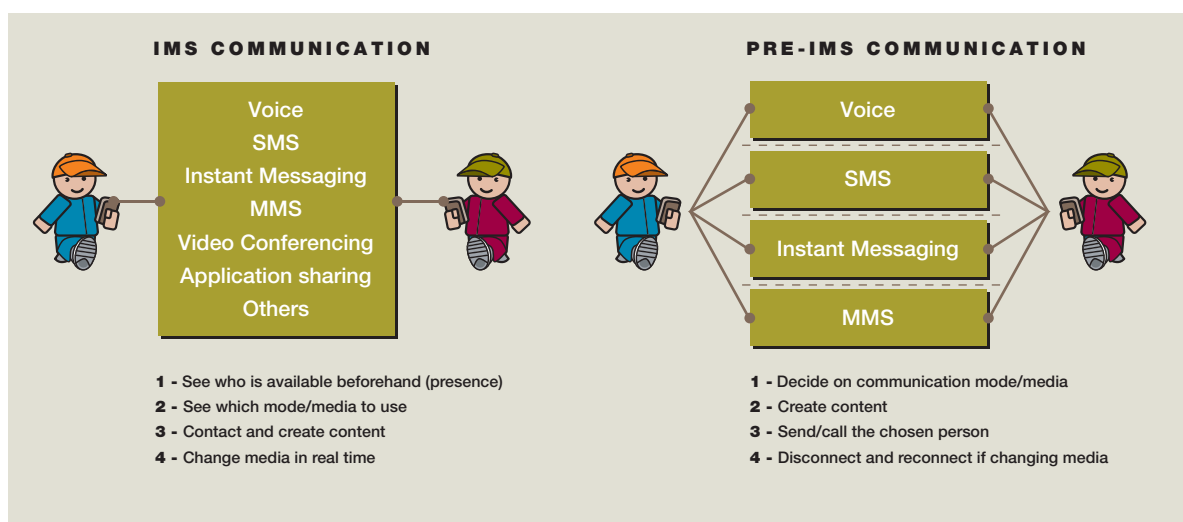
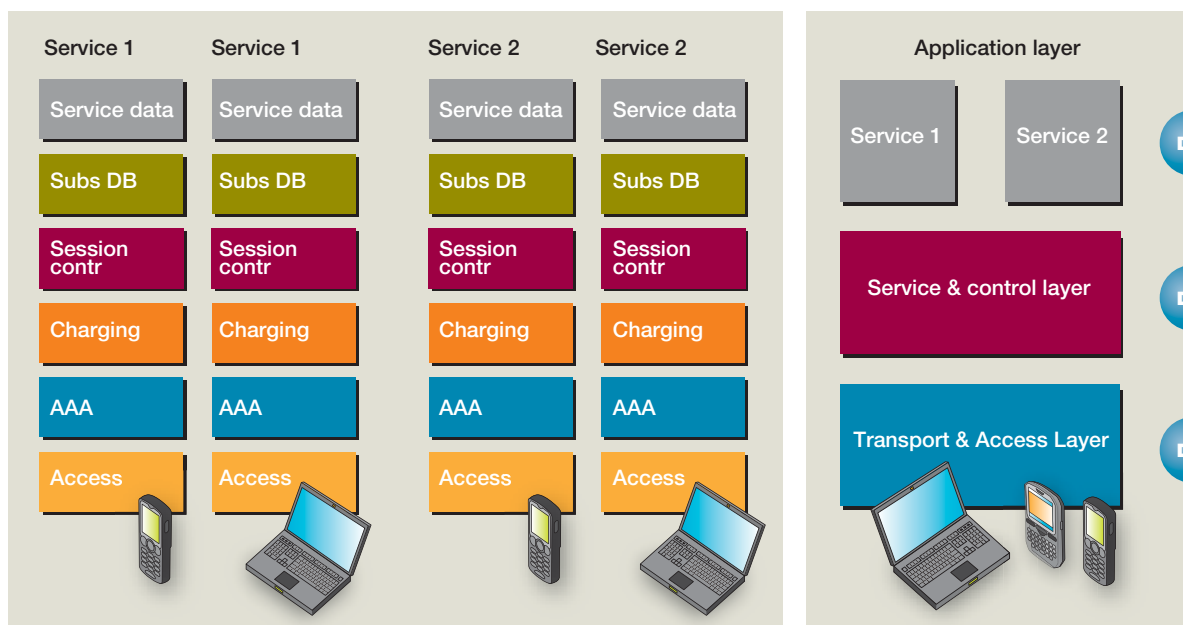
Executive summary

This white paper describes the role of the smart card in the IMS network, and the benefits to the operator of using the smart card for authenticating the subscriber, securing exchanges and managing the subscriber presence.

