Electronic Identity

Efforts to Establish Electronic Identities in Sweden

See http://www.umu.se/it/personal/tvw/pub/

Torbjörn Wiberg
CIO, Umeå University

Electronic Identity

- eGovernment, eBusiness, eLearning, eEurope all require that you have an electronic identity
  - you have to be able to show to the system that you are you - the system has to be able to **authenticate** you
  - you show this by "presenting" your Electronic Identity to the system
- Electronic identities are needed to develop the Information Society
- Who shall issue them and how strong do they need to be?

Electronic Identity?

- The electronic Identity is either a Username/Password or a pair of crypto keys for Public Key Cryptography
  - You normally **choose** your electronic **identity** yourself
  - By some means the electronic identity shall be bound to the person
- Electronic Identities are not foolproof
  - How high is the risk that a particular electronic identity has been compromised? (With the obvious consequence that someone can be pretending to be you)
  - Depending on the estimated risk – what functions in an application should be available to a user with such an identity

Increased Self-Service and Electronic Workflow

- Two general trends can be observed:
  - there is an increase in Self-Service in our IT Applications
  - non-specialist users are active in electronic workflow
- These trend tends to make all our students and/or all our personnel (non-specialist) users of more and more of our systems
  - Tur och Retur (travel expenses)
  - Ladok på webb (student records)
  - Personal portals
- These systems are examples of systems where we need electronic identities
  - Irrational to have to maintain user accounts on each system
- Many of these applications are provided as Web Services

The Strength of the Electronic Identity

- The strength of the electronic identity depends on
  - the routines and methods used by the application for managing "account" (meta) information
  - the means and routines of binding the electronic identity to the individual
  - the mechanism used in the authentication process to present the credentials for the electronic identity to the system (tunnels?)
  - the measures undertaken to avoid that the secret component of the identity is compromised/stolen (how is it stored)
- These are a mix of manual routines and automated procedures

Binding an Identity to Its Owner in the Public Key Approach

- In Public Key systems, the binding is done when the user registers her public key with the application or with a trusted Certificate Authority (CA)
  - In the binding process the user proves that she is in possession of the private key by encrypting something that can be decrypted and checked by the application or the CA
  - Another step of the binding process is to establish the identity of the possessor of the key pair. Usually this means
    - binding the key pair to an email address through an email exchange or
    - binding the key pair to an individual by means of for ex an ID card
  - If a CA is involved, it issues a certificate which contain the public key, the identity and it states the nature of the binding

Binding an Identity to Its Owner in the Username/Password Approach

- A Username/Password is bound to an entity when they are registered with the application. Some alternatives ordered in increasing strength:
  - The Username/Password is communicated to the application/user in an eMail exchange
  - The Username/Password is submitted encrypted through a web form and confirmed in an eMail exchange
  - The Username/Password is sent in a letter or delivered personally
- We should configure our systems to require a higher authentication strength for more sensitive operations

Electronic Identity
Elektronic Identities in a PKI

- The PKI is responsible for binding the electronic identity to its owner
- In a PKI, certificates of public keys are stored and distributed together with lists of revoked identity certificates
- In order to trust the identity you have to trust the PKI
- Trust has to be earned
- It is partly done by the PKI stating its policy (Certificate Policy) and its working procedures (Certificate Practices Statement)
  - The CP also includes requirements on the user
  - For example on how the private key shall be protected

How Can an Electronic Identity Be Used? – For Authentication

- It can be used to **authenticate**
  - you (to systems)
  - documents or messages you have digitally signed (PKI based eID)
  - systems, you are responsible for, to its users (PKI based eID)
- **Authenticate** – establish the originality of
- **Non-repudiation** – A process or method that ensures that once you have signed a document or identified yourself to a system you can't deny that (PKI based eID)
- **Authentication** – can be realised as a middleware service
  - Requires a PKI and/or a Username/Password database
  - Implemented as a server or plug-in

Electronic Identity
The Role of the Government

- I believe that we shall
  - strive for electronic identities based on Public Key Cryptography
  - be satisfied if the private key is stored in a file (not require "smart cards")
  - require that the government takes responsibility for the organisation of a national PKI for citizens
  - require that this PKI shall be suitable for frequent use of electronic identitie
- This still means that we need additional PKIs for specific needs within organisations
- Note that private keys MAY be stored in a smart card

Electronic Identity
With the PKI in Place We Can ...

- Bind user accounts and authorisation attributes to the electronic identity in our Enterprise Directories
- Offer Authentication and Authorisation (SPOCP) to our systems as middleware services
- Also authenticate potential students

Arriving at this position has been a process

- In 99 I believed we would organise it ourselves
  - I ran a project to establish a PKI for Swedish higher ed – Swupki
- I realised that this is better done once for citizens
  - We took part of the task assigned by the government to the tax authorities to make citizens' certificates available for eGovernment purpose
- Just to realize that there are different views of eGovernment
  - The resulting business model is based on the assumption that an identity is used infrequently but by many authorities
    - We need to use it frequently
  - The procurement was done for file stored certificates since people were assumed to sit at home filling in their tax forms
    - It upset me a lot, but now there are USB memories

Swupki has its role

- It is running since feb -01
- It is used mainly for server certificates
- It is a club with 5 members (out of around 40, which is a disappointment)
- Some of us will act as certificate service providers (CPS) to the others
  - A certificate practice statement (CPS) has to be written by each member
  - It has to become easier
  - It can be based on the CPS of the CSP
  - Local handling of requests the only original material

Where Do We Stand Today?

- There is a citizens' certificate we can't afford to use
- The universities has made the government aware of the fact that the tax authorities have not solved our problem
- It will probably be a new procurement within the next year and we will try to make sure that the result suit us better

Will the PKI Technology Take Off?

- I believe so
- I have received more inquiries from system owners and potential members of Swupki the last three months than the previous two years
- We get requests for person certificates for specialist users that want to sign things
- The reports on experiments indicates that browsers handle certificate issues a lot better than say a year ago
- Interoperability between cards and readers are improved
- We need to be able to use Authentication and Authorisation services in our systems

Some web addresses

- www.umu.se/it/personal/tvw/pub
- www.swupki.su.se
- www.umu.se/it/projupp/spocp

Efforts to Establish Electronic Identities in Sweden

See http://www.umu.se/it/personal/tvw/pub/

Torbjörn Wiberg
CIO, Umeå University