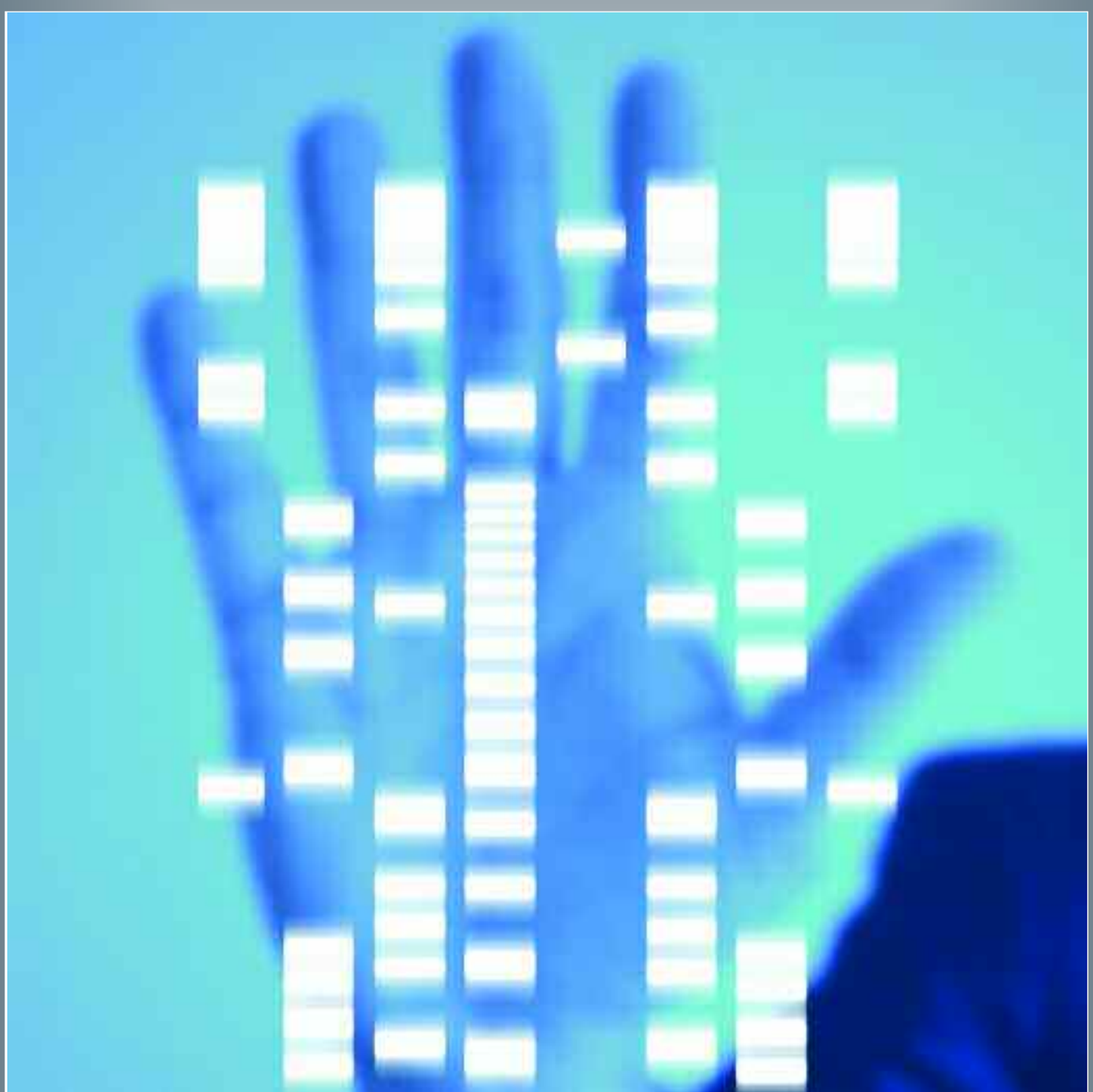
UNIFIED SIM STRONG AUTHENTICATION

for

CardSpace and Liberty Alliance



Simple, efficient and secure

strongSIM

FOR FURTHER INFORMATION PLEASE VISIT:
WWW.STRONGSIM.ORG

Index

gemalto telenor Sun microsystems høgskolen i oslo Ulticom Software Advancing Communications Lucent Technologies Bell Labs Innovations linus