The IP multimedia subsystem is a core network architecture based on IP standards to enable peer-to-peer communications sessions.

IMS is an intermediate layer between the operator core network and the operator application, which offers greater flexibility in new service deployment. IMS offers system interoperability, a convergent, backward-compatible and access-agnostic platform, flexibility and ease of introduction of new applications, and gradual migration to IP.

IP Multimedia Subsystem – standard architecture uses VoIP implem. Based on SIP, runs over IP



IMS Network

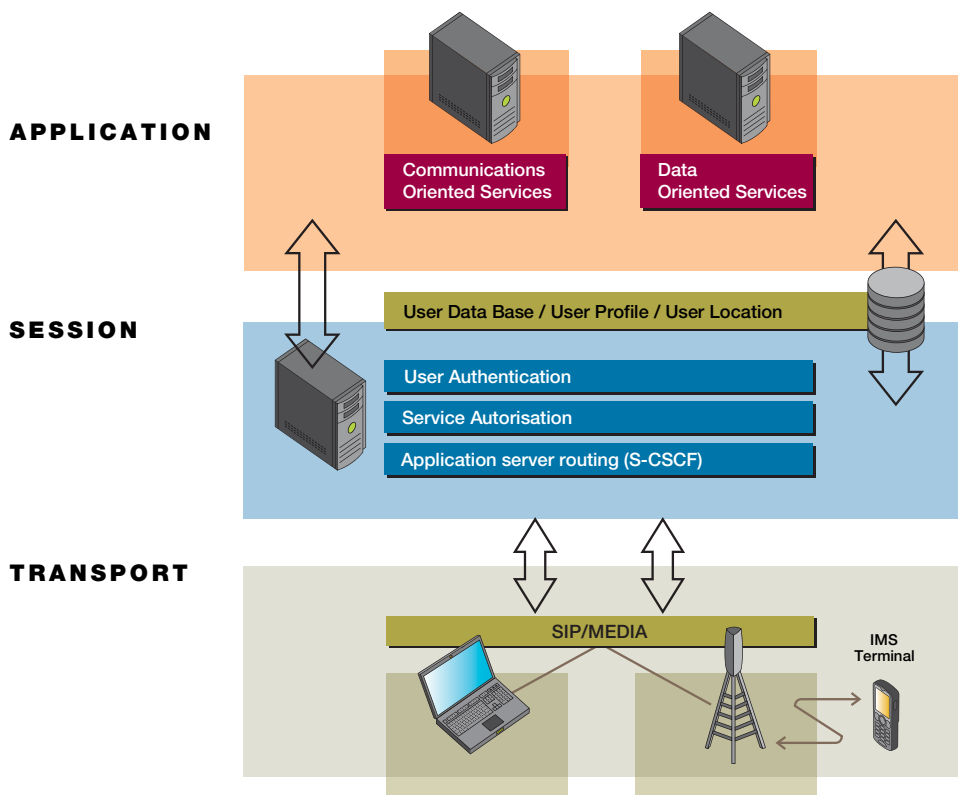
TABLE OF CONTENTS

| | |
|---|----|
| EXECUTIVE SUMMARY | 2 |
| IMS NETWORK | 3 |
| Authentication in IMS ... | 4 |
| SIP registration | 4 |
| The ISIM in the wired environment | 4 |
| ISIM Architecture | 5 |
| GBA USAGE | |
| Goal of GBA | 7 |
| STANDARDS | 9 |
| SIP CALL PROCESSING | |
| Presence and Call Processing | 9 |
| On Card, SIP User agent | 9 |
| OPERATORS' AND END-USERS' BENEFITS | |
| Operators' benefits: Facilitates and secures deployment | 10 |
| End-users' benefits: Easy access to Wifi & services | 10 |
| GLOSSARY | 10 |

> IMS network

IMS is a network for telecommunications carriers using the IP protocol for voice, video and data. Core elements of this network are the signaling protocols: Session Initiation Protocol (SIP) and Session Description Protocol (SDP).

