



# Securely access to WLAN

Feeling at home. Everywhere.

February 2007

BANKING & RETAIL

ENTREPRISE

INTERNET CONTENT PROVIDER

PUBLIC SECTOR & TRANSPORT

TELECOMMUNICATIONS > WHITE PAPER

# Executive summary

The telecom ecosystem is evolving - and the pace of change is increasing.

## TABLE OF CONTENTS

EXECUTIVE SUMMARY .....	2
GLOBAL GEMALTO CONVERGENCE OFFER .....	3
WHAT IS EAP	
SIM usage in WIFI .....	4
SIM based WLAN authentication key advantages .....	4
TECHNOLOGY OVERVIEW OF EAP-SIM / AKA .....	4
DETAILED ARCHITECTURE OF EAP-SIM / AKA .....	6
ALTERNATIVE AUTHENTICATION MECHANISMS .....	7
EAP-SIM AND EAP-AKA IMPLEMENTATION .....	8
OPERATORS' AND END-USERS' BENEFITS	
Operators' benefits: Facilitates and secures deployment .....	9
End-users' benefits: Easy access to Wifi & services .....	9
REFERENCES .....	9

Telecom operators are adapting their offers to meet customer demands - they're offering IP network coverage at home and in urban area, for example, and giving customers unlimited service access (voice and data) on any device and via any connection - wireless, DSL, WiFi and so on.

This convergence of services, based on multiple channels and multiple devices, can be optimized with Gemalto know-how. We have built a dedicated offer, spanning different form factors such as the smart USB Dongle and SIM/USIM, to give operators a real advantage in all these key areas:

- **strong authentication** - maintaining the link with subscriber (and ensuring billing!)
- **device personalisation** - deploying and configuring the operator environment on any device
- **security** - protecting the link between customer and operator and guarding against phishing and spoofing, for example
- **connectivity** - enabling any communication application and generating new revenues

Gemalto also provides a complete server infrastructure to manage the convergence offering throughout its life cycle, and support customer interactivity.

As the undisputed leader in security, Gemalto will help 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.

This document explores the advantages of using a SIM or USIM with the EAP protocol to authenticate a user connecting to the network through a WiFi hotspot. It also demonstrates how the EAP solution reuses the existing operator infrastructure to provide the highest security levels in WLAN connections.

# Global Gemalto Convergence offer

With emergence of new services and devices based on IP deployment, subscribers are now using different types of devices and requiring appropriate connectivity for each of them. To address this convergent ecosystem, Gemalto defines several offers to match operator characteristics - pure mobile operator, mobile and ISP, and so on - and segmentation.

• **PC Link application:** By connecting a mobile phone to a PC with a local link (USB cable or WiFi for example) the subscriber automatically gains the benefits of an advanced personal data management solution, with local synchronization and on-line storage, and simple access to internet operator services with SIM -based authentication

• **Smart Dongle:** By inserting Smart Dongle in a USB port on the PC, the subscriber gains access to operator IP services including voice and IM, and gains the benefits of the operator's proposals for attractive services using multimedia content and video, for example

• **Embedded smart card in PC:** The operator can easily build packaged offers for the corporate sector, including a PC with a complete and off-the-shelf connection manager.

• **Multi mode handset:** By using the SIM-based solution for managing GSM/3G service access and WiFi/Wimax service access, the operator can come to the subscriber with a uniform trusted environment and combined offer.

This document focuses on (U)SIM-based authentication to WiFi and WLAN networks. Based on EAP-SIM & EAP-AKA, the Gemalto WLAN authentication solution is available on the four offers described above.

