EAP-SIM White Paper

How EAP-SIM can help operators secure their services

FINANCIAL SERVICES & RETAIL

ENTERPRISE

INTERNET CONTENT PROVIDERS

PUBLIC SECTOR

TELECOMMUNICATIONS > PRODUCT

TRANSPORT

gemalto
security to be free

AGENDA

Executive Summary	3
Introduction	4
Definitions, symbols, abbreviations and coding conventions	5
What is EAP ?	6
What is EAP-SIM ?	7
Overview	7
Standards	7
How does EAP-SIM work?	7
Security	9
What about EAP-AKA?	10
The EAP-SIM client: the supplicant	11
Architecture	11
Supplicant - EAP Legacy	12
Supplicant - EAP Native	13
Supplicant on the PC Client	15
Supplicant in the Handset	17
The EAP SIM Server architecture	18
802.1x-compliant architecture	18
EAP-SIM compatible architecture for non-802.1x-compliant hotspot	18
Alternative authentication mechanisms	19
Basic Authentication	19
Digest Authentication	19
WEP/WPA keys	19
OTP - one-time password	19
Certificate	20
EAP-SIM use cases	21
EAP SIM for Wi-Fi security	21
EAP SIM for Generic Access Network security	21
Operator and end-user benefits	22

1 Executive Summary

The Telecom Ecosystem has now reached the stage where broadband internet access is as critical as voice services, from the end user's perspective. Telecom operators are now offering IP network coverage at home and in urban areas, giving customers unlimited service access (voice and data) on any device and via any connection - wireless, DSL, Wi-Fi . . .

Gemalto has a key role to play in this convergence of services based on multiple channels and multiple devices.

In the context of new devices and mobile broadband evolution (3G, Wi-Fi, LTE..), and based on UICC key assets, Gemalto has adapted its form factors (smart devices) to fit all new connected devices (PC and MIDs).

The Gemalto value proposition in all these key areas is:

- Device personalization - deploying and configuring the operator environment on any device.
- Security – both local, on the PC to protect the SIM identifier and credentials, and remote, to protect network access.
- Integration - providing middleware and aggregating the different network and application solutions
- Administration – using the one-to-one marketing server to deploy, update and manage all devices and their contents.

These elements are supported by a range of smart devices:

- Smart Dongle for PC devices connected to a LAN network - a USB Key offering CD-Rom and private and public partitions, with embedded SIM-USIM.
- A 3G USB Key for PC devices without connectivity – a modem key with R/O and R/W partitions.
- A SIM in 3G Laptop for devices embedding a modem – a Multimedia card offering CD-Rom and private and public partitions embedded in a Mobile Broadband PC.
- A SIM in a Handset – for recent handset models offering broadband connection and application hosting.


Smart Dongle


3G USB key


SIM in
3G Laptops


Handset

Gemalto provides a complete client/server infrastructure to manage the convergence offering throughout its life cycle, and support customer interactivity. As the undisputed leader in security, Gemalto helps operators to deploy integrated solutions to retain their subscribers' trust while extending their network and surface contact. Whatever the device used, the subscriber will benefit from mutual authentication, and thus secured transactions.

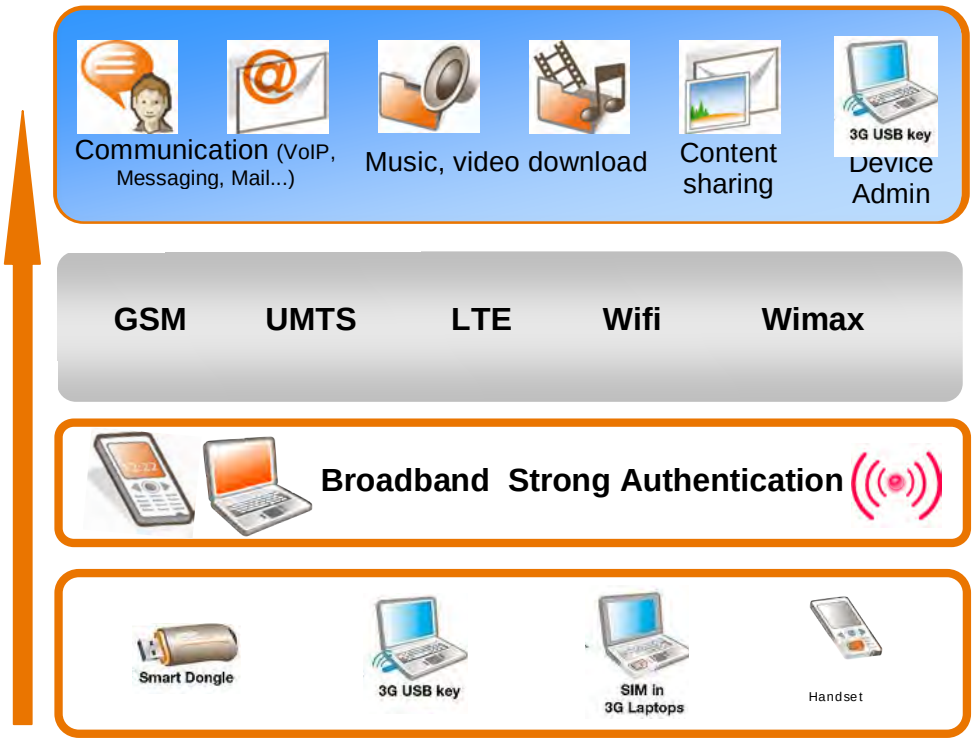
Within this global value proposition, this document focuses in particular on the security provided by the SIM and, specifically, EAP-SIM solutions. It explores the advantages of using a SIM or USIM with the EAP protocol to authenticate a user connecting to the network through a Wi-Fi hotspot or for generic network access, including the benefits of:

- dramatically improved security
- a simple (and consistent) user experience, including familiar billing procedures
- consistent deployment across a range of devices
- simple lifecycle management

It also demonstrates how the EAP solution provides the highest security levels in WLAN connections, while utilizing the existing operator infrastructure.