The architecture of this network is designed to ease the addition and removal of new application servers, when previous network architecture induced a close interaction between the applications and the access technology (ie: GSM or PSTN Voice).



> Authentication in IMS

We will begin by discussing the first service the card can bring to IMS network:

- A strong and secure authentication mechanism.

We shall note at this stage, that the ISIM - *the collection of IMS security data and functions on a UICC that delivers this authentication function* - can be used in all networks using the SIP protocol even when the IMS infrastructure is not fully deployed (SIP being a major part of the IMS but not the only used protocol).

The SIP user will have many devices that can be connected to the network at the same time. These devices can connect the IMS through many access channels (WiFi, DSL, LAN, 3G ...).

For this reason the way the end user will be identified and authenticated is important as fraud will be difficult to detect from the network. The use of simple username and a password that is easy to steal does not ensure the safety of the relationship between the operator and his customer.

This makes the case for strong authentication and a way to distribute the security keys and identifier. In GSM and UMTS, the same need is already answered by the UICC.

If the smart card is used to respond to these security concerns, it can also be used to manage and store all end user information

such as Contact book, Call processing rules, setup by the end user and linked to his contacts, and presence information.

The UICC can assure the way to connect access networks (3G, 3.5G, WIFI or WIMAX), and be used to register to the service network (IMS) using SIP protocols.

> SIP registration

A User registration to an IMS network shall be authenticated. 3GPP already made the choice to leverage on ISIM to perform this strong mutual authentication. The ISIM provides the AKA mechanism that is used to authenticate the subscriber and generate key materials to establish the IP-SEC tunnel between the user equipment and the SIP Proxy.

The ISIM application also serves as the user IMS data repository that is used when connecting to the IMS network. These data are both user identifiers and network configuration data (i.e.: home domain).

The authentication protocol using SIP protocol is a HTTP digest AKA (described in the RFC 3310).

Exchanges between different network proxy or server are sequences as follows.

