Offering SIM strong authentication in a Liberty Alliance Circle of Trust

Dr. Do van Thanh

Barcelona
13-16 February
2006

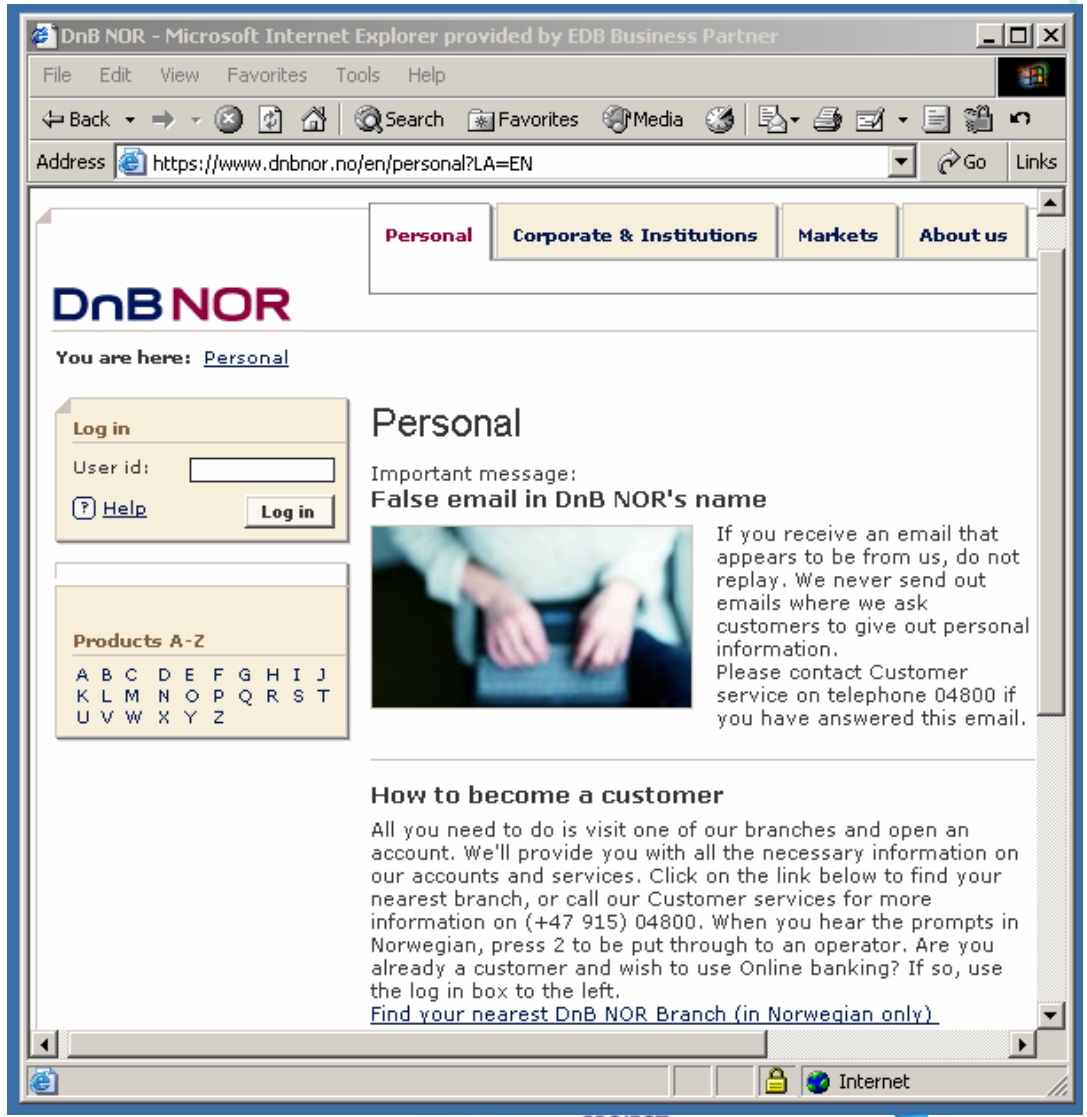
Introduction

- Telenor wants to explore new businesses and new roles than the traditional telecommunication.
- Identity Management is getting more and more important
- Telenor wants to experiment the role of 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

