eGovernment as a driver for a culture of security – the case of Identity Management (IDM)

Katarina de Brisis, senior adviser, Department of national IT policy (ITP)

Norway – an advanced IT-Nation

— at the front in the use of ICT
— developing innovative ICT solutions
Early adopters

How to communicate under challenging conditions is at the core of Norwegian culture and skill base.

The long coast line, the vast distances and the rugged nature have fostered a unique taste for using and creating new ways of communicating.

The country’s research community has produced standards and products with worldwide reach, like the European standard for mobile telephony, GSM.

In 1919, Fredrik Rosing Bull patented the first punch card.

A connected society

Today, Norway has one of the world’s most connected populations and is one of the world’s most international economies.

Share of households with Internet-connection

### Government incentives

- Facilitating online services and providing valuable content to afford a competitive advantage for businesses and a simplification for the public
- Incentives for research and innovation

The government service AltInn allows over 50% of the reporting required from businesses to be done online, either directly from accounting systems or by filling a web form.

### Legal framework and strategy for identification enabling eGovernment is in place

- **eSignature as a guarantee for legal protection and validity** (Law on electronic signatures)
- **Regulation on the use of security services in electronic communication with and within the government**
- **A mandatory common specification for eID and eSignature (PKI) in the public sector, to be used in public procurement at central and local level**
- **A common strategy for deployment of eID and eSignatures to support eGovernment – mandatory use of a common security portal**

Under the Law on electronic signatures, e-signatures serve as a guarantee for legal protection and validity. They are widely used in the public sector, particularly in procurement, ensuring secure and efficient electronic communication.
eNorway 2009 – a forward looking policy for IT-society

- The individual in the digital Norway
- A coordinated and user-oriented public sector
- Innovation and growth in the Norwegian economy

Published June 2005

Focused goals in eNorway 2009

- Electronic service delivery through government portals MinSide and Altinn
- Common IT-architecture principles, based on open standards
- Extensive exchange and reuse of government register data
- Common solutions for eID/eSignatures, Identity Management and secure electronic service delivery and intergovernmental exchange of information (security portal)
- Common policy principles for access to public sector data for commercial services
- Paperless government
PKI (digital signature) in Norway

There is no interoperable infrastructure covering the whole of society available yet, but:

- The BankID cooperation targets 2 mill. homebanking users; 600.000 users expected by end of 2005
- Buypass/State Betting and Gaming Service targets 2,1 mill. customers with their new betting and gaming card / electronic purse; ca 500.000 new users expected by end of 2005
- Telenor Mobile plans for mobile PKI-supported services; 2 mill. PKI-enabled SIM-cards had been distributed to customers
- Skandiabanken operates a closed infrastructure with soft certificates for ca 300.000 homebanking customers
- Ergo Group provides national health network users with certificates (soft&hard); xx doctor’s offices subscribe
- St. Olav’s Hospital project (1 mill. certs to staff and users) - Telenor

Common security levels for eID and eSignature in the context of eGovernment

- High
- Standard
- Enterprise

Designated by:

- Certificate format and content requirements, inclusive naming conventions and unique identity determination
- Certification Service requirements ("Qualified")
- Enrollment procedure requirements, inclusive identification of users and key distribution
- Storage and protection of the private key
- Access to the private key
### What is Identity Management?

Identity management (ID management) is a broad administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity.

**IDM needs to be built on a set of policies, e.g. for:**
- Naming and Certificates
- Passwords
- Encryption and Digital Signatures
- Directories
- Privacy
- Authentication
- Provisioning
- Federation
- Data Confidentiality Agreement

### Why Identity Management in eGovernment?

- Prerequisite for effective rollout of new e-services
- Cost control - ROI
- Security and trust
- Quality and robustness of access control systems
- Simplification for end users

**Challenges:**
- Definition of identity in a “global” context
- Unique identification
- How to federate in a “global” environment – the question of trust
- Interoperability across heterogeneous IT-platforms
The FEIDE Identity Management System

The Altinn reporting portal

Altinn

- Reception
- Validation
- Distribution

Public registers

- Authentication
- Role delegation
- Authorisation

- Role delegation
- Authentication
The common public sector security portal

- The portal shall integrate minimum 3 suppliers of eID/e-signature (PKI); no upper limit
- The portal service provider will assume responsibility as an identity provider for service providers
- The PKI service suppliers shall be required to register with a public authority as compliant with the Common Requirements Specification for PKI in the public sector.
- The security portal shall manage eID/e-signature at the security level High and Standard. It shall be able to communicate with various service providers' systems (HTTP, SMTP, XML)
- The portal shall be able to validate identities issued under current schemes in the national health network and in Altinn.
- The portal shall provide identity federation for single-signon, both for various service portals and across government agencies, central and local
- The portal shall support an eID distribution service for both security levels
The common public sector security portal

- eID supplier 1
- eID supplier 2
- eID supplier X
- Security portal
- eID distribution Service
- Integration module
- Government agency
- MinSide
- AltInn
- Citizens and businesses
- eID/e-signatur

Advantages with a common portal

- Solves the PKI-service interoperability problem
- Provides generic mechanism for identity federations, and thus eliminates the need for separate SSO-solutions for various government service portals
- Simplification of procurement / implementation of PKI for smaller government agencies and municipalities
- Coordinated and fast rollout of eID to eGovernment users
- Cost control, ROI for government agencies wishing to implement PKI/SSO-functionality
- Common framework agreement allows for volume-based pricing strategies, saving money for the government, and eliminating barriers to broad uptake of eGovernment services
Why is this driving the adoption of a culture of security?

- The citizens and businesses gain simple and efficient access to a number of government services, using quality-assured security solutions (PKI-based eID and e-signature)
- The ubiquitous use of eID will heighten the level of security consciousness in the general public
- Cost-effective implementation of secure information exchange of government information and data (security is no longer an insurmountable barrier to going online)
- Improved access control to, and privacy protection of, government held identity and authorisation data, by centralizing the databases and coordinating the updating procedures of such data

Thank you for your attention