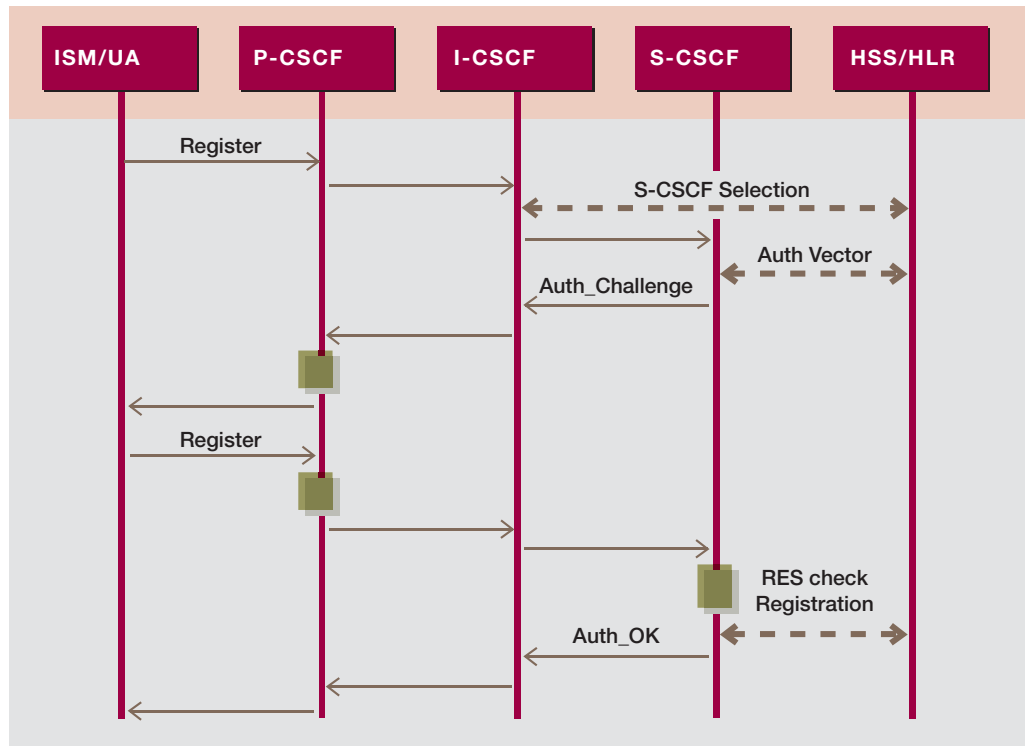


Fig1: SIP registration

Description of each message

- The SIP User Agent, send a Register SIP message to the network (through the P-CSCF (Proxy-Call Session Call Session Control Function)).
- The request is forwarded to the I-CSCF (Interrogating-CSCF) which connect the HSS (Home subscriber server) to get the S-CSCF (Serving-CSCF) providing the capabilities in line with the type of services subscribed by the end user.
- The register message initiated by the User Agent is then sent to the S-CSCF that connects the HSS to get an authentication vector.
- This S-CSCF builds a WWW-authenticate header that is sent back to the P-CSCF.
- The SIM computes the AKA for the device user agent, that send back its register to the network with the HTTP-digest response.
- The S-CSCF is in charge to verify the computed response and to accept the User Agent register.

The authentication vector provided by the S-CSCF described here after is embedded into the authentication header as follows.

```
WWW-Authenticate: Digest realm="registrar.home1.net", nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5
```

> The ISIM in the wired environment

TISPAN (Telecoms & Internet converged Services & Protocols for Advanced Networks), a working group ETSI, addresses standards for wired network and defined a lot of different authentication method including the simple username password (Digest authentication) declare recently that due to the fact that ETSI SCP chose the USB interface make now possible to use the ISIM for any device. Optionally, HTTP-digest restricted to fixed access to IMS from legacy terminals and NASS-IMS bundled are possible.

For network authentication servers, using the ISIM application on any device will be easier to manage. This make possible to authenticate a user from any device (wired or wireless) with the same level of strong security.

Each device will have its own UICC representing the end user in the network.

The UICC can also provide lot of useful services such as storage and synchronization of the contact book, QoS information linked to the user subscription level or Call processing rules.

> ISIM Architecture

The ISIM is an UICC Application providing authentication computation for SIP authentication. It contains files dedicated to SIP and algorithm for user authentication on the network...

