Offering
SIM Strong Authentication
to Internet Services

Whitepaper

Simple, efficient and secure



FIRST PRESENTED AT THE 3GSM WORLD CONGRESS,
BARCELONA 13 - 16 FEBRUARY 2006

Index

Offering SIM Strong Authentication to Internet Services

A joint white paper by Telenor, Axalto, Lucent Technologies, Ulticom, Linus, Oslo University College and Sun Microsystems

Dr. Do van Thanh, Telenor
Armand Nachef, Axalto
Jean Daniel Aussel, Axalto
Ivar Jørstad, Telenor
Richard Perlman, Lucent Technologies
John Vigilante, Ulticom
Do van Thuan, Linus
Dr. Tore Jønvik, Oslo University College
Fulup Ar Foll, Sun Microsystems

Executive Summary

This paper presents an innovative service called SIM strong authentication service that extends the usage of GSM SIM authentication to Internet Web services. The goal of this proof-of-concept is to demonstrate the possibility of implementing innovative service in a heterogeneous environment using Liberty Alliance Federation Standard. Telenor, Axalto, Linus and Oslo University College have implemented a proof-of-concept prototype in Oslo. The architecture is based on a multi-vendor environment where SUN provides the Identity Provider, IBM the Identity Provider and Service Provider Proxy to connect non-Liberty Alliance Service Providers to the system, Lucent Technologies the Radius server and Ulticom the SS7 MAP Authentication Gateway connecting the prototype to the Telenor mobile network.

A typical user flow for such a service would be the case of a user browsing on the World Wide Web from home, a customer premise, an Internet café, etc. When trying to access a protected resource such as Webmail, company portal, or bank account, he logs on to the requested secured site simply by placing his mobile phone close by and communicating with his PC via Bluetooth, or using a SIM card-equipped dongle, card reader, or 2G/3G PC card.

This service is available anywhere and can support any Internet services. It is ideal for services like Internet Banking, eAdministration or enterprise internal web pages. The SIM strong authentication is both user-friendly and cost efficient, with a low deployment threshold. The technology is also capable of supporting other Smart-Card based identity services such as USIM (UMTS), certificate based schemes (E.g. TLS) and One Time Password schemes (OTP). A demonstration of the SIM based service is being demonstrated at the 3GSM World Congress in Barcelona, February 2006.

1 Introduction

The popularity of the World Wide Web continues to grow due to the abundance of information, services, commerce, and recreation that people enjoy from Internet based resources. However, in order to have access to much of the most useful information and services - while keeping an acceptable level of security, users must remember more and more usernames and passwords. The growing number of username and password pairs continue to increase and will soon be a nightmare to users. Furthermore, the use of passwords as a means of authentication is not strong enough for services that require added security, like e-commerce, online banking, government portal, corporate Intranet access, IP telephony, etc. Stronger authentications are required but unfortunately, they are usually both costly and not particularly user-friendly.

Telenor, Linus, Oslo University College and Axalto in collaboration with SUN, IBM, Lucent Technologies and Ulticom have designed and implemented a strong authentication service that is both cost efficient and user-friendly. The idea is to extend the usage of the current SIM authentication used in GSM to Web services. Indeed, this is a step further from earlier work that uses SIM authentication for WLAN (Wi-Fi – EAP-SIM). The idea of making the mobile phone and its SIM a universal authentication token is compelling since the mobile phone is definitely the most used device nowadays and the GSM network is currently the largest mobile network and is ubiquitous in much of the world.

This paper presents the Telenor SIM strong authentication service. It starts by summarising the state-of-the-art solutions for strong authentication and their limitations. An overview of our SIM strong authentication service will then be given. A scenario showing how our SIM strong authentication service works will be depicted. The values brought to the users and the service provider will be identified. The business opportunities for the mobile operators are also analysed.

It then explains how the Liberty Alliance Framework can be used to leverage this SIM based strong authentication solution in a heterogeneous multi-vendor environment, that bridges Internet based services and the GSM network.

2 Limitations of state-of-the-art solutions

2.1 Passwords

As mentioned earlier, the most common authentication scheme today is based on passwords. It is both weak and not user-friendly due to its plurality. There are many issues with user password management but from a security point of view there are three main issues as follows:

- User Friendly: It is always possible to propose systems with high security but if they are not sufficiently simple and friendly the user will find a way to bypass them.
- Phishing: (stealing user password by having them to give their credential away to the wrong party): Keep asking gently a passwords to a user and at some point he will give it away. Most well known methods for phishing user password is either to reproduce an almost identical login page to the one the user is used to, or by pretending to be from customer service and requesting a password for some special operation. The main rule of phishing is “if you can lock a user for a reason” then will be ready to give you all the passwords he knows to unlock the situation “current one, old one, one from another site…”.
- Brain limit: Typical user will only remember from 3 to 5 login/passwords. They will either reuse the same credential all over, creating a potential risk of correlation in between service providers, or will stick the most secure one on a “post-it” somewhere on a very well hidden place such as “under his keyboard”.