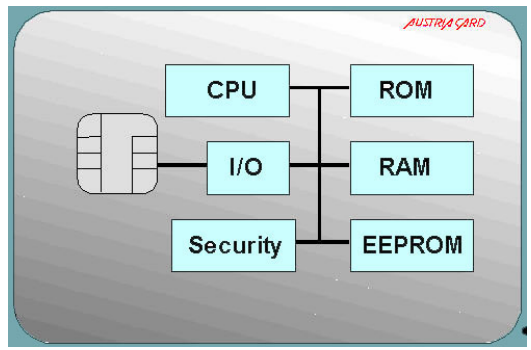
Limitation of current authentication solutions

- Single password is not strong enough
- It is expensive for the service provider to introduce stronger authentication
- For ex. Using one-time password as the bank DnBNOR will require a password calculator.
- Alternatively, 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
- Unconvenient for the users
  - many cards that fill the wallet
  - many pin codes to remember



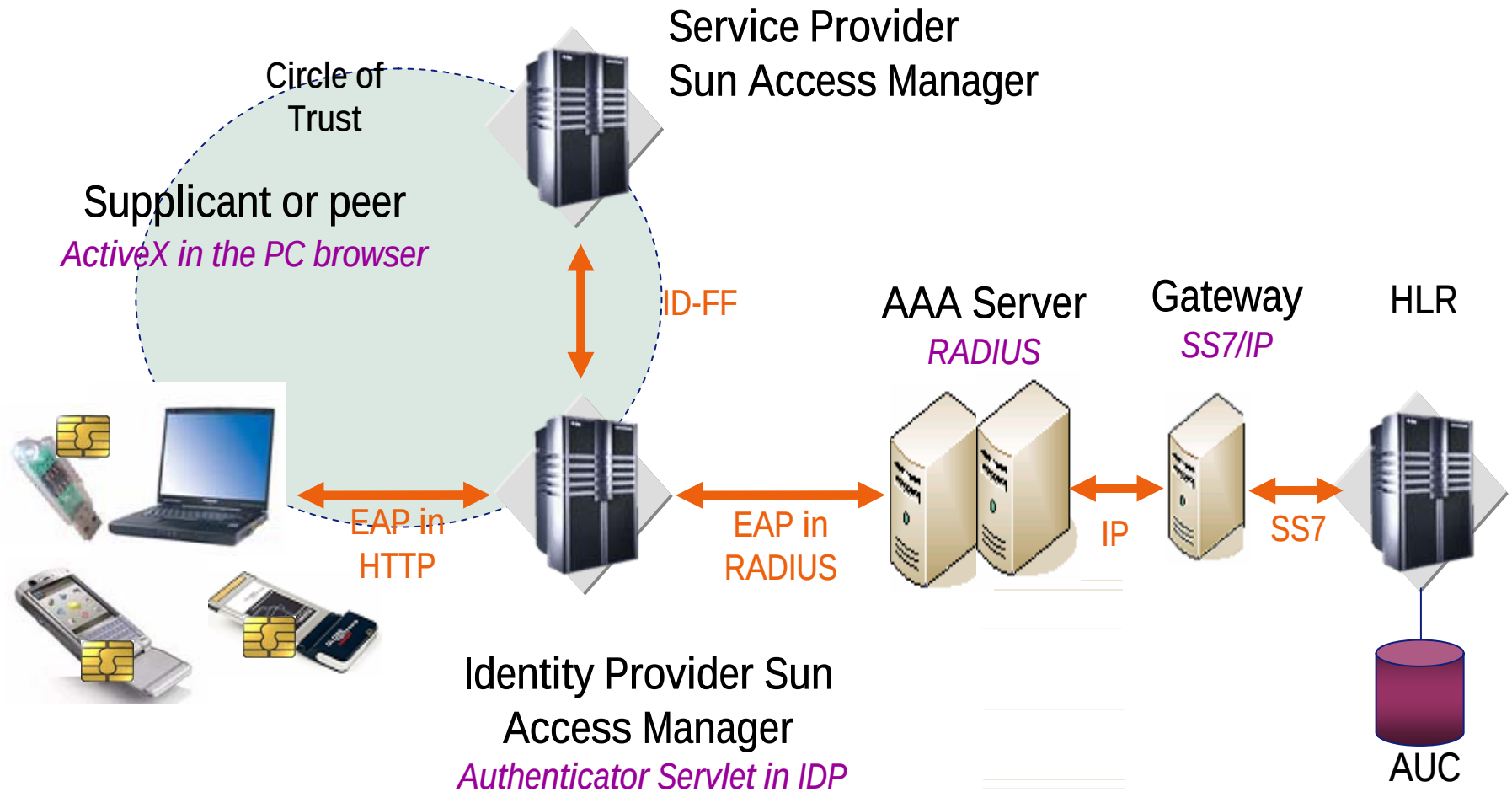
Our SIM strong authentication service

- 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 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