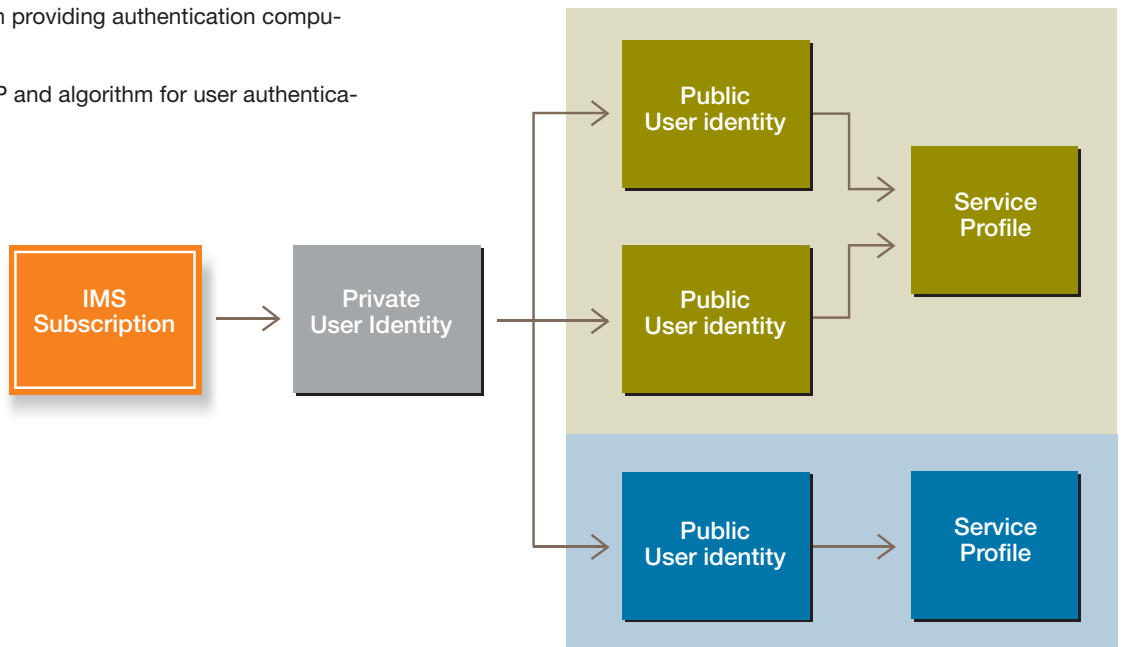


Fig3: Gemalto offer

> Files

Requirements on the ISIM application

The ISIM includes:

- The IMPPI; (IMS private identifier)
- At least one IMPU; (IMS public Identifier)
- Home Network Domain Name;
- Support for sequence number checking in the context of the IMS Domain;
- The same framework for algorithms as specified for the USIM applies for the ISIM;
- An authentication Key.

The ISIM shall deliver the CK to the UE although it is not required that SIP signaling is confidentiality protected.

At UE power off the existing SAs in the MT shall be deleted.

The session keys and related information in the SA shall never be stored on the ISIM.

> ISIM options

For the purposes of this document the ISIM is a term that indicates the collection of IMS security data and functions on a UICC. The following implementation options are permitted:

- 1 - Use of a distinct ISIM application on a UICC which does not share security functions with the USIM;
- 2 - Use of a distinct ISIM application on a UICC which does share security functions with the USIM;
- 3 - Use of a USIM application on a UICC.

There shall only be one ISIM for each IMPPI.

The IMS subscriber shall not be able to modify or enter the IMPPI. The IMS subscriber shall not be able to modify or enter the Home Domain Name.

Guide to select the option adapted to your needs

| | SERVICE PROVIDER | NON 3GPP TERMINALS (PC/PDAs) | SECURITY | |
|---|--|--|----------|---|
| USIM based IMS authentication | <input checked="" type="radio"/> Telco Only | <input checked="" type="radio"/> No | | IMS using 3GPP terminals only and not allowing the introduction of IMS service providers having their own security |
| SIM based IMS authentication | <input checked="" type="radio"/> NA | <input checked="" type="radio"/> NA | | Not allowed by 3GPP |
| ISIM based IMS authentication | <input type="radio"/> Third parties allowed | <input type="radio"/> Allowed | | With separate SQN, Key and algo |
| Stand-alone ISIM | <input type="radio"/> Third parties allowed | <input type="radio"/> Allowed | | Not allowed by the standards, although it is feasible. The user does not need to move his/her card around but has several subscriptions |
| Other (This could be more than one, e.g. EAP-SIM) | <input checked="" type="radio"/> Telco Only | <input checked="" type="radio"/> No | | Not allowed by 3GPP (SIM based and Secret exposure) |

> GBA Usage

Goal of GBA

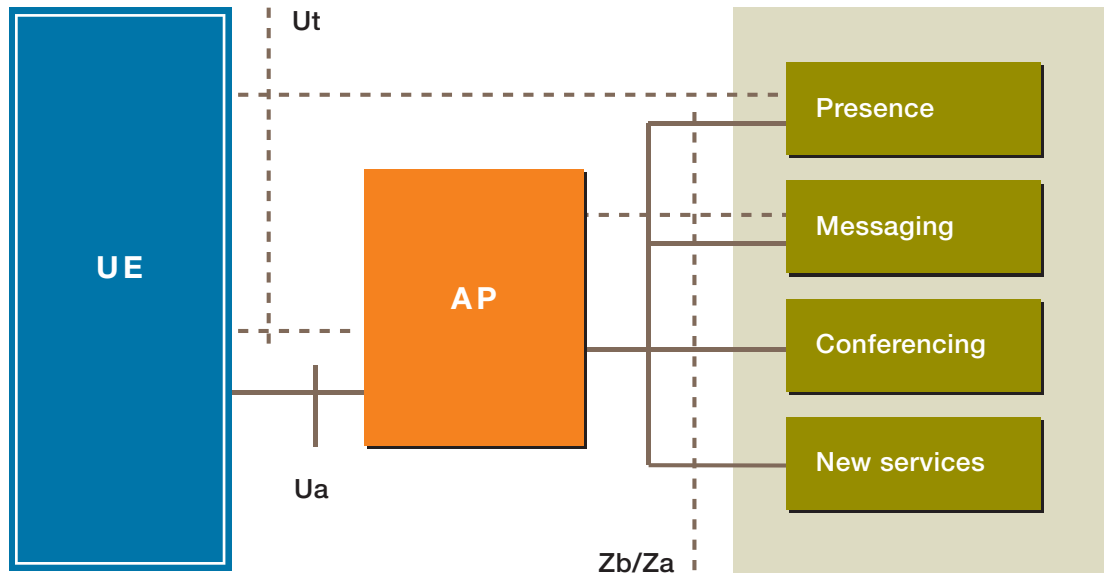
The Generic Bootstrap architecture is used to authenticate to applications provided in the IMS network. This can be achieved between an end user device and the Application Server (NAF : Network application function) or between the end user and an application proxy that will process the TLS layer for all applications that can be accessed.