2 Introduction

This paper focuses on (U)SIM-based authentication to Wi-Fi and WLAN networks. Based on EAP-SIM and EAP-AKA, the Gemalto WLAN authentication solution is available on the smart devices described above.



The use of a security scheme like this guarantees end-to-end security for the user and for the operator. As in most security scheme, the deployment of this solution spans multiple entities - networks, servers, terminals and smartcards - and all these elements are considered here.

3 Definitions, symbols, abbreviations and coding conventions

Acronym	Definition	Comments
AP	Access Point	Typically a Wi-Fi hotspot
IP	Internet Protocol	
EAP	Extended Authentication Protocol	
SIM	Subscriber Identification Module	Smart card inserted in a handset or modem used for 2G and 3G network authentication.
WEP	Wired Equivalent Privacy	A deprecated algorithm to secure IEEE 802.11 wireless networks. It precedes WPA.
WPA	Wi-Fi Protected Access	WPA and WPA2 is a certification program created by the Wi-Fi Alliance to indicate compliance with the security protocol. This protocol was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP).
MNO	Mobile Network Operator	
IKE	Internet Key Exchange	
TKIP	Temporal Key Integrity Protocol	TKIP was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as a solution to replace WEP without requiring the replacement of legacy hardware. This was necessary because the breaking of WEP had left Wi-Fi networks without viable link-layer security, and a solution was required for hardware already deployed. On October 31, 2002, the Wi-Fi Alliance endorsed TKIP under the name Wi-Fi Protected Access (WPA).[1] The IEEE endorsed the final version of TKIP, along with more robust solutions such as 802.1X and the AES based CCMP, when they published IEEE 802.11i-2004 on 23 July 2004.[2] The Wi-Fi Alliance soon afterwards adopted the full specification under the marketing name WPA2.[3] TKIP has reached the end of its designed lifetime and has been deprecated in the next full release of the 802.11 standard.[4]

4 What is EAP ?

EAP, the Extensible Authentication Protocol, is a universal authentication framework frequently used in wireless networks and Point-to-Point connections.

EAP is a generic framework for network authentication, with application beyond Wi-Fi authentication, and is not a 'SIM only' solution. EAP-SIM is one of several EAP implementations designed to reuse MNO credentials, and to fully understand it, it is helpful to know something of EAP in general.

EAP is defined in RFC 3748 by IETF (Internet Engineering Task Force), updated in RFC 5247.

EAP is an authentication framework, not a specific authentication mechanism. The protocol provides some common functions and negotiation of the desired authentication mechanism. Such mechanisms are called EAP methods and there are currently about 40 of them. Methods defined in IETF RFCs include EAP-TLS, EAP-MD5, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, and EAP-AKA, EAP-OTP, and so on, plus a number of vendor-specific methods and new proposals.

Although the EAP protocol is not limited to wireless LANs and can be used for wired LAN authentication, it is most commonly used and deployed in wireless LANs.

The Wi-Fi alliance proposes a certification program for Wi-Fi materials and software, under the WPA (Wi-Fi Protected Access) label. It defines several levels of certification:

- WPA
- WPA 2
- WPA 2 Enterprise

EAP types currently included in the Wi-Fi alliance certification program are:

- EAP-TLS (previously tested): Based on client and server certificates deployed through a Public Key Infrastructure. Client certificate can be stored on a smartcard.
- EAP-TTLS/MSCHAPv2: Based on server side certificate only. Well supported by Cisco and Microsoft.
- PEAPv1/EAP-GTC: Not supported by Windows OS, so not really deployed.
- PEAPv0/EAP-MSCHAPv2: Method mainly supported by Microsoft.
- EAP-SIM: Based on SIM card: uses cryptographic algorithm for 2G network authentication
- EAP-FAST (since 19/05/2009): Flexible Authentication via Secure Tunneling is a protocol proposal by Cisco Systems
- EAP-AKA (since 19/05/2009) : Based on SIM card: uses cryptographic algorithm for 3G network authentication

Certification began in September, 2004. From March 13, 2006, WPA2 certification is mandatory for all new devices bearing the Wi-Fi trademark. (Concerning the Wireless Access Point, the device shall follow the 802.1x norm to obtain WPA-2 certification and thus allow EAP negotiation.)

When EAP is invoked by an 802.1X-enabled NAS (Network Access Server - a device such as an 802.11 a/b/g Wireless Access Point), EAP methods can provide a secure authentication mechanism and negotiate a secure PMK (Pair-wise Master Key) between the client and NAS. The PMK can then be used for the wireless encryption session which uses TKIP (Temporal Key Integrity Protocol) or CCMP (based on AES) encryption.

The EAP-SIM solution is an end-to-end solution that implies some mandatory elements:

- a software client to manage the connection
- Wi-Fi device material: hotspot and device client
- a Radius server supporting EAP to manage authentication
- a gateway to the HLR (Home Location Register) of the operator, containing the subscriber list and its credentials.

Each of these elements is discussed in further chapters.

5 What is EAP-SIM ?

5.1 Overview

EAP-SIM is a standard for authentication to Wireless LAN access. It implies SIM cards and the GSM mobile phone authentication network. It uses the subscriber identity and the credentials of the SIM card to authenticate the user and create a session key which can be used to secure Wi-Fi access or to establish a VPN (Virtual Private Network), for example.