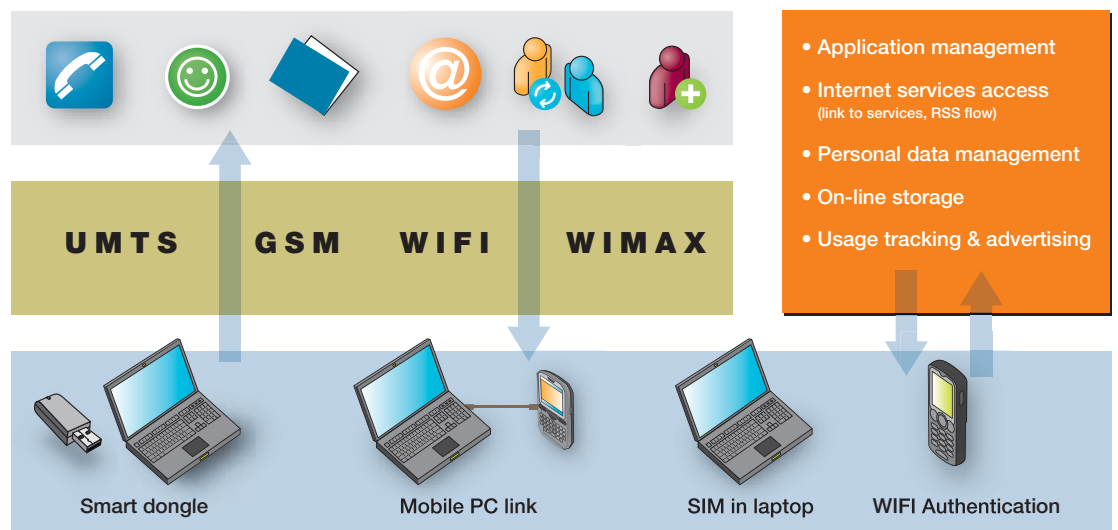


Fig1: Gemalto offer

## > What is EAP

### The SIM in WIFI

EAP-SIM specifies an Extensible Authentication Protocol (EAP) Type, for authentication and session key material generation using the SIM. EAP-AKA is the same protocol, but based on the USIM and the 3G Milenage algorithm.

Wifi can be used in multiple situations:

- At home, to connect to the network through a DSL box using a PC or a bi-mode handset.
- When travelling, in an airport for example, to connect to the network via a hotspot.
- A third case - which may not involve the SIM - is when WiFi is used in a corporate environment

## > Technology overview of EAP-SIM / AKA

EAP-SIM or AKA addresses networks with WiFi access hotspots. The application can be hosted on a high-end UICC.

EAP-SIM is required to authenticate the end-user on WiFi. The EAP architecture defines three main components:

1) The supplicant: is the end user hardware/software that requires access to the network. The supplicant is divided into two parts, the SIM and the handset.

### SIM based WLAN authentication - the key advantages

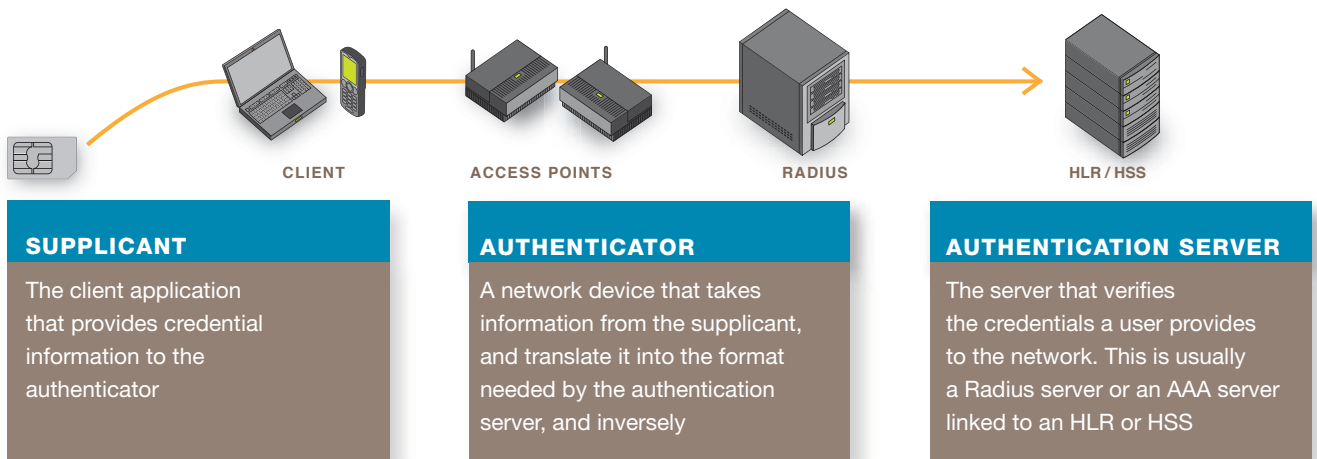
Gemalto is the world leader in digital security, providing end-to-end solutions to 350 customers. Our acknowledged expertise in security and personalization is the core of our offer on EAP-SIM or EAP-AKA authentication to WiFi hotspots.