To tackle the latter problem and other identity related issues, the Liberty Alliance [1] has promoted the concept of federated network identity that enables users to seamlessly jump from one service provider to an other one using single-sign-on, while warranting user privacy, an adequate level of authentication for the requested service and provider independence. However, while Liberty specifies how a service provider requests for a given level of authentication it does not normalize how the CoT authentication authority (i.e. Identity Provider) negotiates credentials with or on behalf of the principal. The problem of weak authentication then remains unsolved, leaving room for user password Web Phishing and Post-It leaking.

2.2 Stronger authentication schemes

There exist today several strong authentication alternatives that require the user to present at least two factors, i.e. something that you know (PIN, code or password) combined with something that you have (a smart card or an authentication token) or sometimes something that characterizes you (biometrics). The smart card or authentication token may carry One-Time-Password (OTP) or Public Key Infrastructure (PKI). These solutions bring sufficient protection both to the users and service providers but, unfortunately, they all suffer from significant drawbacks:

- Costly infrastructure: Strong-authentication solutions require specialized security hardware (such as tokens and smart cards), dedicated software and IT server infrastructure. In addition, there is a cost related to the administration of the keys and certificates.
- Lack of interoperability: Strong authentication solutions are quite often proprietary and do not operate with each other.
- Poor structure: They do not provide well-defined interfaces that allow integration with new applications or services.
- Lack of scalability: Most current solutions are standalone and it is very difficult to extend them to be a global solution that can be used by every user, everywhere and anytime.
- Cost of deployment: Not only special devices have to be given to each user, but each service provider needs to be customized to support the specific API and handshake protocols specific to the chosen device.

Because of the cost of deployment, this solution has been mostly limited to protect access gate to a secure zone (typically a VPN for an enterprise).

2.3 Dynamic passwords

One alternative addressing some of the mentioned issues is to provide the users with a dynamic password they can use to log in. The users do not have to remember the passwords and there is no risk of compromised passwords since they are used only once. What the users need is a mobile phone that is capable of receiving SMS messages used to carry the dynamic passwords transferred by the service provider. This solution is, however, not very user-friendly since the users have to type in the password. In addition, a system for generating dynamic passwords is also needed and may be costly.

Because of the lack of user friendliness, this solution can not be use for day to day operation, and is mostly limited to exceptional operations such as connecting to the Internet from a hotspot at an airport, hotel, gas station, etc.

3 Our SIM strong authentication service

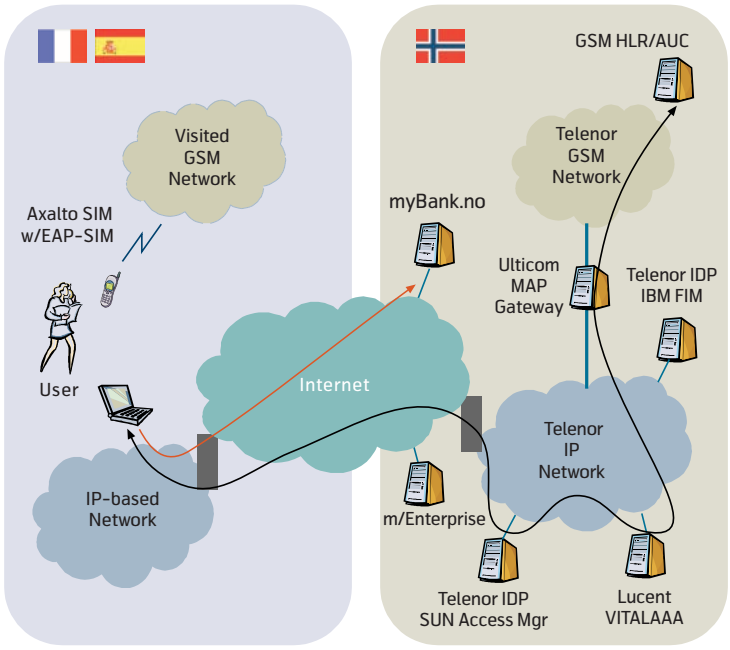
To remedy the situation described above, it is proposed a SIM based strong authentication service that extends SIM card GSM authentication to Web services.