GBA provides mutual authentication capability based on shared secret that is derived using existing 3GPP authentication mechanisms (i.e. AKA). The UE (User Equipment) and the NAF (Network Application Function) share NAF-specific keys (GBA credentials). GBA supports two options for application-specific key derivation

- GBA_ME: does not require any changes to the UICC applications.
- GBA_U : Requires specific files and commands in the USIM or ISIM application, but provides enhanced security by storing certain GBA keys on the UICC.

GBA credentials can be used as Single Sign-On

GBA allows direct access to an Application Server (AS) and access to an Application Server through an Authentication Proxy (AP) using HTTP over TLS



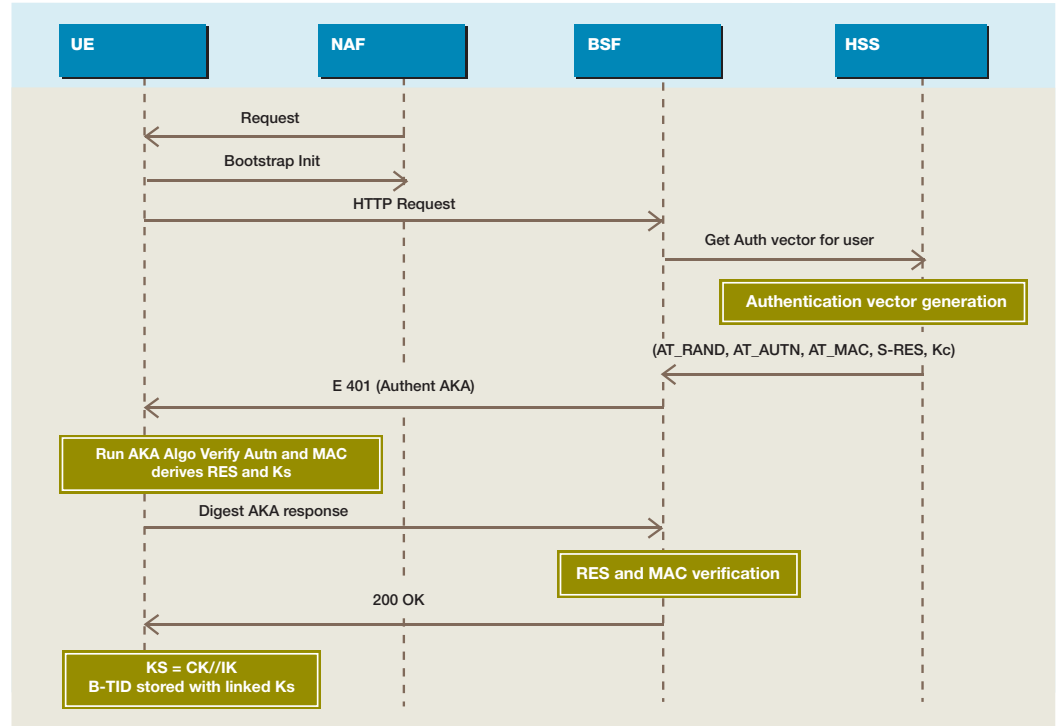
UE is authenticated by means of:

- HTTP Digest with GBA credentials
- Pre-shared key TLS (PSK-TLS with GBA credentials)
- Certificate-based TLS