On top of the key assets of the SIM card - customer identification, life cycle management, personalization, roaming - an EAP-SIM or EAP-AKA application offers two main advantages for operators:

- the existing infrastructure can be re-used
- operators can give users the same levels of security they already provide on their GSM and 3G networks

2) The radius or AAA server is the server that allows or denies the end user access to the network

3) The authenticator (or access point, in W LAN): is a proxy between the supplicant and the AAA server



This supplicant described here above is composed of 3 bricks for EAP-SIM:

**EAP:** EAP-request packet parsing and EAP-response packet construction

**MAC:** Server MAC verification and Client MAC construction, providing mutual authentication above A3/A8 authentication

**Algo:** A3/A8 algorithm execution (this part is always performed by the SIM, as it runs the GSM algorithm)

There are three ways to share this supplicant work between the handset (which may be WM2003/5 or Symbian or a proprietary O/S) and the SIM:

### 1) All on the SIM

In this case, all the calculation and ciphering is done inside the SIM card. The handset supplicant receives the EAP requests from the access point, sends them to the SIM card in an “EAP AUTHENTICATE” APDU command, receives the EAP-response in the APDU response, and sends it to the access point.

### 2) Shared between SIM and device

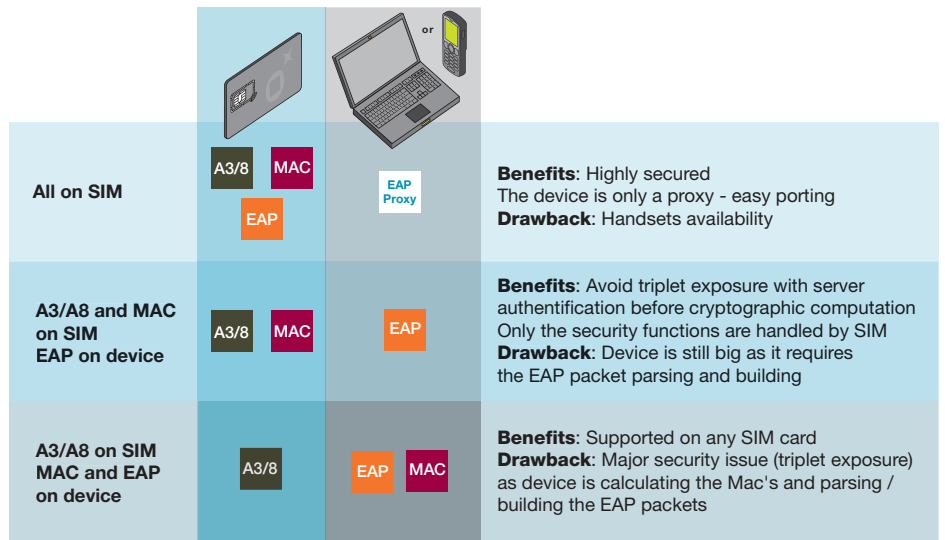
As for WLAN-SIM, where the SIM handles the cryptographic calculation and the device analyses the EAP packets received from the access point and builds the EAP packet responses.

### 3) All on the device

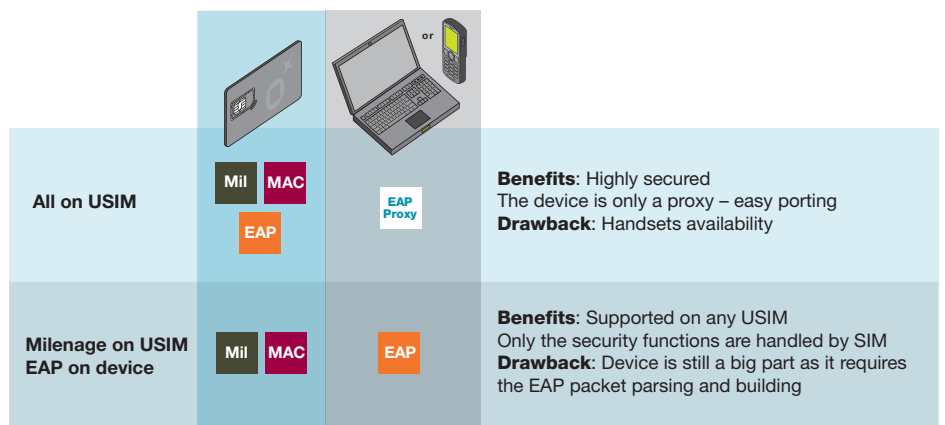
Where there is no need for a specific EAP application on the SIM, the device supplicant normally sends the standard 2G authentication command (Run GSM Algorithm) to the card and handles the MAC calculation/verification and the EAP packet part. This option is only applicable to handsets.