Briefly, the SIM strong authentication service can be described as follows:

- A user with a valid Telenor mobile subscription having one of the following:
  - A mobile phone with a SIM and Bluetooth placed close to a Bluetooth enabled PC
  - A dongle (with a SIM) mounted on the PC
  - A card reader (with a SIM) installed in the PC
  - A GPRS/3G PC card (with a SIM) installed on the PC
- May quite easily and securely log on to
  - An Internet bank
  - A corporate intranet
  - A commerce webshop
  - An Enterprise web site
  - An eGovernment application
- At anytime and anywhere in the world.
- The authentication is done by the Telenor Identity Provider (IDP) server based on Sun Access Manager in collaboration with a Lucent Technologies Vital*AAA* server that communicates with the Telenor Home Location Register (HLR) via an Ulticom SignalwareSS7/IP MAP Authentication Gateway.

The overall architecture of the SIM strong authentication service proof-of-concept implementation is shown in Figure 1.

Figure 1.
Overall architecture of the SIM strong authentication service



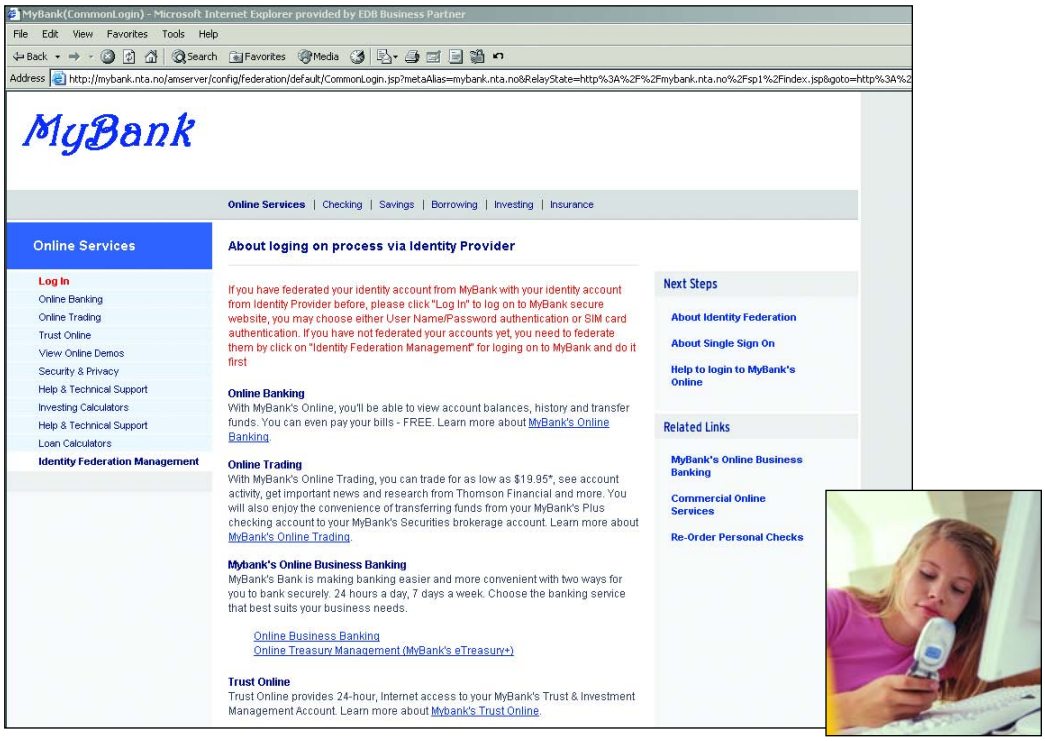
The advantages of the SIM strong authentication service can be summarised as follows:

- Removes the user's burden of remembering passwords
- Provides an authentication service that is both strong and easy to use
- Allows rapid deployment due to the high penetration of mobile phones
- Reuses existing GSM authentication structures (SIM card and HLR)
- Allows the integration of all services and applications
- Uses open standards and supports interoperability with other systems
- Provides scalability and supports a large number of users and service providers

4 How does SIM strong authentication service work?

To illustrate how the SIM strong authentication service works, let us consider the scenario of Kari, a user travelling abroad who attempts to log on to her Internet bank. Kari has a mobile subscription at Telenor and her mobile phone is equipped with an Axalto SIM which supports the EAP-SIM protocol, provided by Telenor. Her bank myBank has a business agreement with Telenor concerning the usage of the SIM authentication service for its customers.

