Norway Post’s Electronic ID Case study on authentication

Oslo 17. June 1999
Terje Kolnes, Norway Post
Presentation Objective

- The Norway Post “National” electronic ID, The enabler for e-Commerce
- Global Postal Trust Services, Universal Postal Union - UPU
- Case study from Norway Post, On-line Government, Tax reports
Norway Post, IT position today

- Among the 5-6 largest IT companies in Norway - the largest IT supplier of computer service to the governmental sector: the leading within electronic services, infrastructure services and business services.

- 8% of Norway Post revenues from IT-Business
Why an electronic ID?

- Today, there are many types of cards with ID’s for many different purposes, and with different levels of security.
- An electronic ID is a prerequisite for many of the new electronic services.
Norway Posts role

- The Post’s strong position is to be a neutral and trusted means of communication between parties, and is an issuer of a visual identity card.

- The Norway Post has launched a smart card initiative in Norway, opening for co-operation with other major Norwegian parties.
Trusted Third Party

- Digital keys for identification are necessary for transactions - and transport of documents in open networks

- The Norway Post goal is to capture the position as Norway's most central and used TTP:
  - Norway Post has a reputation for its continued reliability as a genuine TTP for 350 years.
  - Will be the central distributor of Smart card solutions.
Content of an electronic ID

- Secure identification
- Digital signature
- Protected communication
- “Role” management
- Local PIN-verification
- Picture and signature
- Visual identity card
- Application Programming Interfaces (on the card and as a toolkit for applications)
Areas of use

- Secure logon to electronic networks
- Secure identification towards web-based “self-service” applications
- Secure electronic mail
- Digital signature on electronic documents/transactions
- Electronic/visual identification incl. picture
- Roles for ”add on” applications
  - Health cards
  - General election identification
  - Drivers licence
Norway Post translates, secures and distributes formal EDI-documents via an EDI-central and has a high market share within this area. Norway Post assumes this market will increase through:

- General increase in electronic reporting to official authorities
- Increased use of formal trade documents and payment transactions
- Stronger integration between EDI services, TTP services and use of internet technology
- Improved trust and security and reduced costs for e-commerce
Norway Post has launched a smart card solution called MultiSmart. The solution is based on a multi application smart card running the MULTOS operating system. Two basic applications are electronic ID (eID) and electronic cash - MONDEX. The electronic ID and MONDEX activities have a high priority in Norway Post.
Current situation

- Smartcards in use today usually have one single purpose (GSM, access, memory cards like telephone cards, ...)
- Smartcards are more expensive
- Terminal equipment for smartcards are cheaper then for other cards
- Security is better with smartcards - enabling “local” transactions without an online connection
- Current infrastructure does not support smartcards
What has to be done?

- Create accept for a common technologic platform enabling one dominant infrastructure
- Co-operation between the large players in the Norwegian market
- Base development on standards and solutions with an international basis
- Use of a multi-application card which increases the user value of the card
- Implement “enabling” applications in the market
- Establish a critical mass
Application layers

Market generated revenue

Value added Applications

Service Applications

Basic Applications

New

Electronic Infrastructure

Existing

Infrastructure

Revenue from public funding

ID with keys and certificates

Electronic purse

Payment

Communications

Logistics

Debit & credit

Loyalty

Pay pr view

Health

Insurance
# Norway Post MultiSmart Applications

<table>
<thead>
<tr>
<th>Electronic ID</th>
<th>Debit card</th>
<th>”Role”-card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash purse</td>
<td>Credit card</td>
<td>Access card</td>
</tr>
<tr>
<td>Gas card</td>
<td>Electronic ticketing</td>
<td>Health card</td>
</tr>
<tr>
<td></td>
<td>Season tickets</td>
<td>Loyalty card</td>
</tr>
</tbody>
</table>

**MULTOS** – Operating system

Silicone (hardware)
Primary interest of the Norway Post

- Maintain the role as a “trusted third party” (TTP) in the secure communication between parties. This is the Post’s historic role
- Issue and administrate a “national” electronic ID
- Participate in an international “Post-based” co-operation - Universal Postal Union
- Create new areas for growth in Norway Post
Universal Postal Union

- Establishing Global Postal Trust Services
Joint Electronic Commerce Services

- UPU role and Objective: To facilitate the establishment of global Postal Electronic Commerce Infrastructures and ensuring the compatibility between Postal systems.

- Trust services are the major foundation of e-Commerce
Working Group Participants

- Global Postal Trust Services Project, using PKI technologies and Cross Border Cross Certification Services.

- Australia, Belgium, Canada, Finland, France, Germany, Hong Kong, Indonesia, Ireland, Italy, Netherlands, Norway, Portugal, Singapore, Sweden, UK and USA

- In the process of joining:
  - Japan, Spain and Malaysia
Global Post Trust Service Business Driver

- Traditional mechanisms used to identify and authenticate documents (such as handwritten signature on paper, Post Mark, and Post Stamp) are not available for authenticating computer-based records and transactions.

- Communications tools, such as telephone, facsimile, and PC (electronic mail and EDI) still lack reliability, integrity, and security.