Unified SIM strong authentication for CardSpace and Liberty Alliance

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

Dr. Do van Thanh, *Telenor*
Jean Daniel Aussel, *Gemalto*
Dr. Ivar Jørstad, *Ubisafe*
Do van Thuan, *Linus*
Dr. Tore Jønvik, *Oslo University College*
Lasse Andresen, *Sun Microsystems*

Executive Summary

This paper presents an innovative service called Unified SIM Strong Authentication that integrates both the Microsoft CardSpace and the Liberty Alliance Identity Management with the GSM SIM authentication. Telenor, Gemalto, Linus, Ubisafe and Oslo University College with the collaboration of SUN, Ulticom and Lucent have implemented a proof-of-concept of the service in Oslo. The goal is to demonstrate the feasibility of a convergent authentication service. The architecture is based on a multi-vendor environment where Sun provides the Identity Provider, Microsoft the Security Token Service (STS), 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 Web mail, company portal, or bank account, he/she logs on to the requested secured site simply by approving the authentication on his/her mobile phone.

This service is available anywhere and can support any Internet services no matter whether they are offered by a Liberty Alliance Service Provider or by a CardSpace Relying Party. The Unified 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).

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 the most useful information and services while keeping an acceptable level of security, users must remember more and more usernames and passwords. The number of username and password pairs continues 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 portals, corporate Intranet access, IP telephony, etc. Stronger authentications are required but, unfortunately, are usually both costly and not particularly user-friendly. There is clearly a need for more manageable identity management schemes and there are currently several activities in the computing community to find solutions for this issue. First, the Liberty Alliance [1] came up with a federated network identity solution that offers single sign-on enabling the user to visit several web sites without having to log in again. The other major solution is CardSpace from Microsoft which provides a user-friendly to manage multiple identities. Unfortunately, these solutions are not interoperable.

Telenor, Linus, Oslo University College, Ubisafe and Gemalto, in collaboration with Sun, Lucent Technologies and Ulticom, have designed and implemented a strong authentication service that integrates both the Microsoft CardSpace and the Liberty Alliance Identity Management. The idea is to integrate the current SIM authentication used in GSM with Liberty Alliance and CardSpace such that it can be used for Internet services. Indeed, this is a step further than 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 so common nowadays, and the GSM network is currently the largest mobile network and is ubiquitous in much of the world.

This paper presents the Unified SIM Strong Authentication Service for Liberty Alliance and CardSpace. It starts by summarising the state-of-the-art solutions for strong authentication and their limitations. Next, a short introduction of Liberty Alliance and CardSpace is given. An overview of our SIM Strong Authentication Service followed by a scenario showing how our SIM Strong Authentication Service works will be depicted. The value brought to users and service providers will be identified. The business opportunities for the mobile operators are also analysed.

Finally, the paper will explain 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 Authentication 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:

- User-friendliness: 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 a user's password by tricking them into giving their credential away to the wrong party): Keep asking gently for a password from a user, and at some point he will give it away. The most well-known methods for phishing user passwords are either to reproduce an almost identical login page to the one the user is used to, or to pretend 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 he 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 users will only remember from three to five logins/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 another using Single Sign-On, while warranting user privacy, and adequate level of authentication for the requested service and provider independence. However, while Liberty specifies how a service provider requests 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 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 do 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 gates 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 users with dynamic passwords they can use to log in. The users do not have to remember them, and there is no risk of compromised passwords since they are used only once. All users need is a mobile phone that is capable of receiving the password as an SMS message from 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 used 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. Introducing Liberty Alliance

The Liberty Alliance [1] uses the concept of network identity which refers to the global set of attributes that are contained in an individual's various accounts with different service providers. Currently the user's network identities are like isolated islands and the user is responsible for remembering numerous usernames and passwords for each of these identity islands. The user will typically either try to always use the same password or to record the password somewhere. Either way, the result is a drop in the level of security.