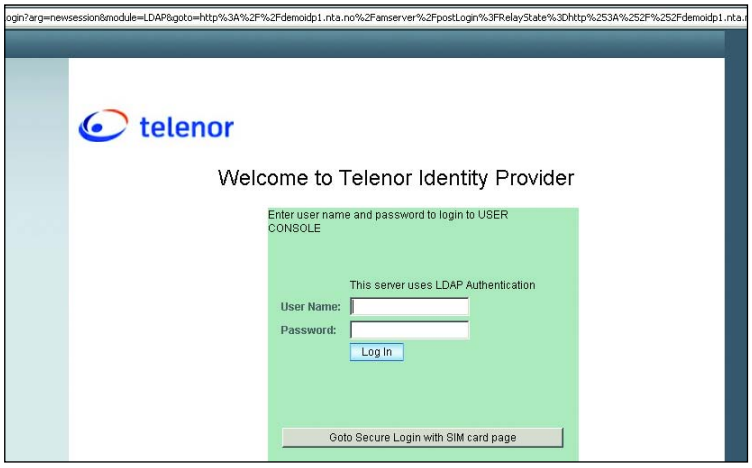
Figure 2.
myBank web site



1. Kari connects her laptop on the Internet and is visiting the myBank web site as shown in Figure 2.

2. When she attempts to log in she is redirected to the Telenor Identity Provider web site as shown in Figure 3.

Figure 3.
Telenor Identity Provider web site

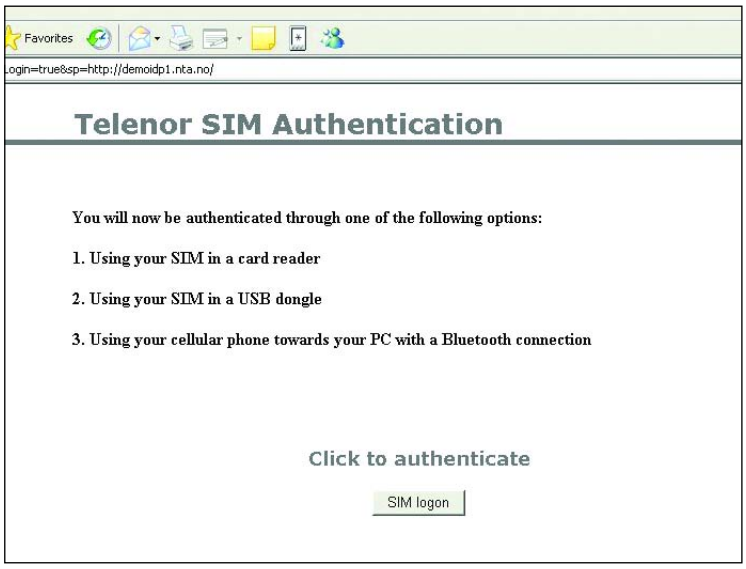


Kari clicks on the “Smartcard logon” button. She is then select one of the three authentication options (Figure 4):

- Using the SIM card in the card reader
- Using the USB dongle or integrating the SIM card
- Using the cellular phone with Bluetooth

When ready, Kari clicks on and the authentication begins.

Figure 4.
Selection of authentication token



3. A mutual authentication using EAP-SIM [2] is performed between the Telenor network and the SIM card (A detailed description of the authentication process is included below). Depending on the security settings Kari has established for her SIM card, she may be asked to enter her EAP-SIM card application PIN code to allow the mutual authentication to be performed

4. After the successful authentication, the Telenor IDP redirects the browser back to myBank where Kari is now logged in and a Welcome page is displayed. Kari can carry out all her transactions.

5. After a while, Kari goes to her enterprise Intranet. This time she is automatically logged in since she has already been authenticated and that authentication is still valid.

5 EAP-SIM

EAP-SIM is a recognized EAP (Extensible Authentication Protocol) Type and is defined in an IETF draft (draft-haverinen-pppext-eap-sim-16.txt). The EAP-SIM peer interface between the terminal and SIM is standardized by:

- ETSI in TS 102.310
- And “WLAN Smart Card Consortium” in “WLAN-SIM-V11.pdf”.

EAP-SIM specifies an Extensible Authentication Protocol (EAP) mechanism, called an EAP *Type*, for authentication and session key distribution using the GSM Subscriber Identity Module (SIM).

GSM authentication is based on a challenge-response mechanism. The A3/A8 authentication algorithms that run on the SIM can be given a 128-bit random number (RAND) as a challenge. The algorithm takes the RAND and a secret key Ki stored on the SIM as input and produces a 32-bit response (SRES) and a 64-bit long key Kc as output.

EAP SIM mechanisms specify enhancements to GSM authentication and key agreement whereby multiple authentication triplets can be combined to create authentication responses and encryption keys of greater strength than the individual GSM triplets. The mechanism also includes network authentication, user anonymity support and a fast reauthentication procedure.

