Offering SIM strong authentication in a Liberty Alliance Circle of Trust

Dr. Do van Thanh
Telenor R&I
Dr. Tore Jønvik
Oslo University College
Fidelity objectives

- To set up 4 Circles of Trust and to manage identities in this pan-European context
- To demonstrate the inter-operability of the Liberty approach
- To evaluate the technical and some socio-economic aspects of the demonstration
- To make standardisation and implementation contributions
FIDELITY-PROJECT: 4 COTs

- Norway Circle of Trust
  - Norwegian Internet provider
  - Norwegian Attribute providers
  - Finnish Internet provider IDP/DS
  - Finnish Attribute providers
  - Spanish Internet provider IDP/DS
  - Spanish Attribute providers
  - French Service providers
  - Norwegian Service provider
  - Liberty Alliance protocols

- Finland Circle of Trust
  - Finnish Internet provider IDP/DS
  - Finnish Attribute providers
  - Spanish Service providers

- France Circle of Trust
  - French Internet provider IDP/DS
  - French Attribute providers
  - Spanish Internet provider IDP/DS
  - Spanish Attribute providers

- Spain Circle of Trust
  - Spanish Service providers
Roaming between Circles of Trust
Identity Management is getting more and more important
Identity Provider based on the Liberty Alliance concepts regarding:
- Technology
- Business:
  - How to establish a Circle-of-Trust
  - Which services are compelling to Service Providers and users?

The SIM Strong Authentication Service
Limitation of current authentication solutions

- Single password is not strong enough
- Expensive for the service provider to introduce stronger authentication
- One-time password requires a password calculator.
- A wallet (secure client) must be installed in the user’s PC
Limitation of current authentication solutions

- Alternatively, smart cards can be used.
- Smart cards are tampered resistant devices that can be used to store the encryption keys and the credentials of the user.
- They can be equipped with encryption/decryption functions.
- However, they introduce cost at deployment time and for management.
  - Inconvenient for the users:
    - many cards that fill the wallet
    - many pin codes to remember.
Our SIM strong authentication service

- 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 GPRS/3G PC card (with a SIM) installed on the PC
  - A card reader (with a SIM) installed in 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.
Components of the SIM strong authentication service

Supplicant or peer
ActiveX in the PC browser

Identity Provider Sun Access Manager
Authenticator Servlet in IDP

Service Provider
Sun Access Manager

AAA Server
RADIUS

Gateway
SS7/IP

HLR

AUC

SS7/IP

ID-FF
EAP in HTTP
EAP in RADIUS
IP
SS7

Circle of Trust

oslo university college

www.hio.no
How does SIM strong authentication service work?

1. Kari connects her laptop on the Internet and is visiting the myBank.no website.
How does SIM strong authentication service work?

2. When she attempts to log in she is redirected to the Telenor Identity Provider web site
How does SIM strong authentication service work?

4. Kari clicks on the “Smartcard logon” button. She is then asked to do one of the following in order for the PC middleware to access the handset SIM card:
   a. Insert the SIM card in the card reader
   b. Plug the USB dongle or integrating the SIM card
   c. Connect the PC to the phone using Bluetooth or a data cable
How does SIM strong authentication service work?

4. The Telenor IDP Sun Access Manager will request the Lucent Vital AAA server to start the EAP-SIM authentication towards the SIM card:
   - Via the Ulticom MAP gateway, the Lucent VitalAAA will request the GSM tripplet (RAND, SRES, Kc) that is used in the authentication.
   - The random number RAND is conveyed to SIM card that returns a XRES.
   - If XRES is equal to SRES the authentication is successful.

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.
1. Kari connects her laptop on the Internet and is visiting the myBank.no web site.

How does SIM strong authentication service work?
How does SIM strong authentication service work?

6. 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.
Values to the users

- Simple and better control and management of their identities:
- Better protection and higher level of security
- Ease of use
- Single-sign-on
- Universal applicability
- Global availability
Values to the Service Providers

- Better protection and higher level of security
- Cost saving
- Lower threshold for deployment
- Simpler customer management
- Reach more customers
Values to the Mobile Operators

- New source of revenues
- Reuse of existing infrastructure
- Improved customer loyalty
- New business customers
- Strengthened position
- Easy adaptability for the future
Conclusion

- The SIM strong authentication service will most likely be a successful service in the near future by
  - usage simplicity
  - high level of security
  - universal applicability
  - cost efficiency
• A proof-of-concept implementation has been completed by Telenor, Gemalto, Linus 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 2006.