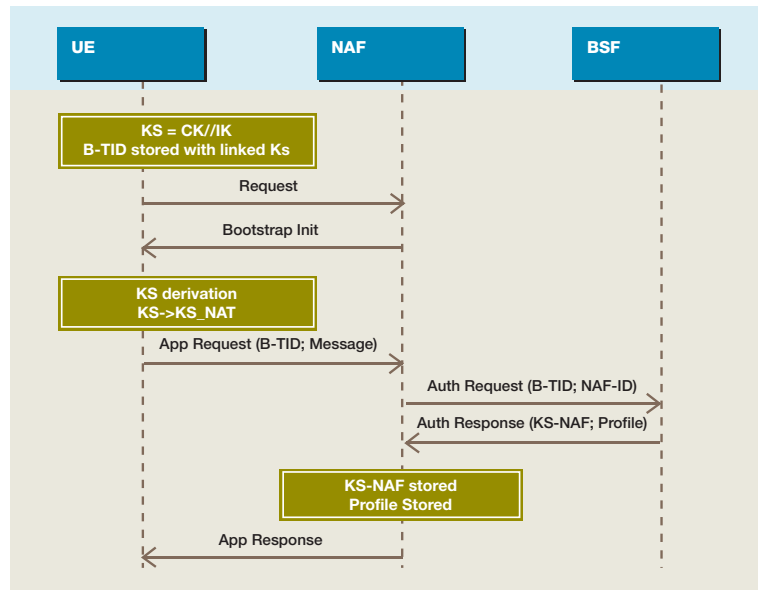
Elements that are part of the GBA are the User Equipment (UE), the Network Application function (NAF), the Bootstrapping Server Function (BSF) and the HSS (Home Subscriber Server).

Bootstrapping is processed in two steps:

The bootstrapping Authentication



The bootstrapping Application



An UICC application itself can also rely on the GBA to connect securely a NAF.

A UICC application can rely on the same protocol and mechanism to authenticate to a BSF and a NAF.

In this case the BIP is used to establish a connection with the NAF and BSF.

> Standards

3GPP. Technical Specification Group Services and System Aspects
Generic Authentication Architecture (GAA)
Generic Bootstrapping Architecture (GBA)
(Release 7)
3GPP TS 33.220 V7 (2005).

3GPP. Technical Specification Group Services and System Aspects
Generic Authentication Architecture (GAA)
Access to Network Application Functions using Hypertext Transfer
Protocol over Transport Layer Security (HTTPS)
(Release 7)
3GPP TS 33.222 V7 (2005).

3GPP. Technical Specification Group Services and System Aspects
Generic Authentication Architecture (GAA)
Early Implementation of HTTPS Connection between a Universal
Integrated Circuit Card (UICC) and Network Application Function
(NAF)
(Release 7)
3GPP TR 33.918 V7 (2005).

3GPP. Technical Specification Group Core Network and Terminals;
Universal Subscriber Identity Module (USIM)
Application Toolkit (USAT)
(Release 7)
3GPP TS 31.111 V7 (2005).

> SIP Call processing

Presence and Call Processing

Presence management is the way an end user will manage the visibility other connected persons will have on him.
Call processing is the way by which the user will manage incoming calls on its different connected and registered devices.
The SIP protocol allows setup presence and calling processing rules. These rules can be setup for a single caller, a group of caller or for all callers and can be enforced on the SIP proxy or the SIP device.
For example, Barbara can setup a rule that shows her not connected after 8PM and reject all calls of caller that are in her contact book if part of its professional group.
She can setup rules that makes ring all her devices when her boyfriend calls.
Or mute when her professional colleagues call and redirect them to a specific web page presenting the hotel she is staying for her holiday.

To setup these rules, the contact book is used because the test field is the caller ID.
All these Call Processing rules can be transferred to the SIP server for enforcement as a payload of the register request.

We shall consider that the user will be present on the network over different devices and different access network and will wish to set specific rules depending of its activity and availability. These rules shall be applied on all connected devices and a live synchronization will have to be processed.

These rules need to be part of the Contact database of the user that will be preferably stored in the removable Smart Card to allow secured OTI/OTA management (backup) and device agnosticism.

The Smart Card can simply assure the storage of these rules or act in a distributed application way where rules are enforced in the card.