Authentication example

Figure 5 shows an example of EAP-SIM full authentication. Authentication is started with a request for client identification. The software process on the client platform that performs the EAP-SIM negotiation is called the supplicant. The supplicant’s 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.

Next, the supplicant 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’s Authentication Centre (AuC) on the GSM network. From the triplets and other authentication parameters (Identity, EAP version, NONCE) the AAA server derives the keying material:

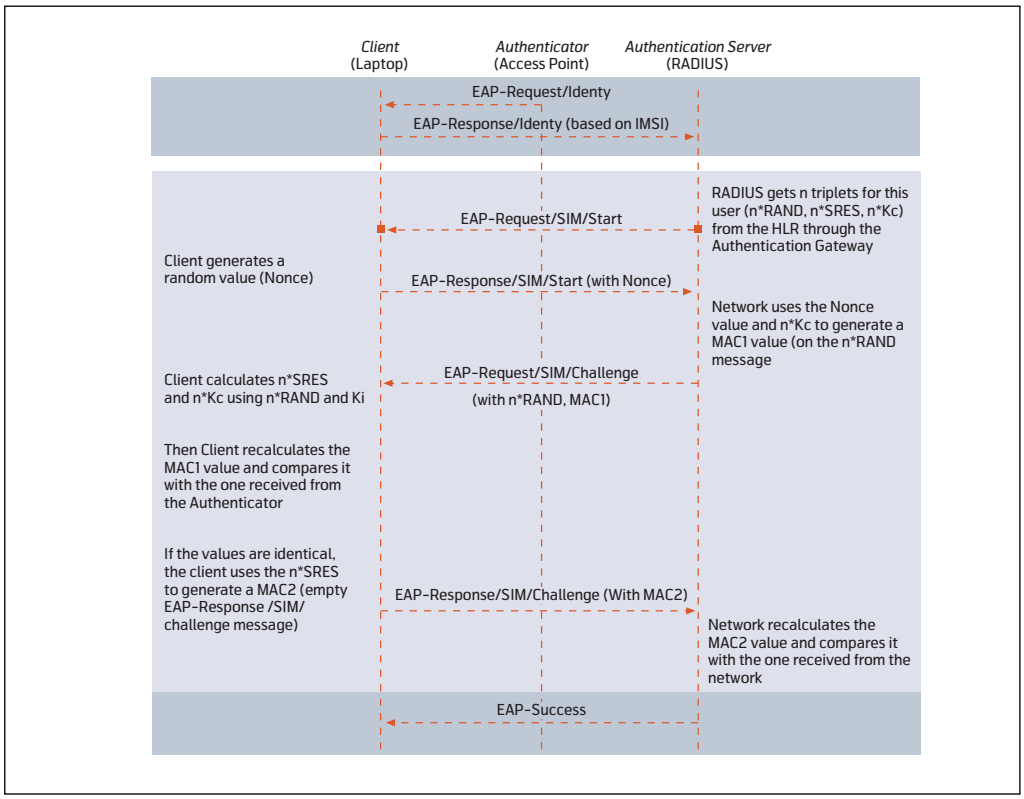
- The authentication key K_aut to be used with the MAC attributes,
- The encryption key K_encr, to be used with the ENCR_DATA attributes.
- Eventually, the master key and other application specific keys may be also derived

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 I NONCE) will be the MAC of concatenation of the EAP message with the NONCE attribute).

The encryption key is used to encrypt the ENCR-DATA attributes. This encryption also uses an Initialization vector (IV) that is a mandatory attribute in all EAP messages where any encrypted attribute is present. Finally, the master key may be used to protect the radio link depending on the different 802 security protocols used.

Once the key has been calculated it is possible for the AAA server to send an EAP Request/SIM Challenge including the RAND of the GSM Triplets, an encrypted next client identity, and the MAC including the NONCE to be sent back to the supplicant.

Figer 5.
Example of EAP-SIM full authentication



Once the supplicant has received this challenge, it will run the GSM Algorithm to obtain the GSM triplets, then derive the keys as done in the server, and compute the MAC to compare it with the server-calculated MAC. If the MACs match the network is identified as one knowing GSM triplets and the client originated NONCE random number. If the network authentication is correct, the supplicant responds with the EAP Response SIM/Challenge, containing the MAC attribute that includes the client's SRES response values.

The *AAA* server verifies that the MAC is correct and sends an EAP-Success packet, to the authenticator indicating that the authentication was successful.

6 EAP-SIM implementation for authentication to Internet services

Installation of EAP-SIM specific software on the client PC is not required.