5.2 Standards

The global definition of EAP is specified in RFC 3748. (www.ietf.org).

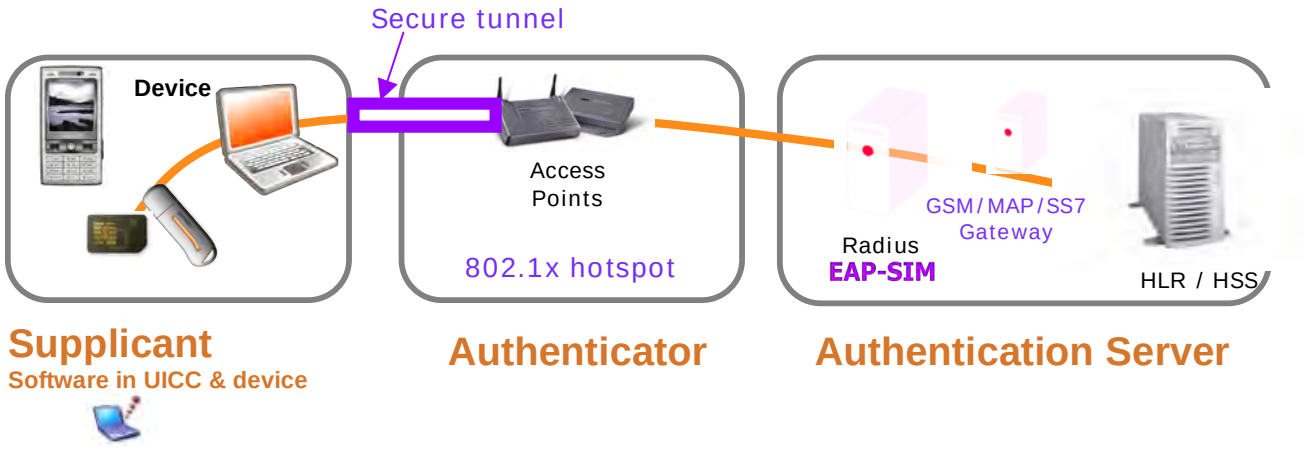
The standard for EAP-SIM authentication is described in RFC 4186 from IETF

EAP-AKA is similar to EAP-SIM and used for 3G network authentication rather than 2G.
EAP-AKA is specified in RFC 4187.

The implementation in the SIM is specified by the ETSI in TS 102.310.

5.3 How does EAP-SIM work?

Typically a network operator's wireless Hot Spot accepts a Wi-Fi connection from a client (PC or handset). This Wireless LAN (WLAN) Access Point (AP) provides access to the MNO's Radius server. The Radius server supports EAP-SIM authentication and is equipped with a GSM/MAP/SS7 gateway linked to the HLR (Home Location Register) of the operator. The HLR contains the identity of the subscriber and the cryptographic secrets to authenticate the subscriber.



A user who wants to connect to the wireless LAN typically needs:

- a PC, a smart phone or a Personal Digital Assistant (PDA) with SIM access and 802.1X wireless LAN –enabled
- EAP-SIM Wireless LAN client software.

The SIM card is provided by the operator, and the Access Point is operated by the same operator (or another operator, in the case of roaming agreements). The SIM card uniquely identifies the user to the 3G or GSM system, and holds the user's IMSI (International Mobile Subscriber Identity).

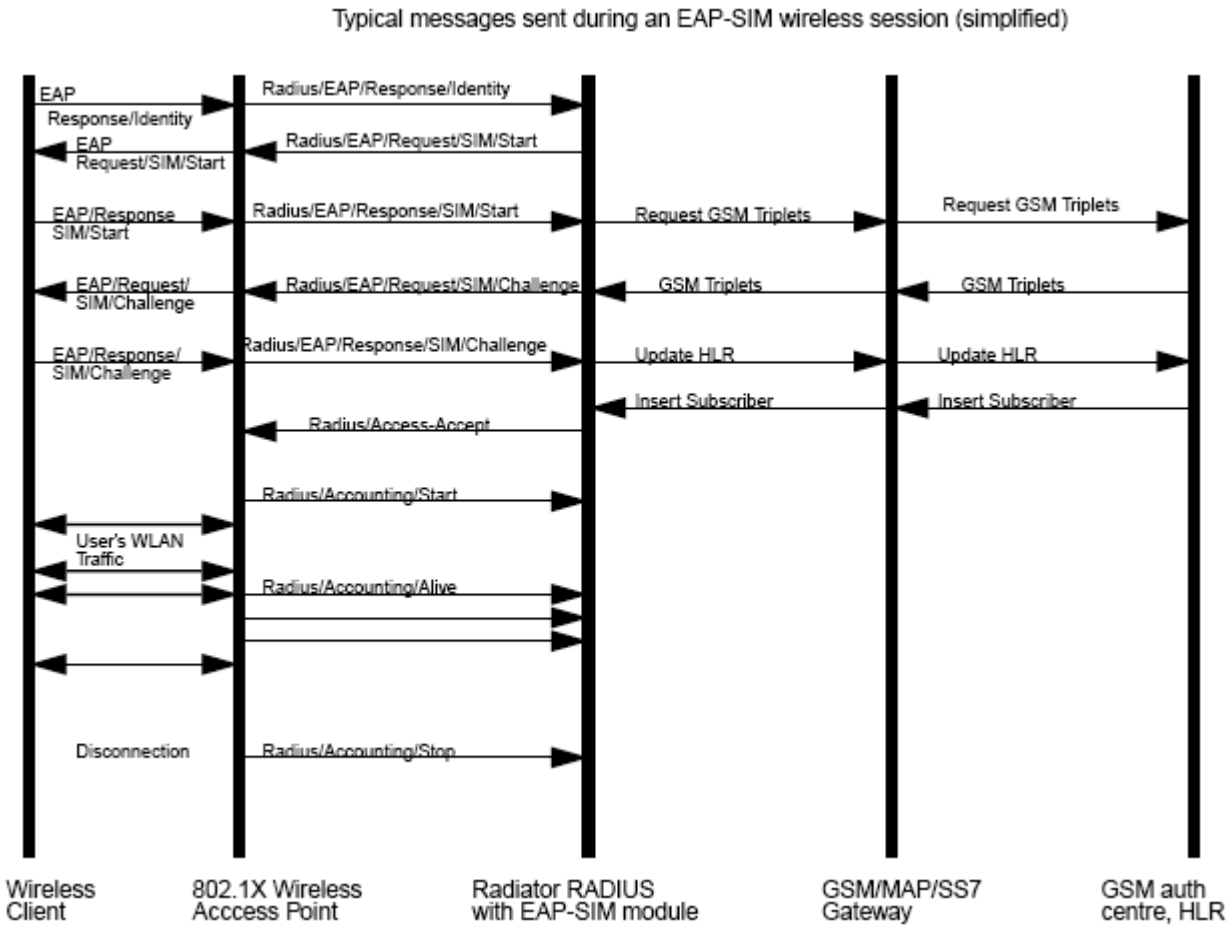
When the user, with computer, roams within range of the WLAN Access Point, the Access Point, Radius server and Wireless client software set up a communications dialog in order to authenticate the user and confirm he or she is allowed to access the network.