The most logical solution to the problem caused by the isolated network identity is to build bridges that interconnect them together and allow information flows between them. This is precisely what "Federation" is doing. Federation refers to the technologies that make identity and entitlements portable across autonomous policy domains. Consequently, the Federated Network Identity is a portable identity.

The establishment of federated relationships between service providers will hence allow the users to move more seamlessly from one service provider to another one. However, if every service provider has to make alliance to each of the other service providers it will be time consuming and require tremendous efforts. For n service providers, it requires n(n-1)/2 established relationships.

To circumvent this problem, the Liberty Alliance proposed a new role called Identity Provider. The Identity Provider assumes the management of the users Federated Network Identity and the user authentication.

A Circle of Trust is group of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment.

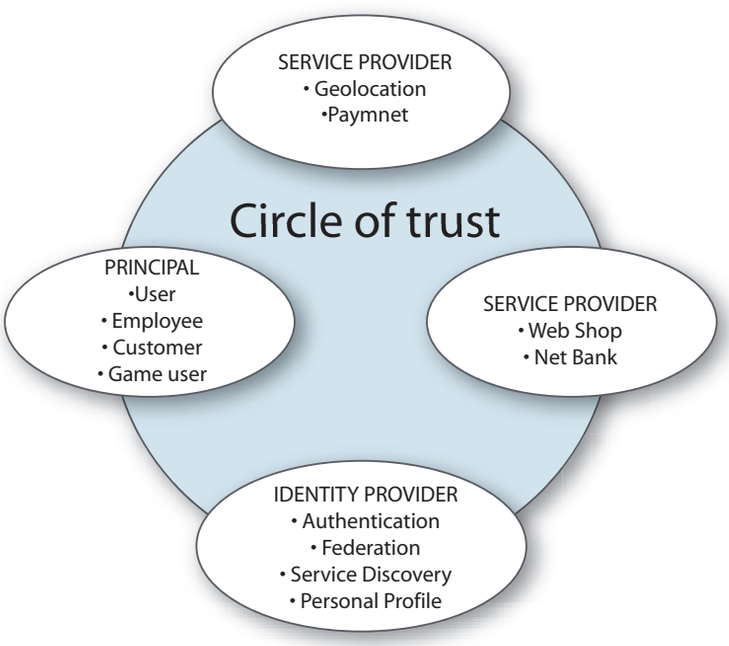


Figure 1
A Liberty Alliance Circle of Trust

Figure 1 shows a Circle of Trust. The Principal is the user, employer, customer, game user, etc. whose Federated Network Identity is managed by the Identity Provider. Once federation is done, the user can enjoy Single Sign-On. As shown in Figure 3, Joe has logged in at his IDP as JoeSelf. When visiting Yahoo.com, he is "automatically" logged in as BostonDude

4. Introducing CardSpace

CardSpace [2] is Microsoft's latest proposal for secure digital identities. CardSpace, originally code-named "InfoCard", lets any Windows application, including Microsoft's own applications such as the next release of Internet Explorer and those created by others, and its users a common way to work with digital identities. Part of the .NET Framework 3.0, CardSpace will be available for Windows Vista, Windows XP, and Windows Server 2003.

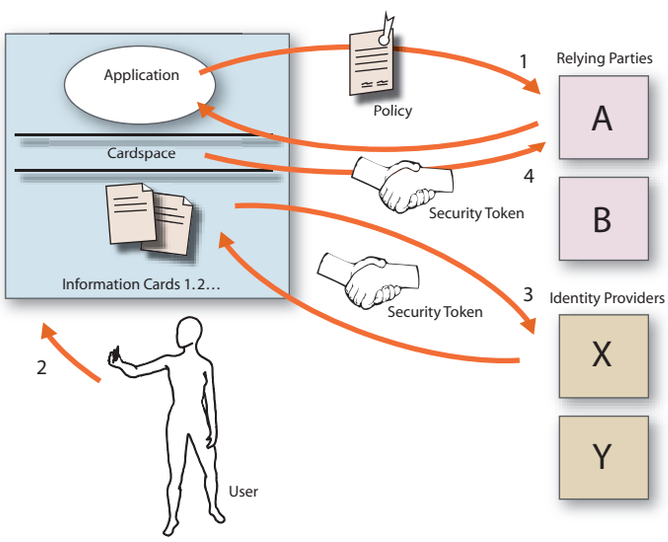
Figure 2
CardSpace and interaction among user, relying party and identity provider

1. First the application gets the security token requirements of the relying party that the user wishes.
This information is contained in the relying party´s policy, and it includes things such as what security token formats the relying part will accept, and exactly what claims those tokens must contain.