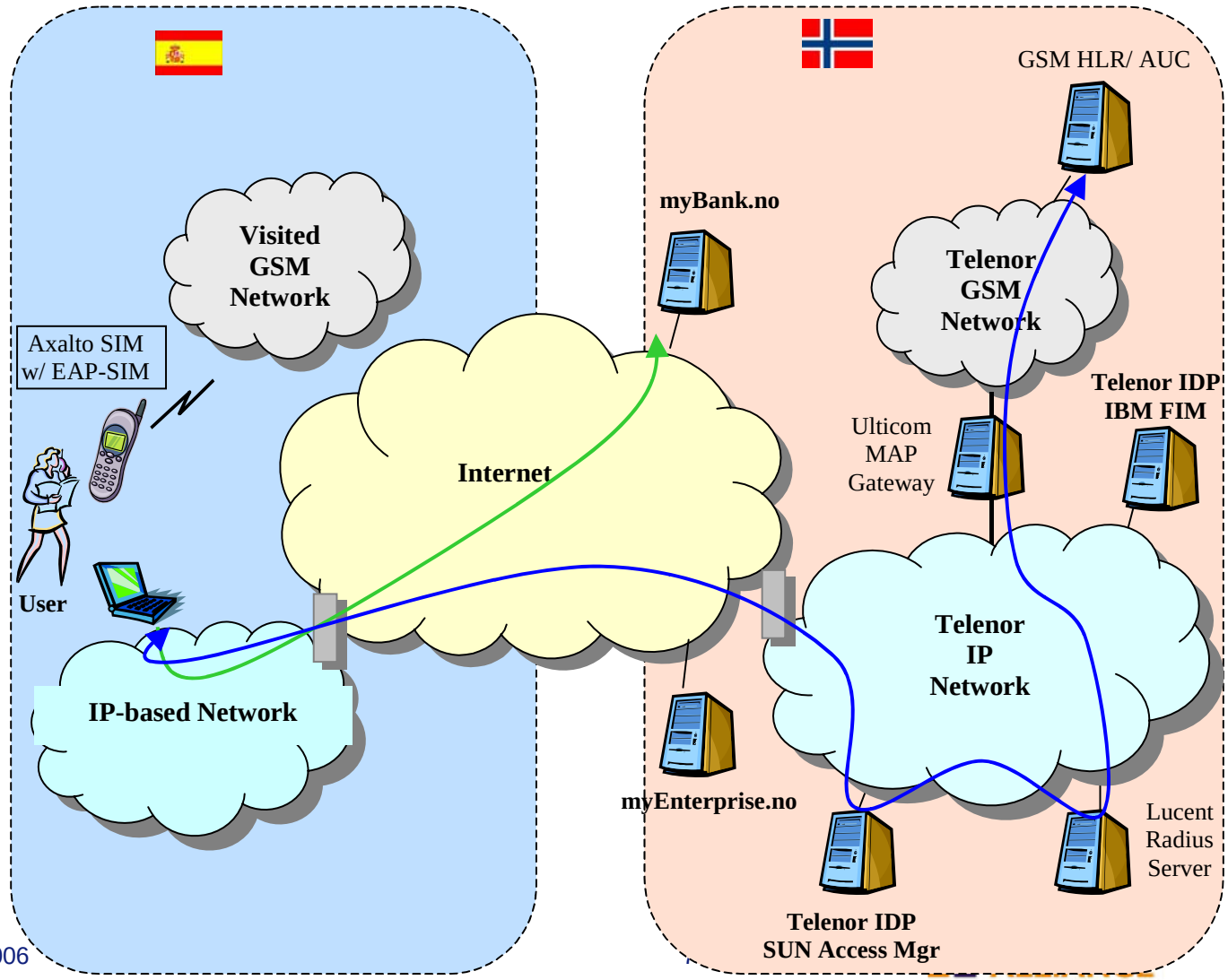
  At anytime and anywhere in the world.

- 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 Signalware** SS7/IP MAP Authentication Gateway.