An ActiveX compliant supplicant with [4] and [5] is automatically downloaded from IDP. This ActiveX supplicant can run in the MS Internet Explorer. Its main functions are

1 Receive the EAP-request packets from the EAP Authenticator
2 Send the contents of these packets to SIM as specified in [4] if the TS 102.310 EAP-SIM card application is installed in SIM, or as specified in [5] if the WLAN-SIM card application is installed in SIM.
3 Build the EAP-response packets from the SIM responses
4 Send back the EAP-response packets to the EAP authenticator

The EAP Authenticator is implemented as a Java servlet inside the Telenor IDP. So, this servlet communicates through the ActiveX module to the Axalto SIM card. The EAP Authenticator first requests the EAP identity from the SIM (via the supplicant) and sends the identity received to the Lucent Technologies Vital*AAA* server. Note the first permanent EAP identity contains the IMSI.

The Telenor IDP communicates with the Active-X supplicant running in the MS Internet Explorer browser on the user's laptop, which in turn communicates with the SIM to request the IMSI (International Mobile Subscriber Identity) or a temporary identity.

After receiving the EAP Identity from the supplicant (relayed via the IDP Authenticator), the Vital*AAA* server sends a request for triplets corresponding to the SIM IMSI to the Telenor HLR. Because the current generation of HLRs are only accessible via the SS7 protocol, an IP to SS7 gateway is required for the *AAA* server to access data stored in an HLR. The Vital*AAA* server sends requests for HLR data to the Ulticom Signalware MAP Authentication Gateway via a special interface application. The Signalware gateway then formats MAP messages which are sent to the HLR and the resulting response is returned to the Vital*AAA* server.

Authentication triplets are not stored in the HLR, but are generated as needed by the Authentication Centre (AuC) in the HLR. After receiving the MAP request from the Signalware gateway, the Telenor HLR requests the triplets from the AuC and returns them to the *AAA* server through the MAP gateway.

The Vital*AAA* server then sends the challenges contained in the triplets to the Telenor IDP authenticator servlet that then forwards them to the ActiveX supplicant in the MS Internet Explorer browser.

The browser ActiveX supplicant communicates with SIM that will

1 Verify the MAC1 received from Radius in order to authenticate the server
2 Calculate a MAC2 to be sent to the *AAA* server (through the IDP servlet).

If the *AAA* server verifies that MAC2 is correct, it informs the IDP about the mutual authentication success and the IDP then redirects the browser back to the application provider, in this case, myBank for Kari.

Upon successful authentication the Telenor IDP will return a Single-Sign-On token to the browser and redirect it back to the service service provider. The service provider will verify the Single-Sign-on token before granting access to its services.

Additional protections:

In addition to the inherent authentication capabilities provided by the SIM based identity, the Vital*AAA* server can also provide other means of controlling system access via authorization policy. For example:

- Users may be limited to a list of applications
- Access may be limited to specific geographic locations
- Time-of-Day and Day-of-Week controls can be applied
- Accounts may be temporarily blocked for business purposes
- Security measures may be applied to reject stolen or compromised SIMs

- Each user access can easily be logged and logs shared in real time with the appropriate application provider.

7 Value proposition

7.1 To End Users

The SIM strong authentication service will deliver value to the end users in the following ways:

- Simple and better control and management of their identities: The user does not have to manage a multitude of passwords. All the end user needs is a SIM card and a mobile phone, a USB dongle, or a PC GPRS/3G Data card with a SIM card.
- Better protection and higher level of security: The SIM strong authentication service will provide much better protection than the passwords.
- Ease of use: The SIM strong authentication service is very simple to use and does not require any particular technical skill. The log in will be easy and quite intuitive.
- Single-sign-on: After a successful authentication, the user does not have to log in again when visiting other service providers using the SIM strong authentication service. The availability of Single-Sign-On access is time limited for security purposes.
- Universal applicability: The SIM strong authentication service can be used for any service or application and the user does not need to use several different authentication solutions.
- Global availability: The SIM strong authentication service can be used anywhere and even when there is no GSM coverage. Indeed, even with a non-operational phone due to lack of coverage, the SIM-based authentication can still be performed via Bluetooth.

7.2 To Service Providers

The SIM strong authentication service will bring the following benefits to the service providers:

- Better protection and higher level of security: The SIM strong and mutual authentication service will provide higher protection of the valuable assets of the service providers and contributes to extend the availability of their services.
- Cost saving: By replacing their current authentication schemes that are mostly password-based with the SIM strong authentication service, the service providers may save money since the operation and maintenance costs are lower due to the simplicity of the SIM strong authentication service..
- Lower threshold for deployment: The service providers do not have to invest large amounts of money to deploy the SIM strong authentication service because the mobile operator manages most of the infrastructure. No great technical expertise is required and the SIM strong authentication service fits very well for larger enterprises and SMEs.
- Simpler customer management: The service providers do not have to take care of the password management since the mobile operators will assume this.
- Reach more customers: The service providers may also reach new customers that are subscribers at the mobile operators.