2. Once it has the details of the security token this relying party requires, the application passes this information to CardSpave.
CardSpace will then ask the user to select the desired digital identity by choosing an appropriate Information Card.

3. With the selected Information Card, CardSpace requests a security token from the identity provider.

4. When this security token has been received, CardSpaces gives it to the application, which passes it on to the relying party.
The relying party can then use this token to authenticate the user or for some other purpose



CardSpace provides the user with a consistent way to work with multiple digital identities, regardless of the kinds of security tokens they use. The user can create, use, and manage these diverse digital identities in an understandable and effective way. She might also be able to choose from a group of identity providers as the source of the digital identity she presents to the relying parties.

5. Our SIM Strong Authentication Service

A SIM-based strong authentication service that extends SIM card GSM authentication to Web services is proposed. It can briefly be described as follows:

- A user with a valid Telenor mobile subscription having a mobile phone with a SIM and SMS service may quite easily and securely log on to
- An Internet bank
- A corporate intranet
- A commerce web shop
- An Enterprise website
- An e-Government application
- At any time and anywhere in the world

The advantages of the SIM Strong Authentication Service can be summarised as follows:

- Removes the user's burden of remembering passwords by using the SIM card
- 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

The SIM strong authentication extends the usage of the EAP-SIM protocol [3] [4] [5] [6] in WLAN authentication to the Internet services.

6. Integration of Liberty Alliance and CardSpace

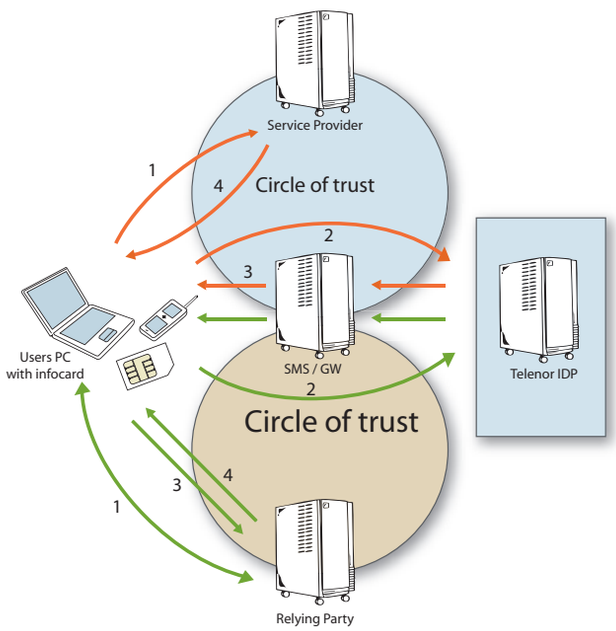


Figure 3
The Unified SIM strong authentication

The Unified Strong SIM authentication as its name says unifies the Liberty Alliance solution and the Microsoft's CardSpace and provides the user with the possibility to log in using both schemes.

When visiting a Service Provider belonging to the Telenor's Circle-of-trust the user will be redirected to the Telenor's Identity Provider for sign in. The user can use his mobile phone to authenticate himself. After successful authentication, the user is logged onto the Service Provider. After a while if the user visits another Service Provider belonging to the Telenor's Circle of Trust, he does not have to sign in again. Single Sign-on is provided.

Now, if the user visits a web site which does not belong to the Telenor Circle-of-trust but is a Relying Party, i.e. uses the Telenor's authentication service, he can use the Telenor ID card in CardSpace to do the authentication. Again, the authentication is carried out via his mobile phone.