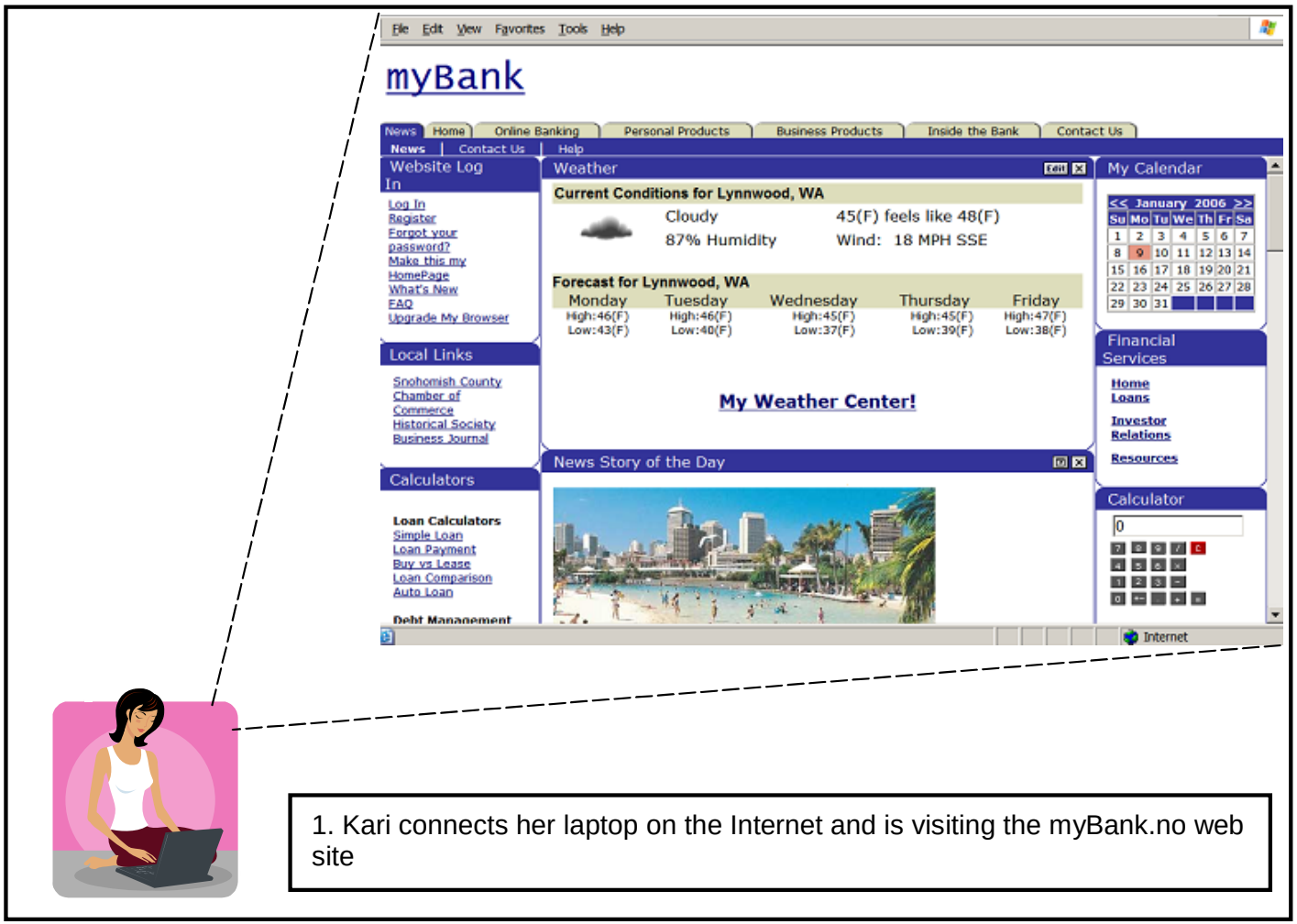
Components of the SIM strong authentication service