- The solution to this problem is a Digital Certification service utilizing Public Key Infrastructure and Certification Authorities acting as trusted third parties.
Definition of the Solution

- **Digital Certification service**
  - A service by a body, that is entrusted domestically, who guarantees that the identity of its customers is true and have been verified. The guarantee is provided in the form of a “certificate” - a signed digital file

- **Public Key Infrastructure**
  - A secure database of “keys”. Each individual is given a key pair unique to him that he can use electronically to identify himself
Definition of the Solution cont..

- Certification Authorities - Trusted Third Parties
  - A trusted entity that verifies the identity of individuals and issues a “certificate” that guarantees the identity of the person and binds him to his unique key
  - Therefore providing digital certification services. The certificate is also made publicly available in directories so that whoever exchanges electronic correspondence with you is guaranteed, by the Post, that you are who you say you are
The need for International Coordination

- Domestically many posts are offering certification services but since electronic commerce is not a domestic business, Certification services have to be offered on a global basis.

- Therefore, internationally there is a need for a trusted entity to harmonise and regulate the policies and procedures enabling Posts to form a global postal trusted network.
The need for International Coordination

- Developing this infrastructure required international cooperation between posts and the UPU to facilitate such cooperation through the Advanced Electronic Services user group of the Telematics Cooperative.

- Aim of this group is to enable posts to provide certification services on a global basis, thus positioning the Posts as a recognized Trusted Third Party in Electronic Commerce enabling them to introduce value added postal applications.
UPU Background

- The Project started in March 1997 with 14 posts. Additional posts have joined since then, now totally 18
- Work is conducted on the basis of short phases with clear objectives
- Posts with installed systems are utilizing their existing infrastructure as a test bed
- Project development of the basic infrastructure is now completed, administratively in September 99 (UPU Congress endorsement)
Business & Project Objectives

- **Business Objective**
  - We are in the business of binding identities of individuals and organizations with public keys through the issuance and management of certificates

- **Project Objective**
  - Create an Infrastructure to support the stated business objective (generic electronic identification) irrespective of application use
Achievements - Business

- Developed a model for the provision of Global Trust Services including a global architecture and the related roles and responsibilities
- Currently planning a number suites of global value added services which can utilise the infrastructure
Achievements - Legally

- Identified the applicable laws for cross border cryptography, digital signature and cross certification (OECD, UNCITRAL).

- Developed an implementation check list to cross border cryptography, digital signature and cross certification in order to avoid legal liability.
Achievements - Policy

- Completed ONE Global medium level assurance certificate policy for digital signature and non repudiation services
- Developed a certificate practice statement (CPS) accreditation program
- Each post shall write their own CPS to comply with the global industry policy.
Achievements - Technically

- Completed a global compatibility framework & Concept of Operation (Trust Model) for cross certification
- Developed interoperability specification which are now industry standards. Completed testing the interoperation of encryption and digital signature algorithms between 5 CA systems and 4 standard email clients
- Documented necessary product changes in of the shelf products in order to achieve global interoperability
Motivate vendors to implement product changes to enable this global business to happen

Implementation and realisation of the planned suite Value added services
Case On-line Government, Tax reports

- ELEKTRA - ELEktronisk RApportering (Electronic Reporting)
- Norway Post run this Project for The Directorate of Taxes (Skattedirektoratet - SKD)
- General effects of using electronic reporting
  - Reduced cost in paper handling and postage
  - Can receive structured and quality controlled data
ELEKTRA is based on existing Norway Post components:
  — Scanning Central
  — EDI central
  — WEB server park

Part of the Norway Post SEIF-concept
Secure Electronic Information Forwarding
The SEIF concept

"If you don’t need SEIFety - go elsewhere!"

Electronic Services

- El. commerce
- El. reporting
- MultiSmart

Infra-structure-services

- Scanning
- CTI
- eID
- Mondex
- EDI-central
- Web-central

Comm.services over open and closed networks

Operation of mainframes and servers
The SEIF concept

"If you don’t need SEIFety - go elsewhere!"

Infra-structure-services

Electronic Services

Operation of mainframes and servers

Comm.services over open and closed networks

Environment

Scanning  CTI  eID  Mondex  EDI-central  Web-central

El. commerce  El. reporting  MultiSmart

ELEKTRA
There are four reporting channels in the solution:

- EDIFACT - Electronic Data Interchange
- WEB-based forms
- Scanning of documents
- TouchTone-Telephone

SKD gets once a day a batch of tax reports from Norway Post.
**Elektra**

- Private persons
  - Misc. forms
- Business
  - Local EDI - software
  - OCR/Scanning
  - WEB - Tax form
  - WEB - VAT

- Message Handling Switch (MHS)

- Skatteetaten
The EDI-solution, and next year Web solution, will make use of Norway Post’ Electronic ID

One of Norway Post’ major new areas is to maintain the role of the Post as a national Trusted Third Party - and become the major issuer of a de facto National electronic ID

The eID will also be linked to a role certificate, making it possible to link a person to a formal role (doctor, lawyer..)