7.3 To Mobile Operators

To the mobile operators, the SIM strong authentication service will bring the following benefits:

- New source of revenues: The SIM strong authentication service constitutes a new source of revenues for the mobile operators which is not based on the sale of air traffic. This source of revenues does have large potential since it brings value to the end users and service providers.
- Reuse of existing infrastructure: Because the SIM authentication solution uses the same SIM and HLR infrastructure used for normal GSM and GPRS services, it allows the reuse of the GSM expertise of the mobile operator.
- Improved customer loyalty: The SIM strong authentication service will be a valuable service to end users and will hence contribute to improving customer loyalty and reducing churn.
- New business customers: As a compelling service, the SIM strong authentication service will attract new customers for the mobile operator.
- Strengthened position: By extending the role and the value of the mobile phone and SIM to the computing world, the SIM strong authentication service will contribute to considerably strengthening the mobile operator's position in the new converged ICT world.

- Easy adaptability for the future: Because the SIM strong authentication is based on easily changeable software elements (Active-X supplicant, IDP Java Authenticator, Vital*AAA* server and Signalware gateway) it can be easily modified and upgraded to support emerging and future technologies. For example: UMTS USIMs, Smart Card based Certificates, Smart Card based One-Time-Password (OTP) schemes, etc. Because of the flexibility of the platform described in this paper it is quite possible to support multiple authentication schemes over a single authentication infrastructure.

8 Conclusion

In this paper, a SIM strong authentication service is presented. By its usage simplicity, its high level of security, its universal applicability and its cost efficiency, the SIM strong authentication service will most likely be a successful service in the near future. A proof-of-concept implementation has been completed by Telenor, Axalto, Linus and Oslo University College in collaboration with SUN, IBM, Lucent Technologies and Ulticom. A demonstration of the service will be shown at the 3GSM World Congress in Barcelona, Spain, February 2006.

Reference

[1] Liberty Alliance	The Liberty Alliance Project - *http://www.projectliberty.org*
[2] EAP SIM	EAP SIM - draft-haverinen-pppext-eap-sim-16.txt- IETF
[3] EAP AKA	EAP AKA - draft-arkko-pppext-eap-aka-15.txt - IETF
[4] EAP on UICC	EAP-support on UICC - TS 102310 v060100p - ETSI - 3GPP
[5] WLAN-SIM	WLAN-SIM, WLAN Smart Card Consortium
[6] EAP	Extensible Authentication Protocol – RFC 3748 - IETF
[7] Radius	rfc2865.txt (Remote Authentication Dial In User Service), IETF
[8] Radius Extension	rfc2869.txt (Radius Extensions – including EAP), IETF

Glossary

Access manager

Sun Java System Access Manager delivers open, standards-based access control across intranets and extranets. It is a security foundation that helps organization manage secure access to an enterprises' Web applications both within the enterprise and across business-to-business (B2B) value chains. It provides open, standards-based authentication and policy-based authorization with a single, unified framework. It secures the delivery of essential identity and application information to meet today's needs and to scale with growing business needs, by offering single sign-on (SSO) as well as enabling federation across trusted networks of partners, suppliers, and customers

A3 Algorithm 3, authentication algorithm; used for authenticating the subscriber

A5 Algorithm 5, cipher algorithm; used for enciphering/deciphering data

A8 Algorithm 8, cipher key generator; used to generate Kc

AAA **server, EAP server, or backend authentication server**

These 3 terms are used interchangeably in this note. *AAA* stands for Authentication, Authorization, and Accounting. A backend authentication server is an entity that provides an authentication service to an authenticator. RADIUS is an *AAA* server.

AuC Authentication Centre. It is the GSM network element that provides the authentication triplets for authenticating the subscriber

Authenticator The component that initiates the EAP authentication. In this document the authenticator is running in IDP.

EAP Extensible Authentication Protocol

EAP-AKA An extension to the EAP (Extensible Authentication Protocol) proposed by the IETF (Internet Engineering Task Force) enabling authentication and session key distribution using the UMTS AKA (Authentication and Key Agreement) mechanism.UMTS AKA is based upon symmetric keys and runs typically on a USIM (UMTS Subscriber Identity Module). EAP/AKA Authentication includes optional user anonymity and re-authentication procedures.