Option (1) is the chosen solution for this demonstration, for the following reasons:

- it minimizes the porting effort from one terminal to another
- allowing the terminal to send a Run GSM Algorithm command is not secure - a brute force attack could break the key
- the terminal has to be ported to different systems (XP, 2K, MAC OS, Linux, Unix, PocketPC, Symbian, PalmOs, J2ME, etc.), so it is convenient to have the terminal component as small as possible

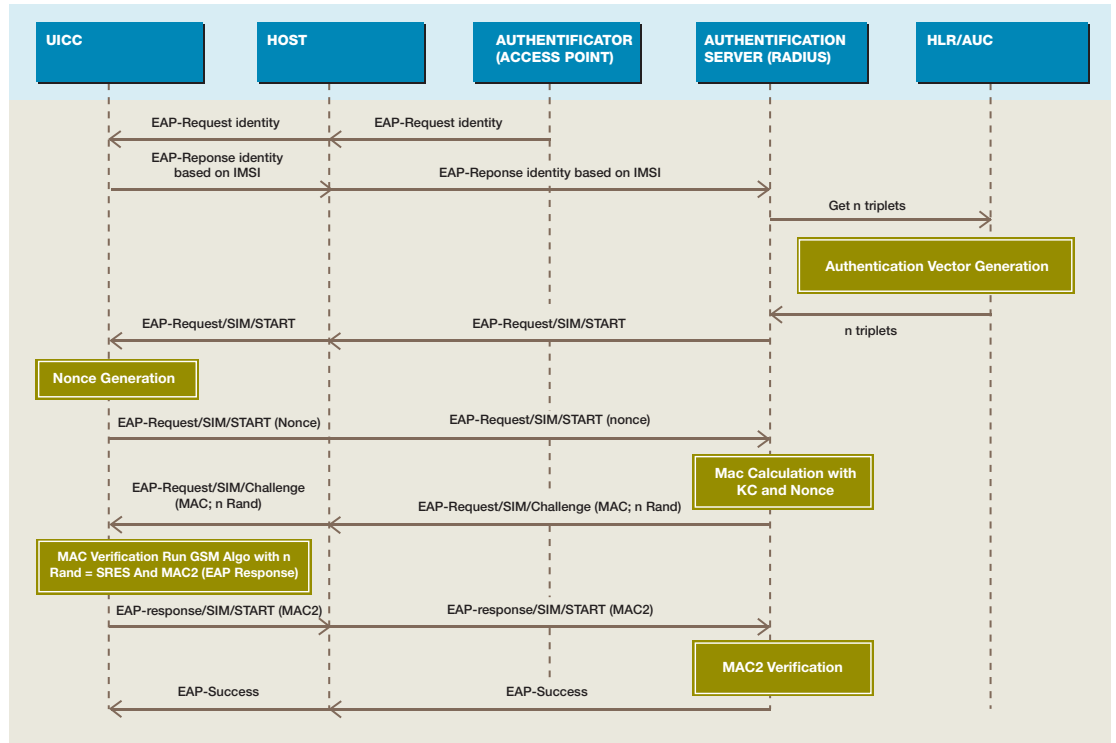


For EAP-AKA only two implementations are possible, as the MAC is part of the AKA mechanism. Again, we recommend executing all the protocol in the SIM, to ease the host implementation.



## > Detailed architecture of EAP-SIM / AKA

EAP-SIM or AKA connection to WiFi network is based on mutual authentication. The following schematic details the information flow performed during authentication



**EAP-SIM exchanges flows**

### Authentication example

Figure 5 shows an example of EAP-SIM full authentication.