To elucidate the Unified Strong SIM authentication service let us consider two cases:

6.1. Sign in to the Liberty Alliance Circle-of-Trust

As shown in Figure 3, the following actions are performed:

1. Kari connects her laptop on the Internet and is visiting a website e.g. myBank.com
2. When she attempts to log in, she is redirected to the Telenor Identity Provider website for authentication
3. The Telenor IDP performs authentication via SMS and Kari receives a message on her mobile phone. She approves the authentication.
4. Kari is now notified that her authentication is successful. The Telenor IDP redirects the browser back to myBank.com where Kari is now logged in and a Welcome page is displayed. Kari can carry out all her transactions
5. After a while Kari decides to go to her enterprise, e.g. myEnterprise.com. There she is immediately recognised and receives a welcome page. She enjoys the convenience of single sign-on.

6.2. Sign in with Card Space

1. Later, Kari goes and visits a web site, e.g. *https://sim10.nta.no/zivasrv,* which is a relying party of the Telenor's Identity Provider.

2. When she clicks on the log in button she is redirected back to CardSpace in her PC.
3. She selects the Telenor ID card. CardSpace requests the Telenor IDP to initiate authentication.
4. The Telenor IDP carries out the authentication via SMS and Kari receives a message on her mobile phone. She approves the authentication.
5. The authentication is successful. Kari is re-directed back to the Relying Party where a welcome page is displayed to her.

7. Unified SIM strong authentication implementation for Liberty Alliance and CardSpace

The architecture of the Unified SIM strong authentication is depicted in Figure 4. The heart of the system is the Telenor's Identity Provider (IDP). It is communicating with all the entities and supervising all the interactions:

- On the Internet side, it is able to communicate with
  - All the Liberty Alliance Service Providers that has joined the Telenor's Circle-of-Trust and provides the SIM strong authentication service to them
  - All the CardSpace Relying Parties that uses the Telenor's Identity Card and offers the SIM strong authentication service to them.
- On the mobile network side, it is able to communicate with
  - The SMS (Short Message Service) gateway to perform authentication using EAP-SIM protocol toward the users' mobile phones. More details about the EAP-SIM protocol is given in Annexe A.
  - The AAA (Radius) server [7] [8] that again is communicating with the Telenor's HLR (Home Location Register) via the MAP gateway to carry out the user's authentication.

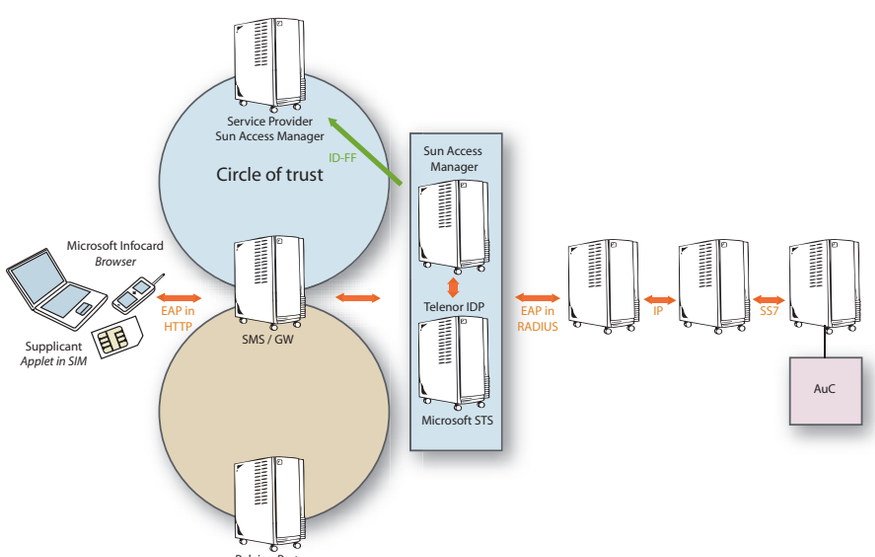


Figure 4 The Unified SIM Strong Authentication architecture

The Telenor's IDP consists of two main elements:

- A SUN Access Manager which is a Liberty Alliance compliant Identity Provider
- A Microsoft STS (Security Token Service)

Since the Unified SIM Strong Authentication Service is an extension of the SIM Strong Authentication [9], which is offered in a Liberty Alliance Circle-of-Trust with the SUN Access Manager as the main element, an interface has been introduced to bridge with the Microsoft's STS. In addition to management and information exchanges methods, this interface offers an Authentication request method that allows the STS to initiate the entire authentication based on the SIM card.