The proof-of-concept demonstrated in Barcelona

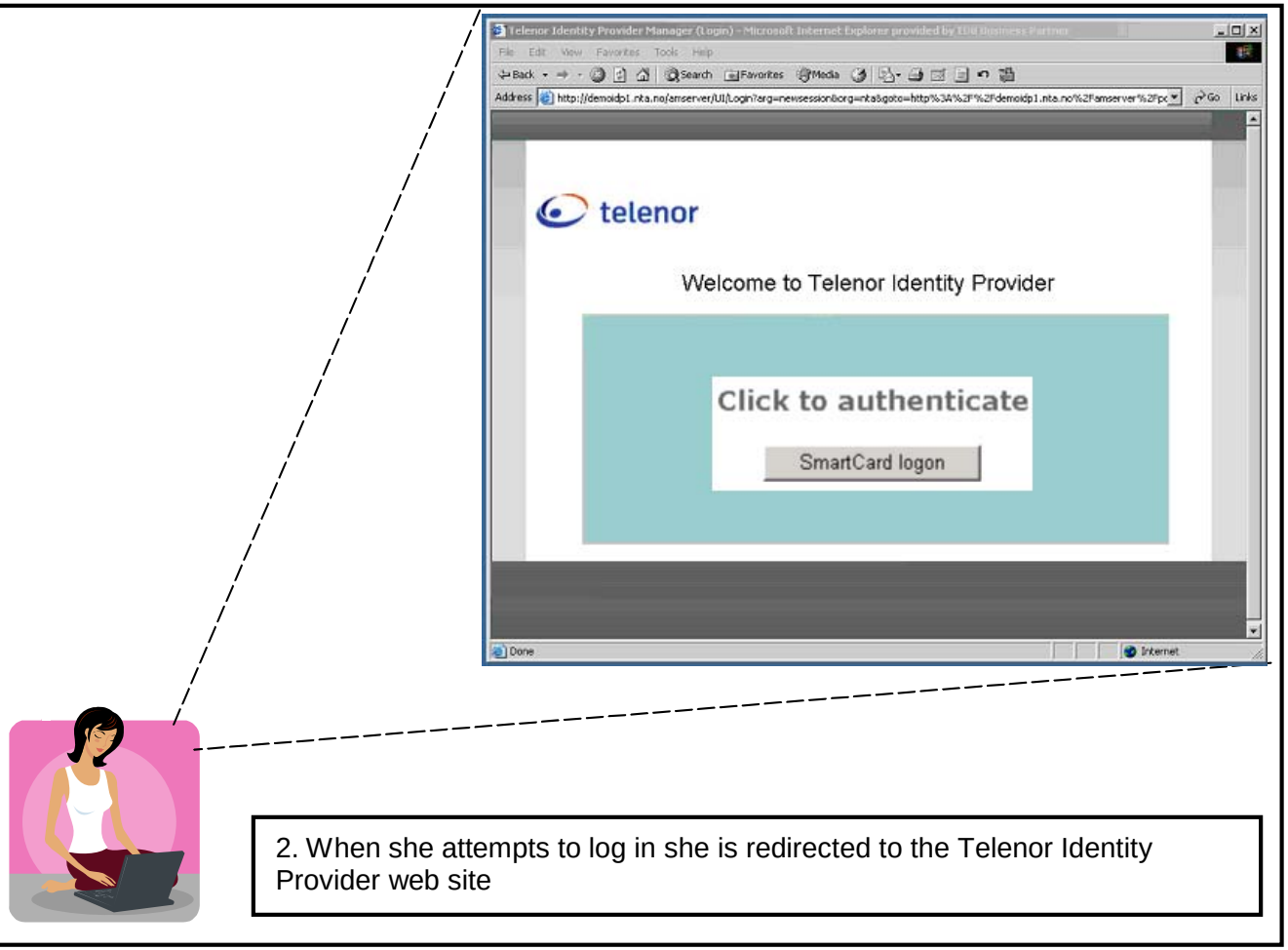


How does SIM strong authentication service work?