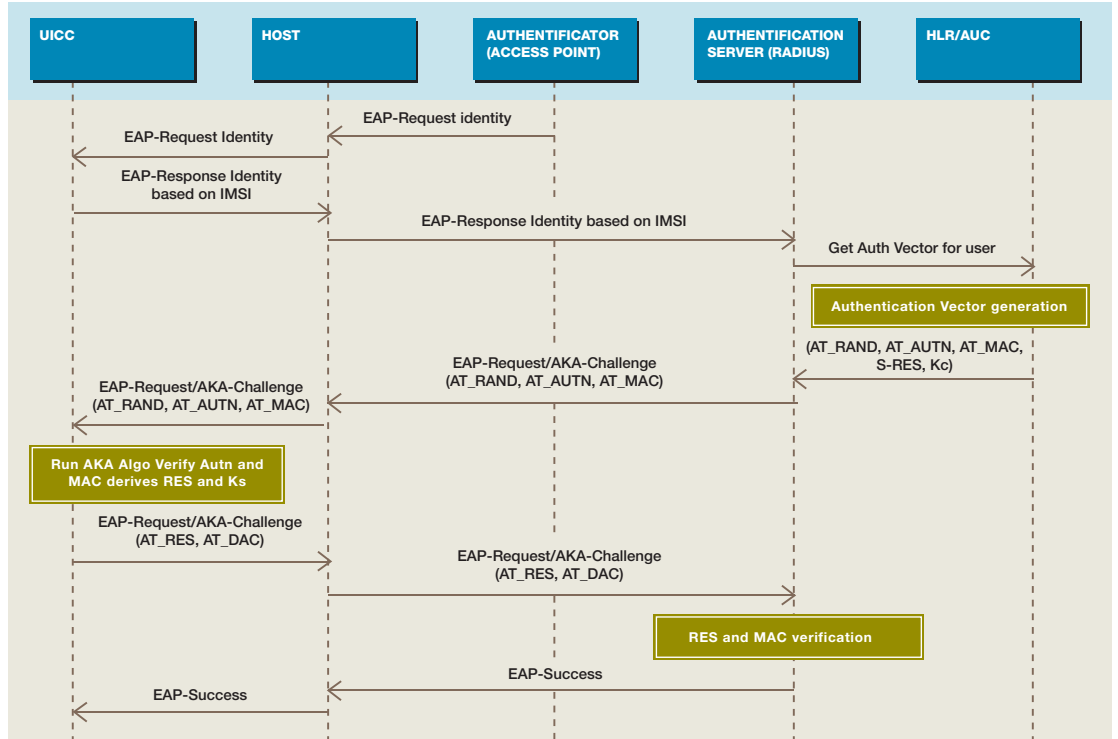
- Authentication is triggered by a request for client identification.
- During the whole authentication, the host role is to transfer requests and response between the UICC and the authenticator
- UICC's (the supplicant) response includes either the user's International Mobile Subscriber Identity (IMSI) or a temporary identity (pseudonym). From this point on, the authenticator only plays the role of a relay agent, shuttling messages back and forth between the supplicant and the AAA server.
- The UICC receives an EAP Request of type SIM/Start from the authenticator and replies with the corresponding EAP Response including a random number (NONCE) chosen by the supplicant.

- After receiving the EAP Response/SIM/Start, the AAA server obtains n GSM triplets from the user's home operator Authentication Center (AuC) on the GSM network. From the triplets and other authentication parameters (Identity, EAP version, NONCE) the AAA server derives the keying material:

- o The authentication key  $K_{aut}$  to be used with the MAC attributes,
- o The encryption key  $K_{encr}$ , to be used with the ENCR\_DATA attributes.
- o Eventually, the master key and other application specific keys may be also derived
- o The authentication key  $K_{aut}$  is used to compute the message authentication code (MAC) to be used in subsequent EAP messages. This MAC may contain message specific content (e.g. as shown in figure1, MAC (message | NONCE) will be the MAC of concatenation of the EAP message with the NONCE attribute).

Authentication using AKA (3G) is broadly similar, except that network authentication is already included in the authentication vector provided by the HLR/Auc.

Note that the same level of security is obtained when the EAP-SIM supplicant is all in the SIM.



**EAP-AKA exchange flows**

### > 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, mainly the low impact level on devices or network. After detailed analysis, however, it appears that these methods endanger the subscriber, as in most cases sessions can be hacked and billed to him.

#### Basic Authentication

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

#### 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 these methods present threats to security, as the information flows could be hacked during the exchange between devices to server.

#### WEP/WPA keys

Mostly used at home for WiFi authentication to DSL boxes, the WEP key method presents two constraints:

- Key provisioning: for first WiFi connection to the box (WiFi pairing) and to hotspots, the user has to enter the WEP key manually, at initialisation stage at least.
- Portability constraints: after the 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 switch on a device or needs to connect to a new hotspot.

### 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 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 needs 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.

### Certificate

It is also possible to use certificate based mutual authentication, but each client must have a certificate. Certificate contains information on the proprietary of it and is cryptographically signed by the certificate issuer.

## > EAP-SIM and EAP-AKA Implementation

The EAP-SIM and EAP-AKA solution is implemented as follows

On the network side the operator will reuse (or install) the Radius Server connected to an HLR, to use SIM or AKA authentication vectors. Most principal Radius server providers already support both EAP-SIM and AKA in their products.