8. Value Proposition

8.1. To End Users

The Unified SIM Strong Authentication Service will deliver value to 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 an operating mobile phone with SIM card.

- Better protection and higher level of security: The Unified SIM Strong Authentication Service provides much better protection than passwords.

- Ease of use: The Unified SIM Strong Authentication Service is very simple to use and does not require any particular technical skill. The log in is 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 Unified SIM Strong Authentication Service. The availability of Single Sign-On access is time limited for security purposes.

- Universal applicability: The Unified SIM Strong Authentication Service can be used for any service or application.

- Global availability: The Unified 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 Unified SIM-based authentication can still be performed via Bluetooth.

8.2. To Service Providers and Relying Party

The Unified SIM Strong Authentication Service will bring the following benefits to service providers:

- Better protection and higher level of security: The Unified SIM strong and mutual authentication service provides higher protection of valuable assets and contributes to extending the availability of their services.

- Cost savings: By replacing their current password-based authentication schemes, service providers can save money on operation and maintenance costs due to the simplicity of the application

- Lower threshold for deployment: Service providers and Relying Partners do not have to invest large amounts of money to deploy the Unified SIM Strong Authentication Service because the mobile operator manages most of the infrastructure. No great technical expertise is required and the Unified SIM Strong Authentication Service fits very well for larger enterprises and SMEs.

- Simpler customer management: Service providers and Relying Parties do not have to take care of the password management since the mobile operators will assume this responsibility.

- Reach more customers: The Service Providers and Relying Parties may also reach new customers that are subscribers at the mobile operators.

8.3. To Mobile Operators

For mobile operators, the Unified SIM Strong Authentication Service will bring the following benefits:

- New source of revenue: The Unified SIM Strong Authentication Service constitutes an additional source of revenue for mobile operators which are not based on the sale of air traffic. This source of revenue has large potential since it brings value to end users and service providers.

- Reuse of existing infrastructure: Because the Unified 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 Unified 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 Unified 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 Unified 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 Unified SIM strong authentication is based on easily changeable software elements (Active-X supplicant, IDP Java Authenticator, VitalAAA 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.

9. Conclusion

Today, service providers have to choose between so many authentication and identity management schemes, and users are left struggling with a variety of digital identities. There are too many duplications and divergences in the digital identity world, and it must end. With the Unified SIM Strong Authentication Service, the mobile phone is indeed the point of convergence of CardSpace and Liberty Alliance identity frameworks. The user is offered the freedom and simplicity of participating and visiting all the web sites no matter whether they are a Liberty Alliance Service Provider or a Microsoft's Relying Party. In addition, high level of security and convenience is ensured via the usage of the mobile phone as a security token.

A proof-of-concept implementation of the Unified Strong Authentication has been completed by Telenor, Gemalto, Linus, Ubisafe and Oslo University College in collaboration with Sun, Lucent Technologies and Ulticom. A demonstration of the service was shown at the 3GSM World Congress in Barcelona, Spain, February 2007.

Annex A

EAP-SIM

EAP-SIM is a recognized EAP (Extensible Authentication Protocol) Type and is defined in IETF RFC4186. 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 re-authentication procedure.