During this process, the Radius server contacts the user's home MNO through a GSM/MAP/SS7 gateway and retrieves the GSM triplets that are used to authenticate the user.

If the user's Wireless client software and SIM card is able to validate the GSM triplets correctly, the Radius server tells the AP to grant access to the WLAN. The AP connects the client computer to the WLAN, and sends some accounting information to the Radius server, indicating that the user's wireless connection is complete. The Radius server can eventually trigger billing information.

The user uses the wireless connection to send and receive internet traffic for a period of time. During this time, the AP will typically send accounting 'Alive' messages to the Radius server, indicating that the wireless session is still connected. During the session, fast re-authentication can be triggered, to renew cryptographic material.

After a while the user may roam out of range of the AP, or turn off the client computer. The AP sends then an accounting 'Stop' message to the Radius server, indicating that the user's session is complete.



The overall result of this process is that only people with a valid SIM card inserted in their terminal are able to gain access to the Wireless LAN.

It reuses the 3G MNO infrastructure and MNO subscriber database, which means:

- No redundant provisioning: subscriber is already declared.
- Credential and user information follow the same scheme as for a traditional subscriber
- Billing infrastructure can be reused, and billing is unique

This simplifies the user's experience when using and paying for Wireless LAN access.

5.4 Security

«
DAILY FINANCE
Hacker who aided Feds charged in theft of 130 million credit card numbers
Aug 18th 2009

Albert Gonzalez, a 28-year-old computer hacker, was indicted yesterday for stealing 130 million credit card numbers, topping his previous record of allegedly stealing 40 million credit card numbers in a series of Wi-Fi based intrusions of U.S. retailers, including TJ Maxx, Office Max and DSW.
”

In this major fraud, the hacker has taken advantage of a Wi-Fi security weakness, illustrating the importance of updating the security rules regularly.

The first Wi-Fi security mechanism, the so-called WEP, was based on a pre-shared key. WEP authentication is no longer adequate - the key can be retrieved in a few minutes. WPA coupled with EAP-SIM enables a dramatic reinforcement in the security level.

The EAP-SIM authentication standard has been developed with high standards of wireless security in mind. With EAP-SIM, passwords are never transmitted over the air or in Radius requests over the internet. EAP-SIM authentication involves secret keys and algorithms that are embedded in the SIM card and at the GSM authentication centre. These secret keys are never accessed by servers and, again, never transmitted over the air or in Radius requests.

The EAP-SIM standard also provides support for pseudonym Temporary Mobile Subscriber Identities (TMSI). TMSIs can be generated for each authenticating client after an initial authentication, allowing the user’s real IMSI to be hidden from wireless packet sniffers.

It also supports Re-authentication (also called fast-reauthent). This permits re-authentication of an EAP-SIM wireless client without requesting new GSM Triplets from the GSM Authentication Centre (AuC), which can result in improved reconnection performance when EAP-SIM clients roam from cell to cell.

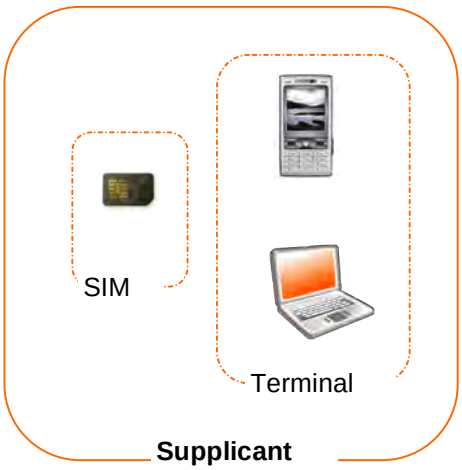
6 What about EAP-AKA?

EAP-AKA is based on the same principle as EAP-SIM. It uses the 3G authentication algorithm (Authentication and Key Agreement, usually called "milenage") instead of the 2G (A3/A8).
Note that in this case mutual authentication and replay protection are "natively" supported by this authentication algorithm.