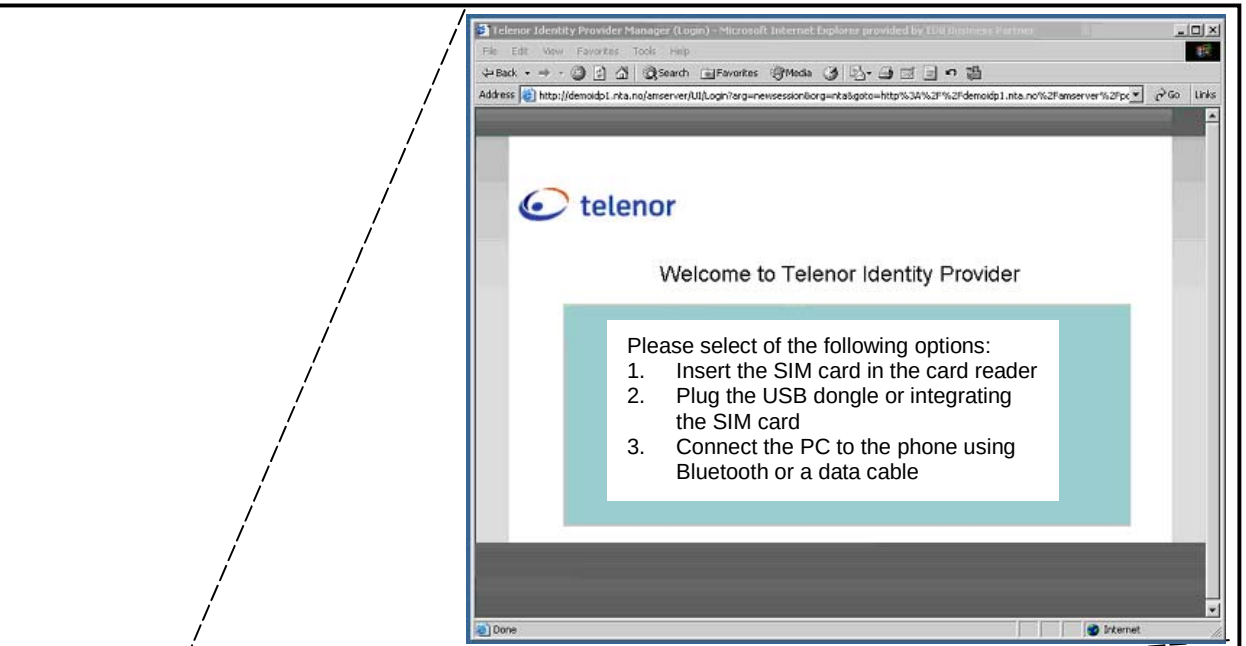
1. Kari connects her laptop on the Internet and is visiting the myBank.no web site

How does SIM strong authentication service work?