On the host side we need to differentiate between mobile phones and PCs - if it is easy to write and install software on a PC, it is not always the case with a mobile phone.

### The PC:

Gemalto can provide a supplicant for PCs running Windows XP. This supplicant makes the link between the PCSC and the PCSC Windows component. The complete EAP-SIM solution is also supported in a Gemalto Smart Dongle, offering a simple way for both operators and users to access WiFi network from any PC.

### The Mobile:

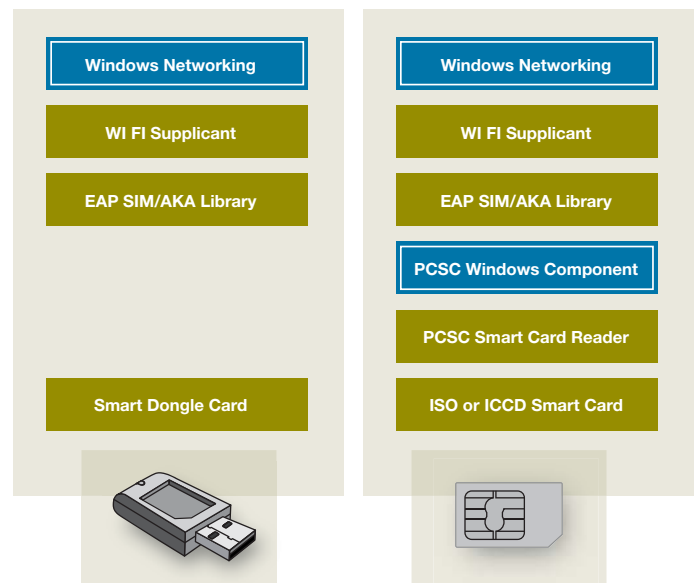
In this case the supplicant is OS-dependent, meaning that it needs to be adapted to each handset operating system: Microsoft, Symbian, non-Open OS, for example.

Certificate usage is based on public key infrastructure (PKI), so is linked to key pair, one being public, and the other secret. The public key will be 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, due to the fact that the certificates with their key pairs need to be distributed in a secure way to their owners.

## Windows XP software architecture



# Operators' and end-users' benefits

The SIM-based approach described above offers significant benefits for operators and end users, which can be summarised as follows:

## For operators, it offers the ability to:

- **launch quickly**, with re-use of existing infrastructure
- **complement existing data services** with a service that is attractive to the most valuable customers (the business users)
- **acquire new non-telephony customers** and partners while re-using existing infrastructure

## End users can enjoy easy access to WiFi and services:

- **highly secure**: the solution gives the business user the highly secure access to PWLANs essential for their work
- **ease of use**: the user selects the access point, and then clicks once to connect
- **simplicity**: users receive one consolidated bill, and have one customer care number to call
- **widely available**:, the SIM-based approach supports the roll-out of roaming partnerships

## About Gemalto

Gemalto (Euronext NL 0000400653 GTO) is a leader in digital security with pro forma 2005 annual revenues of 1,7 billion (\$2.2 billion), operations in 120 countries and 11,000 employees including 1,500 R&D engineers. The company's solutions make personal digital interactions secure and easy in a world where everything of value -from money to entertainment to identities- is increasingly represented as bits and bytes communicated over networks.

Gemalto thrives on creating and deploying secure platforms, portable and secure forms of software in highly personal objects like smart cards, SIMs, e-passports, readers and tokens. More than a billion people worldwide use the company's products and services for telecommunications, banking, e-government, identity management, multimedia content, digital rights management, IT security and other applications. Gemalto was formed in June 2006 by the combination of Axalto and Gemplus International S.A. For more information please visit [www.gemalto.com](http://www.gemalto.com).

## References

ETSI TS 102 310, Smart Cards: Extensible Authentication Protocol support in the UICC Release 6

IETF RFC 4186, EAP SIM

IETF RFC 4187, EAP AKA

3GPP TS 33.102 Release 6. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture

3GPP TS 35.206 Release 6. Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1\*, f2, f3, f4, f5 and f5\*; Document 2: Algorithm Specification

3GPP2 S.S0055-A v2.0 Enhanced Cryptographic algorithms

3GPP TS 55.205 Release 6. Specification of the GSM-MILENAGE Algorithms: An example algorithm set for the GSM Authentication and Key Generation functions A3 and A8

# A wide range of solutions

[www.gemalto.com](http://www.gemalto.com)

© Gemalto 2007 • All rights reserved • 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