7 The EAP-SIM client: the supplicant

7.1 Architecture

The software client is called a supplicant, and is split between:
- The terminal (such as a handset or a PC)
- The SIM

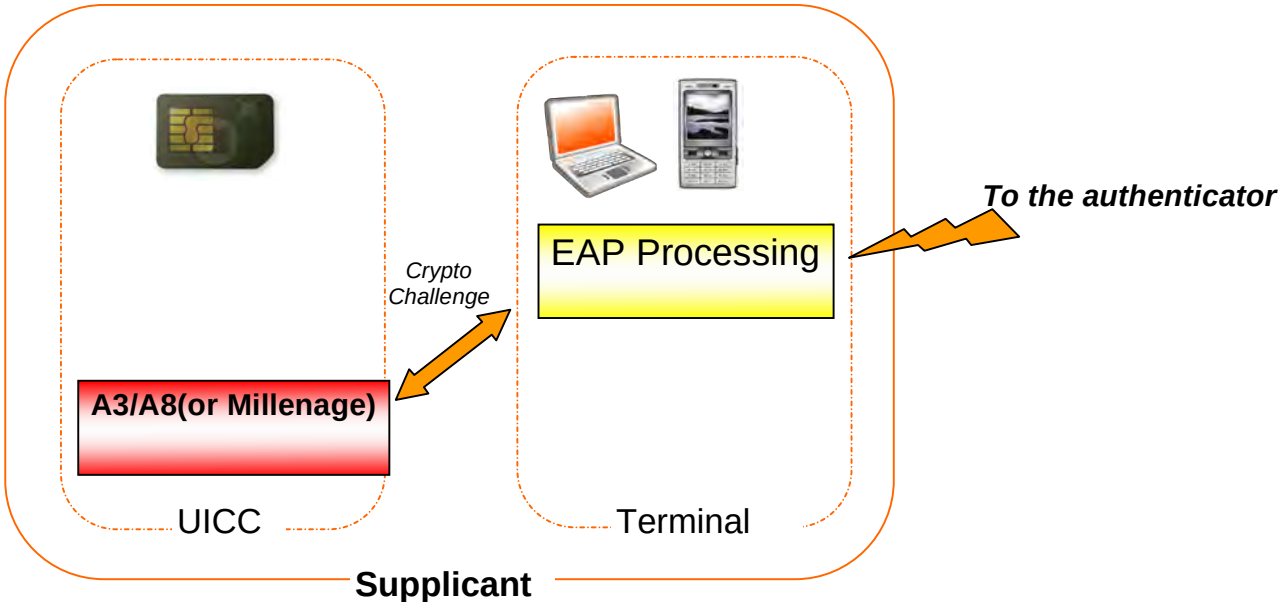


The supplicant performs two main tasks:
- EAP request and response processing: : it analyses EAP Requests, initializes a machine state to guarantee consistent data flow, and builds responses following a standard encoding.
- Cryptographic computing: calculation of A3/A8 (or milenage) challenge.

Implementations can use two possible architectures:
- Supplicant - EAP Legacy: the EAP requests and responses are processed by the terminal and the cryptographic computing is performed by the UICC. This implementation is more terminal-oriented.
- Supplicant - EAP Native: these two main tasks are performed by the SIM, and the terminal is only used to forward EAP requests to the UICC and EAP responses to the authenticator. This implementation is more SIM-oriented.

7.1.1 Supplicant - EAP Legacy

A terminal-oriented implementation.



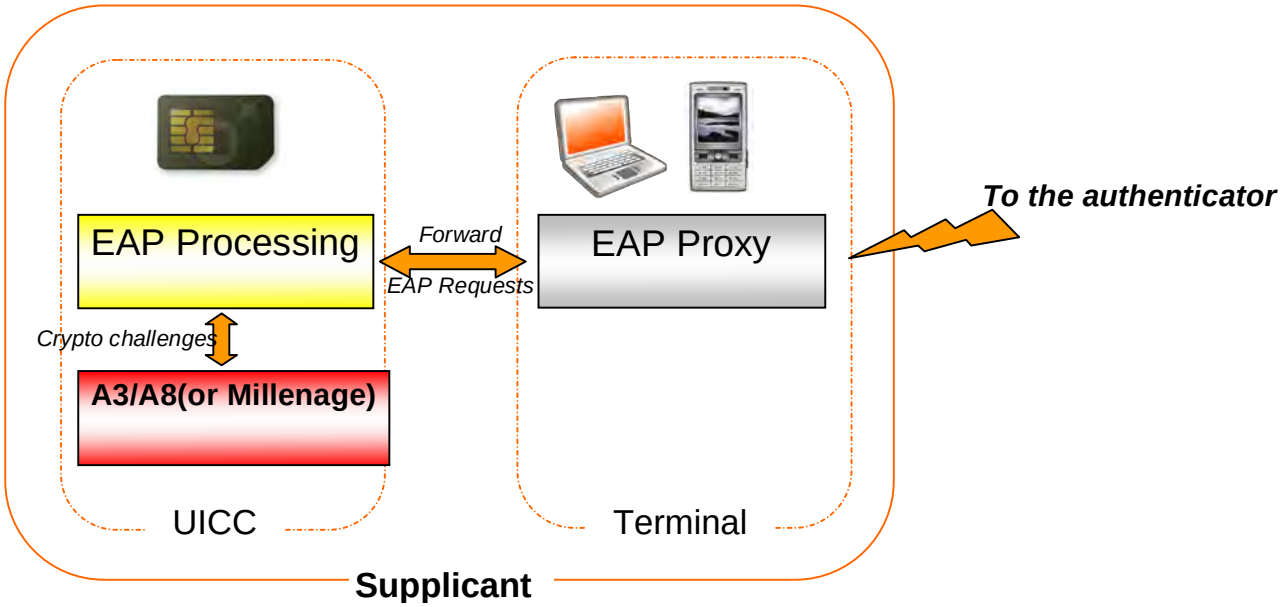
EAP Processing: this component is in charge of analyzing the EAP request, to maintain a state machine and to build the response. The device supplicant normally sends the standard 2G authentication command (Run GSM Algorithm) to the card and handles the calculation/verification.