Authentication Example

Figure 5
EAP SIM Authentication

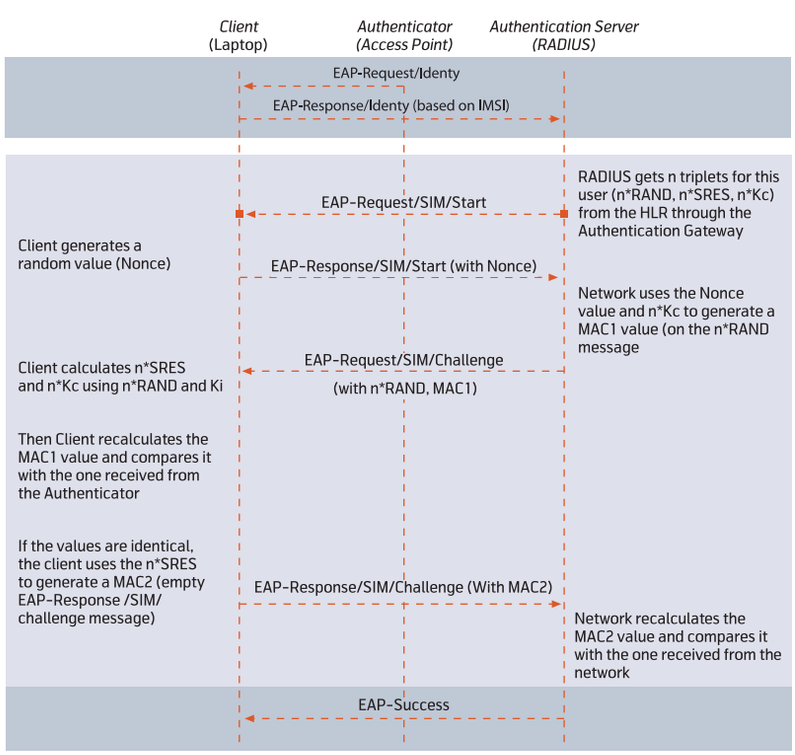


Figure 5 shows an example of EAP-SIM full authentication. Authentication is started with a request for client identification. The software process on the client platform that performs the EAP-SIM negotiation is called the supplicant. The supplicant's response includes either the user's International 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 also be 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 can 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.

Once the supplicant has received this challenge, it will run the GSM algorithm to obtain the GSM triplets, and 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.

Reference

[1] Liberty Alliance	The Liberty Alliance Project - http://www.projectliberty.org/
[2] CardSpace	Microsoft's CardSpace - http://cardspace.netfx3.com/
[3] EAP SIM	EAP SIM - draft-haverinen-pppext-eap-sim-16.txt- IETF
[4] EAP AKA	EAP AKA - draft-arkko-pppext-eap-aka-15.txt - IETF
[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
[9] SIM strong	Offering SIM strong authentication to Internet Services – http://www.simsgtrong.org

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

STS

Security Token Service

Partners

StrongSIM.org

This white paper has been written by the founding members of the SIM Strong Authentication Task Force. For more information or details on how to join, visit http://www.StrongSIM.org.

Telenor

Telenor is one of the largest mobile operators worldwide with ownership interests in 12 mobile operators across Europe and Asia, constituting a total subscriber base of 82.7 million at year-end 2005. Telenor is Norway's largest telecommunications company and one of the fastest growing providers of mobile communications services worldwide. Telenor is also the largest provider of TV services in the Nordic region. In 2005, 57% of the Group's revenues were derived from the mobile operations. Telenor has mobile operations in some of the world's fastest growing markets, and the home market, Norway, is one of the most advanced in the world today. Group revenues for 2005 reached NOK 68.9 billion - a growth of 14 per cent compared to 2004. At year-end 2005, Telenor employed 27,600 people (man-years) - 16,700 of whom were employed outside Norway.

www.telenor.com

Gemalto

Formed in June 2006 by the combination of Axalto and Gemplus, Gemalto is the world's leading provider of microprocessor cards and a major supplier of point-of-sale terminals. Gemalto'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 $2.2 billion in combined pro-forma 2005 revenue. Its 11,000 employees come from over 85 different countries and serve customers in more than 100 throughout the world.

www.gemalto.com

Linus

Linus, a small consultant and system house located in Oslo, Norway. The company provides SW development services to major player in the Norwegian Oil & Gas and Telecommunication business segments.

www.linus.no

Ubisafe

Ubisafe, a Norwegian SME based in Lillehammer and specializing in Internet security solutions based on the mobile phone and the SIM card. For more information, visit

www.ubisafe.no

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-essential signalling 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 http://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 headquarters 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. to its position as a leading provider of 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 http://www.sun.com.

strongSIM

Unified SIM strong authentication for CardSpace and Liberty Alliance

Whitepaper rev. 2.4 Feb 2007

Simple, efficient and secure

FOR FURTHER INFORMATION PLEASE VISIT:
WWW.STRONGSIM.ORG

UbiSafe Ulticom Software Advancing Communications linus gemalto Sun microsystems telenor høgskolen i oslo Lucent Technologies Bell Labs Innovations