On Card, SIP User agent

We call the SIP user agent the part of a Communicator User Agent. (With VoIP, IM, and more) handling the SIP protocol to establish communications.
The idea is to let the card manage internally all SIP operations for the hosting device. By this the authentication process of the SIP registering is transparent to the hosting device closing the door to some possible attacks and assuring the best level of security and confidentiality.
The other interest of this separated implementation is to deliver directly the rules (call processing) to the networks, or enforce them internally in the UA. A modification on these rules can be pushed to other SIP UA if needed.

> Operators' and end-users' benefits

The smart card remains the best way to provide authentication mechanism with a high level of security due to its tamper resistance. It constitutes also the way to distribute the keys used for authentications in an easy and secure way. Its memory capabilities and its removability make of this token a good place to store user personal informations that will follow the end user even when renewing his equipment.

The different form factors of the card makes possible to plug it in a lot of devices. For the mobile network operator another advantage is to leverage on its already existing USIM, ISIM infrastructure, as the HLR/AuC or HSS and OTA card management server.

Operators' benefits: Facilitates and secures deployment

- Able to launch quickly with re-use of existing infrastructure
- Able to **acquire new non-telephony customers** and partners while re-using existing infrastructure

End-users' benefits: Easy access to Wifi & services

- **Highly secure** way to access services
- **Ease of use**, no user name and password to remember
- **Simplicity**, all services on one bill and the same customer care number to call
- **Global reach**, a SIM based solution will propagate the roll-out of roaming partnerships

Glossary

2G – Second generation network – usually relates to GSM

3G – Third generation network – broadband wireless communications systems that combine high-speed voice, data and multimedia

Authentication - The process whereby a card, terminal or person proves who they are. A fundamental part of many cryptography systems.

BSF – Bootstrapping Server Function

CDMA – Code Division Multiple Access – A wireless communication standard predominantly found in Asia and Latin America

CRM – Customer Relationship Management

GBA – Generic Bootstrapping Architecture

GBA_ME – ME-based GBA

GBA_U – GBA with UICC-based enhancements

GSM – Global System for Mobile Telecommunications - A European standard for digital cellular telephones that has now been widely adopted throughout the world.

HSS – Home Subscriber Server

HTTPS – HTTP – Secure (HTTP over TLS)

IMS –IP Multimedia Subsystem

IP/PC – Internet Protocol / Personal Computer

Java – A network-oriented programming language invented by Sun Microsystems. Java was specifically designed so that programs could be safely downloaded to remote devices (e.g., Web pages).

Ks_int_NAF – Derived key in GBA_U which remains on UICC

Ks_ext_NAF – Derived key in GBA_U

MMS – Multimedia Message service

NAF – Network Application Function: NAF is hosted in a network element. GBA may be used between NAFs and UEs for authentication purposes, and for securing the communication path between the UE and the NAF.

OS – Operating System - A smart card OS ensures secure access to data as well as file management functions, much like the operating systems on a personal computer.

OTA – Over The Air - Transmission using microwave channels. This acronym is used in the world of wireless telecommunications. Roaming - An arrangement whereby a mobile handset is be recognized by networks other than that of the issuer (notably for subscribers traveling abroad).

ROI – Return on investment

SIM – Subscriber Identity Module - A smart card for GSM systems holding the subscriber's ID number, security information and memory for a personal directory of numbers thus allowing him to call from any GSM device. It can also store and run applications enabling end-user services.

SIP – Session Initiation Protocol

SDP – Session Description Protocol

Smart Card - Also called IC card, chip card or memory card (for certain types). A card formed of a plastic body with a chip (or module) embedded in a special cavity.

SMS – Short Message service, or text message, is a service that sends and receives messages of up to 160 characters to and from a mobile phone. It can also be used as a bearer for data applications.

UMTS –

USIM – Universal Subscriber Identity Module used in UMTS networks.

WAP – Wireless Application Protocol

WLAN – Wireless Local Area Network

A wide range of solutions

www.gemalto.com

© Gemalto 2007 • All rights reserved • Gemalto, the logo Gemalto, the logo Gemalto, are trademarks and service marks of Gemalto and are registered in certain countries • January 2007 • Design: Blend.fr

gemalto
security to be free