A3/A8 (or Milenage): this component handles the cryptographic processing, using exactly the same calculation as used for GSM or 3G networks.

Pro	Cons
Availaility for deployment Any UICC can be used	Consistant deployment Each EAP-SIM Processing implementation has to be tested and validated for each terminal.
	Security Intermediate computations can be reused to hack the network. A brute force attack could break the key
	Update and life cycle management Each supplicant implementation has its own way of storing parameters. Update and life cycle management is possible but it is terminal dependant.

7.1.2 Supplicant - EAP Native

A SIM-oriented implementation.



EAP Proxy: this is a simple component that forwards EAP requests and returns EAP responses.

EAP Processing: this component is in charge of analyzing EAP requests, to maintain a state machine and to build the response.

A3/A8 (or Millenage): this component handles cryptographic processing, using exactly the same calculation used for GSM (SIM) or 3G (AKA) network authentication.

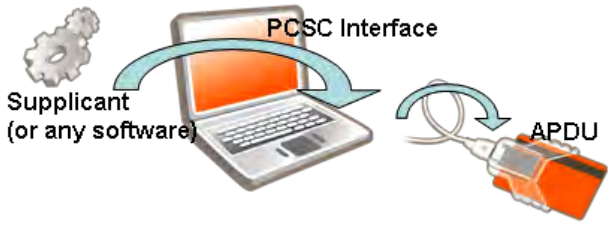
Pro	Cons
Consistant deployment The SIM offers an interoperable platform owned by the MNO. EAP implementation is terminal-independent and guarantees consistent interaction with the MNO network back end. Only EAP Proxy has to be changed, according to the terminal: no requirement to validate a full EAP use case. Update and life cycle management Life Cycle Management of Wi-Fi parameters through OTA platform to manage identity, credential and network configuration It is possible to modify, post-issuance, the settings of the SIM Card in a standard and interoperable way. Standard parameters below can be updated Over The Air or Over The Internet. - EFdir: hide/show EAP SIM - EF PUID to modify permanent identity - EFKEY (0001) to change Ki, op/opc , algo: - op or opc: computing mode for session key computing - algo : A8, Millenage, - EFrealm: domain name (optional parameter) - EFuwsidl: user controlled WLAN Specific Identifier List → Prefered SSID of the user. - EFowsidl: operator controlled WLAN Specific Identifier List → Prefered SSID of the MNO. Note: the update of such parameters is not standardized in case of software implementation	Availability for deployment Needs specific SIM with EAP-SIM/AKA inside Remains dependent on the handset, even if the EAP Proxy is easy to develop and validate.
Security Intermediate computations remain inside the UICC and reduce the risk of network key hacking.	

7.2 Supplicant on the PC Client

Both architectures can be used in a PC environment. Whatever the platform (laptop, netbook, desktop), a SIM is required to perform the authentication. This can be accessed by the PC software through an intermediate device such as a smart card reader, smart dongle or modem.

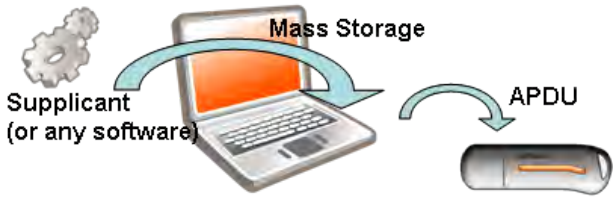
Several use cases are possible:

- Smartcard reader: The card reader is connected to the PC. The SIM card is inserted in the reader, and is then directly accessible by software on the PC. On Windows OS, it is generally accessed via the PCSC interface.



SmartCard reader

- Smart Dongle: The Smart Dongle is a Gemalto secured USB Key combining mass storage and a SIM card. Communication with the SIM is done using USB mass storage and is highly secure. Only trusted applications can access the SIM.



Smart Dongle

- 3G USB Key: this is an external USB 3G modem with a SIM inside. PC Software applications cannot communicate directly with the SIM, but the modem device offers a communications interface, generally via AT commands. In this case, the software sends an AT Command to the modem (AT+CSIM, AT+CGLA, ...). The modem processes the command, and then forwards the request to the SIM.

3G USB Key

- PC with 3G Modem inside: this is an internal USB 3G modem with an embedded SIM. PC Software applications cannot communicate directly with the SIM, but the modem device offers a communications interface, generally via AT commands. In this case, the software sends an AT command to the modem (AT+CSIM, AT+CGLA, ...). The modem processes the command, and forwards the request to the SIM.

PC with 3G Modem inside

Communication between the modem and the SIM is handled via AT Commands. AT Commands follow TS 27.007 defined by 3GPP. Commands like AT+CSIM and AT+CGLA support the exchange of data between the PC Application and the SIM.

Command AT+CSIM is optional in the standard, but is generally implemented by modem makers. Command AT+CGLA is standard, but optional. The implementation is close to AT+CSIM but it filters some commands to the card (Channel 0 is reserved for the modem). To improve security, Gemalto recommends using AT+CGLA. If AT+CGLA is not available, it is still possible to use AT+CSIM.

7.3 Supplicant in the Handset

For proprietary Operating Systems, EAP-SIM support (legacy or native) is the responsibility of the handset maker.