EAP-SIM An Extension of the Extensible Authentication Protocol (EAP) using the Global System for Mobile Communications (GSM) Subscriber Identity Module (SIM). EAP-SIM is described in internet-draft for EAP-SIM

ETSI European Telecommunications Standards Institute

GSM Global System for Mobile Communications

HLR Home Location Register. It is a central database containing the subscriber profiles and the associated keys

IDP According the Liberty Alliance specifications an Identity Provider creates and manages the identity of the users, and authenticates them to the service providers;

IMSI International Mobile Subscriber Identity

Kc Cryptographic key; used by the cipher A5

Ki Subscriber authentication key; the cryptographic key used by the authentication algorithm, A3, and cipher key generator, A8

LAN Local Area Network

MAC Message Authentication Code

MNO Mobile Network Operator

NAI Network Access Identifier

Peer or Supplicant The end-user software that responds to the authenticator. In this document, the supplicant is the ActiveX running in MS Internet Explorer

RAND A random challenge issued by the network

SIM Subscriber Identity Module

SME Small or medium-sized enterprise

Telenor

Telenor is the largest provider of telecommunications services in Norway, and has substantial international operations. Telenor is a total telecom operator having mobile, fixed and broadcast operations. Mobile is Telenor's principal focus area for future growth. Telenor has ownership interests in 12 mobile operations in Europe and Asia. In the fixed operation, Telenor provides communications solutions to both the business and residential markets, including analogue and digital (ISDN) telephony, broadband, Internet access, data services and leased lines. In the broadcast operation, Telenor has a stake in all parts of the TV value chain, all the way from content and transmission (transfer of signals) to distribution (subscriptions).

www.telenor.com

Axalto

Axalto is the world's leading provider of microprocessor cards (Gartner, 2005) and a major supplier of point-of-sale terminals. Axalto's span of intervention covers the telecommunications, public telephony, finance, retail, transport, entertainment, healthcare, personal identification, information technology and public sector markets. The company recorded sales of over $960 million in 2004 and is fully-listed on Euronext, the pan-European market. Its 4,500 employees come from over 60 different countries and serve customers in more than 100 throughout the world.

www.axalto.com

Linus

Linus is an SME that provides mobile services to leading Norwegian content providers and SW development and system integration to the Telecommunication business segment. Linus is active in several pan-European research projects.

www.linus.no

IBM

IBM is the world's largest information technology company, with 80 years of leadership in helping businesses innovate. Drawing on resources from across IBM and key Business partners, IBM offers a wide range of services, solutions and technologies that enable customers, large and small, to take full advantage of the new era of e-business. For more information about IBM, visit

www.ibm.com

Oslo University College

Oslo University College is the biggest governmental university college in Norway with approximately 8,700 students and more than 1,000 staff members. They offer twenty-two professional study programs and a large number of credit courses at bachelor, master and higher level and within a broad range of fields. Oslo University College prepares students for professional careers in public institutions - within health and social services, education and management, libraries and archives, in media and fine arts, and for technical, economic and administrative occupations in trade and industry. The Faculty of Engineering focuses on civil engineering, computer and information technology, including informatics and network and system administration.

www.hio.no

Ulticom, Inc.

Ulticom provides service-enabling signaling software for wireless, wireline, and Internet communications. Ulticom's products are used by leading telecommunication equipment and service providers worldwide to deploy mobility, location, payment, switching, and messaging services. Traded on NASDAQ as ULCM, Ulticom is headquartered in Mount Laurel, NJ with additional offices in the United States, Europe, and Asia. For more information, visit

www.ulticom.com.

Lucent Technologies.

Lucent Technologies designs and delivers the systems, services and software that drive next-generation communications networks. Backed by Bell Labs research and development, Lucent uses its strengths in mobility, optical, software, data and voice networking technologies, as well as services, to create new revenue-generating opportunities for its customers, while enabling them to quickly deploy and better manage their networks. Lucent's customer base includes communications service providers, governments and enterprises worldwide. For more information on Lucent Technologies, which has head-quarters in Murray Hill, N.J., USA.

www.lucent.com.

Sun Microsystems

Since its inception in 1982, a singular vision – "The Network Is The Computer" – has propelled Sun Microsystems, Inc. (Nasdaq: SUNW) to its position as a leading providerof industrial-strength hardware, software and services that make the Net work. Sun can be found in more than 100 countries and on the World Wide Web at

www.sun.com



Ulticom
Software Advancing Communications

linus

axalto

Sun
microsystems

telenor

høgskolen i oslo

Lucent Technologies
Bell Labs Innovations