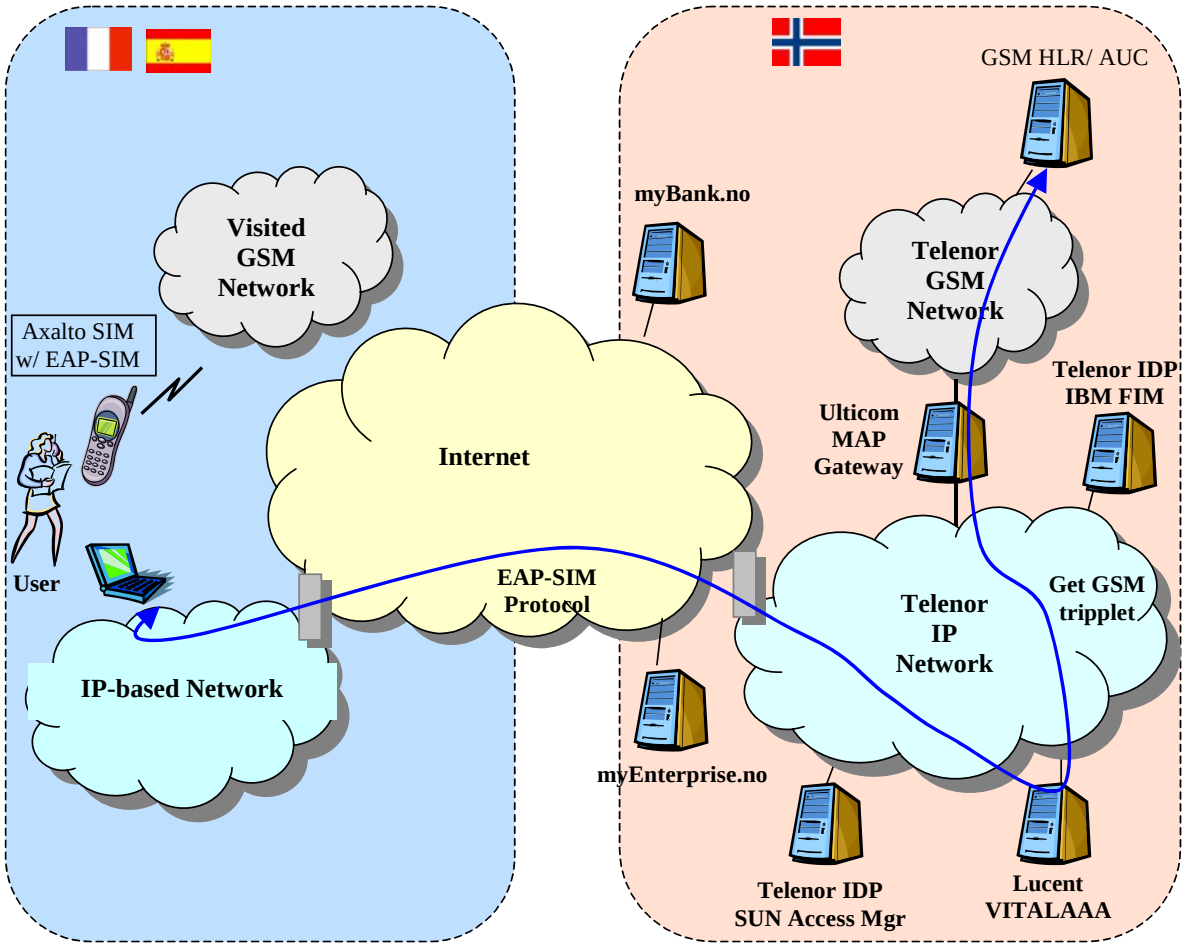


2. When she attempts to log in she is redirected to the Telenor Identity Provider web site

How does SIM strong authentication service work?



How does SIM strong authentication service work?