For open Operating Systems like Windows Mobile, Symbian, Androïd, or Linux, it is theoretically possible to develop a supplicant, provided that the operating system offers all needed accesses. In reality, only a few operating systems allow the supplicant to access the SIM: for security reasons, SIM access is generally restricted to the operating system itself. As the result, in this case, EAP SIM support has to be implemented by the handset makers themselves.

Below is a (non-exhaustive) list of handsets which support EAP SIM (legacy), and have been tested.

Manufacturer	Model	OS	Connectivity: Wi-Fi	EAP-SIM "Legacy"
APPLE	iPhone 3G A1241	Mac OSX	802.11b,802.11g	Supported
Nokia	E61-1	Symbian	802.11g	Supported
Nokia	E63	Symbian	802.11b/g	Supported
Nokia	E66	Symbian	802.11b/g	Supported
Nokia	N95	Symbian	802.11b,802.11g	Supported
Nokia	N96	Symbian	802.11b,802.11g	Supported

8 The EAP SIM Server architecture

On the back-office side, there are two possible architectures.

The first architecture is based on facilities in recent-generation Wi-Fi hotspots. These hotspots already support EAP negotiation before any other network exchanges, and are 802.1X compliant.

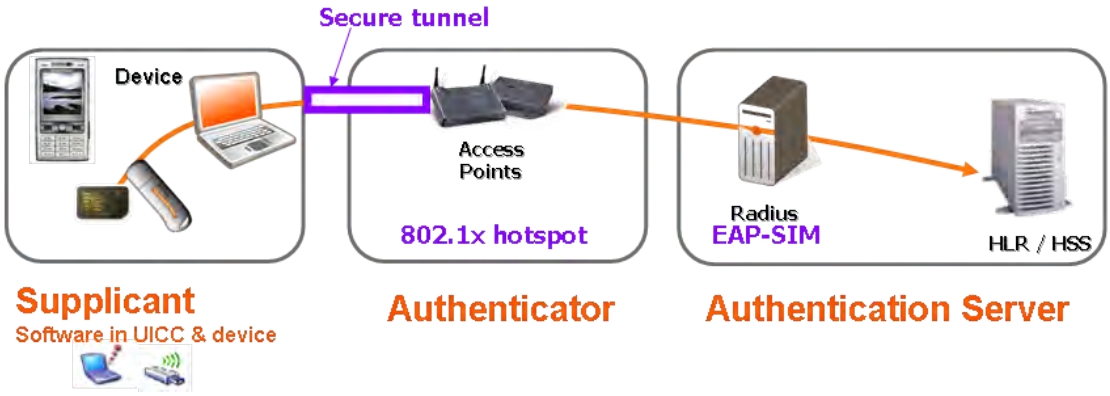
The second architecture has been designed to offer EAP-SIM authentication on older hotspots. These hotspots are called EAP-SIM-compatible hotspots.

8.1 802.1x-compliant architecture

IEEE 802.1X is an IEEE Standard for port-based Network Access Control, released in 2001.

An 802.1X hotspot supports native EAP-SIM. The authentication is carried out between the client and the authentication server as soon as the hotspot is detected; once completed, an IP address is assigned to the client.

Exchanges between the client and the hotspot are encrypted.



8.2 EAP-SIM compatible architecture for non-802.1x-compliant hotspot

Older hotspots are not 802.1x-compliant, and EAP-SIM authentication is not supported at a low level layer. They can also be used, however, with limited impact on the infrastructure. When the client detects the hotspot, the hotspot accepts the connection, and an IP address is assigned to the client by the Access Network Controller.

However, the client has only limited network access until completely authenticated. Traffic is filtered and only authentication requests are permitted. At this stage, either the user has to enter credentials (login/password) manually, or plug-in software is used to trigger EAP-SIM authentication.

The authentication request is generally handled by a servlet of the ANC and forwarded to the Radius server.

9 Alternative authentication mechanisms

EAP-SIM and EAP-AKA are not the only solutions for connection to WLAN networks. Other identification mechanisms such as basic authentication, digest authentication, OTP or certificate-based authentication are available, and some are already deployed.

At first glance, these authentication methods have some advantages - the impact on devices and network is minimal, for example. But after detailed analysis, however, it appears that these methods endanger the subscriber, as in most cases sessions can be hacked and billed to him or her.

9.1 Basic Authentication

This method is used in HTTP protocols to verify access rights to a server. The authentication header is sent by the server in an E401 response. The user then provides a username and password, which are sent as plain text.

9.2 Digest Authentication

This method is a variant of HTTP authentication, where the username and password are not sent as plain text. Instead, an MD5 hash of the combined user name, authentication realm and password is calculated and sent back to the server.

Both methods present some weaknesses, as the information flow can be hacked during the exchange between devices and server.

9.3 WEP/WPA keys

Mostly used at home for Wi-Fi authentication to DSL boxes, the WEP key method has two drawbacks:

- Key provisioning: for the first Wi-Fi connection to the box (Wi-Fi pairing) and to hotspots, the user has to enter the WEP key manually, at initialization stage at least.
- Lack of portability: after initial installation, the key is stored on the user's PC, thus restricting its usage.

This method is not convenient for the end user, as a new key needs to be entered every time he switches on a device or needs to connect to a new hotspot.

9.4 OTP - one-time password

This mechanism requires the use of a specific server with the ability to generate a new password that will change at each connection. The software client contains the same algorithm, and server and client are synchronized with a counter to avoid replay attacks.

It is possible to automate OTP presentation by adding a plug-in to the browser that will generate the OTP when required by the server. As a key is used to compute the OTP, this key need to be stored securely - in a secure token, for example - and is never transferred to the device used for connection.

Gemalto provides this type of solution for authentication and easy access to services.

9.5 Certificate

It is also possible to use certificate-based mutual authentication, but each client must have a certificate. The certificate contains information on its owner, and is cryptographically signed by the certificate issuer.

Certificate usage is based on a public key infrastructure (PKI), so is linked to a key pair, one being public and the other secret. The public key is inserted into certificates that need to be signed by a certificate authority with a private key.

The client (or server) certificate signature will be verified using the public key of the certificate authority. That means a "good" public key must be used for this operation - the certificate authority certificate containing the public key must itself be stored securely. A certificate with a private key that needs to remain secret must also be stored securely and used from a tamper-resistant device - normally a smart card.

A PKI is costly and difficult to put in place, because of the need to distribute certificates with their key pairs in a secure way to their owners.

10 EAP-SIM use cases

10.1 EAP SIM for Wi-Fi security

Such a system would typically be used with publicly accessible Wireless LAN hotspots such as those operated by airports, hotels, cafes, kiosks and so on. The hotspot operator would install the Access Points, and the EAP-SIM equipped Radius server would be operated by a telecommunication carrier or other GSM operator.

The user is automatically connected to the Wireless LAN, and will be billed for LAN usage through the mobile phone bill.

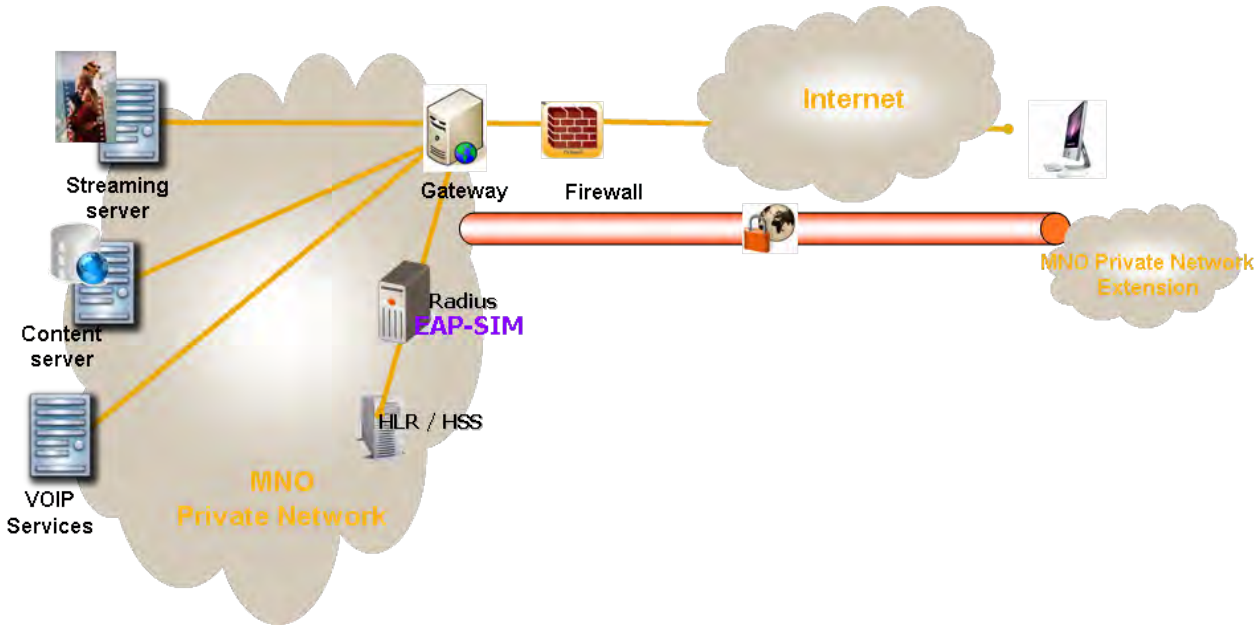
Where there are roaming agreements, users can be connected to the Wireless LAN of an other MNO, thus extending coverage for subscribers and providing operators with a share of the revenue. Roaming is facilitated by interconnecting the Radius servers of two MNOs and exchanging a subset of user information and credentials.

Swisscom and TMN Portugal have already launched an automatic Wi-Fi access service based on EAP-SIM.

10.2 EAP SIM for Generic Access Network security

MNOs can use the Generic Access Network infrastructure to extend their service offer (Voice Over IP, for example) using the internet. To guarantee the security of these services, a secure channel must be established between the client and the MNO network.

IP Sec is one of the largest deployed solutions offering this type of security. A tunnel is established and all data sent through this tunnel are encrypted. A session key is negotiated between the client and the IP Sec gateway. This session key is established using IKE v2 (Internet Key Exchange) protocol, using EAP-SIM for client authentication. (Note that other EAP methods, such as TLS or Pre-Shared Key, can also be used.)



11 Operator and end-user benefits

The SIM-based approach described in this paper offers significant benefits for operators and end users, which can be summarized as follows:

- Reuses 3G MNO infrastructure to authenticate the user
  - No redundant provisioning
  - Credentials and user information follow the same scheme as a traditional subscriber
  - Billing is unique

- Offers lifecycle management of Wi-Fi parameters through OTA platform to manage identity, credential and network configuration
  - SIM card settings can be modified in a standard and interoperable way

- Provides state of the art security

- Enables consistent deployment of EAP on all connected devices, the UICC offering an interoperable platform
  - Allows deployment additionally in 3G laptops and MIDs

- Capable of securing other networks such as IMS and UMTS by offering an IP Sec IKE v2 secure channel based on EAP.