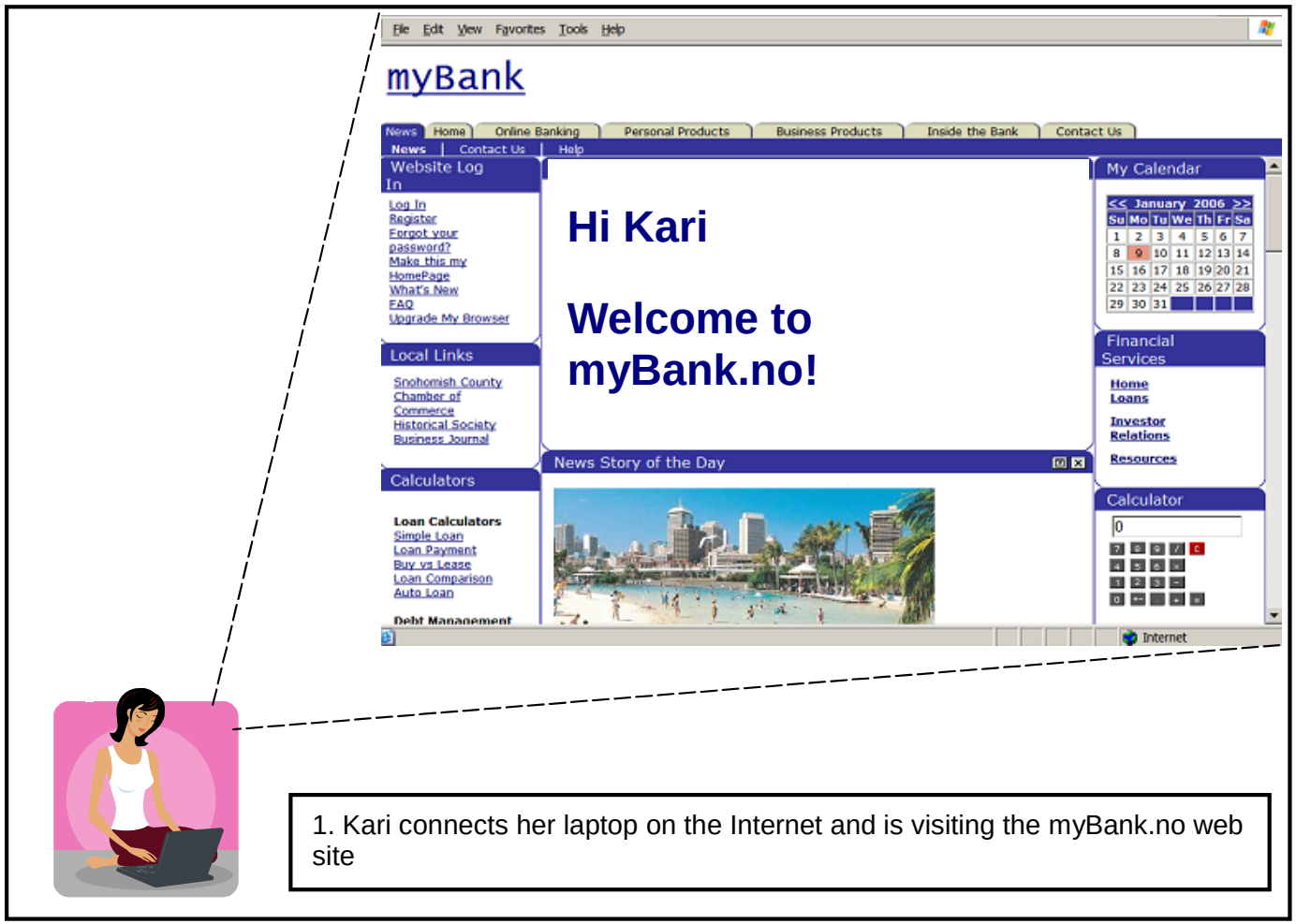


4. The Telenor IDP Sun Access Manager will request the Lucent Vital AAA server to start the EAP-SIM authentication towards the SIM card:
   - Via the Ulticom MAP gateway, The Lucent VitalAAA will request the GSM tripplet (RAND, SRES, Kc) that is used in the authentication.
   - The random number RAND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

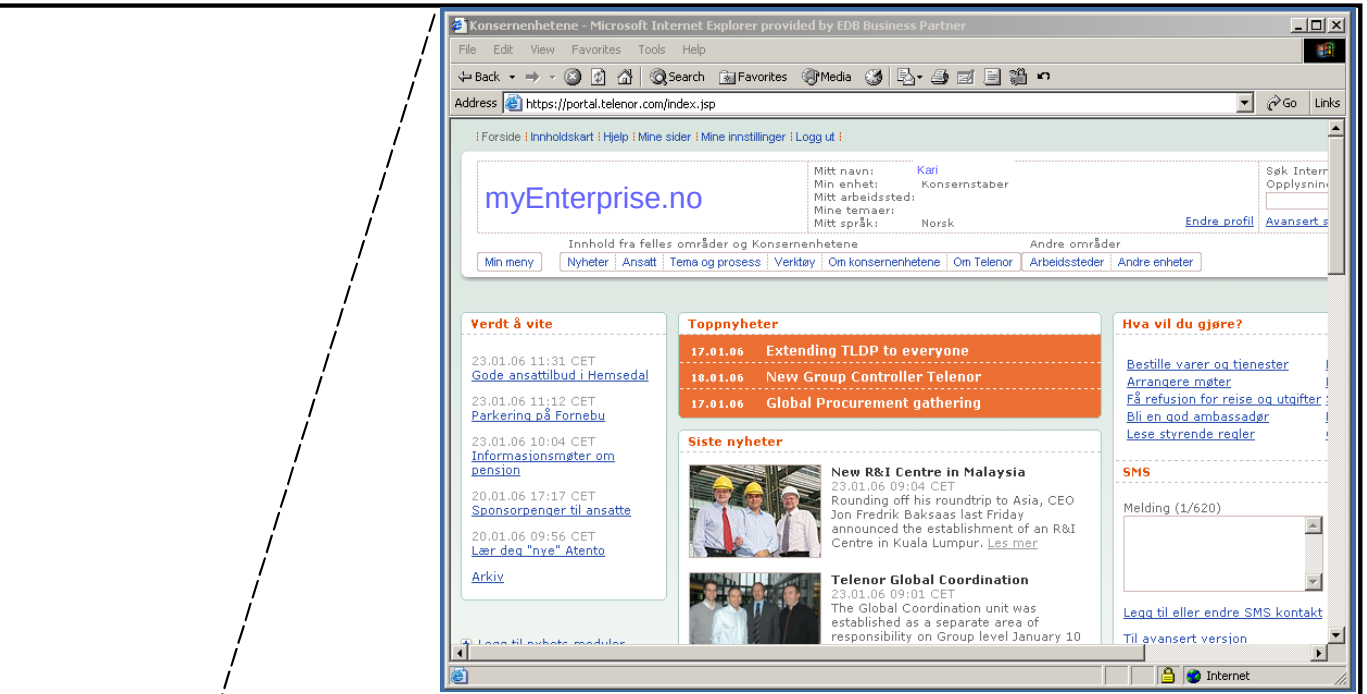
Depending on the security settings Kari has established for her SIM card, she may be asked to enter her EAP-SIM card application PIN code to allow the mutual authentication to be performed

telenor

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 by
  - Its usage simplicity
  - Its high level of security,
  - Its universal applicability
  - Its cost efficiency,

will most likely be a successful service in the near future.

- Next, we will explore the delegation of authentication between two CoT, i.e. two IDPs.
- 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.