ROYAL NORWEGIAN MINISTRY
OF GOVERNMENT ADMINISTRATION AND REFORM

Proposal for a New Strategy

(in the process of public review, due to end in May 2007. Final strategy will be proposed to the Government in August/September 2007)

Strategy for the Use of eID and Electronic Signatures in the Context of eGovernment

Liberty Alliance
eGovernment Workshop
Brussels, 23 April 2007

Katarina de Brisis, Senior Adviser, Dep. of National IT policy

Why a New Strategy?

- Previous strategy (2005-2006) built solely upon PKI as the enabling technology for eID and e-signatures
- Government Specifications for PKI – current standard for central and local government entities
- Self declaration of compliance for PKI services' suppliers– within the National Post- og Telecom Authority
- Contractual agreement with a private service provider about a PKI-based government authentication portal had been abandoned in 2006
- Lessons learned:
  - Better coordination of government agencies' needs
  - Manageability, government's role
  - Broader technology approach
  - Financing schemes that are compatible with government budgeting principles

The Government Authentication Framework

- The Framework represents a common set of requirements and guidelines to be implemented by government agencies when developing electronic services for citizens and businesses
- The Framework defines:
  - **4 vulnerability levels** relating to the need for authentication and non-repudiation in online government transactions
  - **4 security levels** covering requirements for authentication solutions, including non-repudiation
- For each vulnerability level there is a corresponding security level

The definition of vulnerability levels

- The following criteria are proposed:
  - Consequences concerning health and welfare
  - Financial loss/ hassle/ increased costs
  - Loss of confidence (trust and integrity)
  - Obstruction of justice
  - Negligent contribution to perpetration of crime
  - Hassle and tort
- Level 1 represents low/no vulnerability for security breach in connection with authentication/signing.
- Level 4 represents high vulnerability.

The definition of security levels

- The following criteria are proposed:
  - Security properties of authentication factors
  - Enrolment procedures and proof-of-possession procedures
  - Secure storage and access to authentication factors
  - Additional requirements to achieve non-repudiation
  - Independent accreditation / declaration of compliance
- 4 security levels had been defined, with level 1 covering open access, up to level 4 covering sensitive / confidential information

Common security levels for eGovernment applications

Security level 4	Single sign-on to many services and direct access to services requiring high level of security. Gradually to replace authentication solutions on level 3.
Security level 3	Single sign-on to many services, as well as direct login to services requiring middle or high level of security.
Security level 2	Most of the existing eGovernment applications are here today. To be gradually migrated to level 3.
Security level 1	Open access to information, directly or through a portal (may involve identification)

Rollout of common authentication solutions on security level 3

- Proposal for a single type of ”authentication PIN” at the security level 3 (involves a dynamic factor as well) Distributed to citizens at no cost.
- Tax Directorate to manage the distribution, building upon the systems created for online tax returns.
- Common technical requirements to be developed for this ”authentication PIN”
- Agencies offering online services to enable login to these with the single ”authentication PIN” from day one (may keep proprietary solutions for a time)

Rollout of common authentication solutions at security level 4

- The proposal from the Ministry of Justice for a voluntary national identity card. The card to hold eID issued by a government CA. Citizens to pay a fee for the card.
- The national identity card with eID to serve as a common authentication solution for high security eGovernment applications.
- The government eID may also be rolled out on other tokens, e.g. social insurance administration's citizen card
- Plan B – a framework contract with a private PKI-supplier

The national identity card

- Voluntary scheme for Norwegian citizens and other applicants with permanent residence permit in Norway.
- To contain visual information, an MRT-area, as well as dual chip – an RFID (which will contain the visual info from the card and biometrics) and a contact chip to store eID
- Based on ICAO-standards to enable Schengen-functionality for Norwegian citizens
- Validity period of 5 years
- Dedicated registry for card owners
- New legislation (Act on national identity card)

The national identity card – II

- eID based on PKI, certificate class ”Person High” according to Common Requirements Specification for PKI in government
- eID to be issued by a public authority(Ministry of Justice)
- Two key pairs: one for authentication and encryption (age limit 13 years), and one for signing (age limit 18 years)
- Enrolment procedures and card issuance to be managed by the police authority, utilising the infrastructure for passport issuance

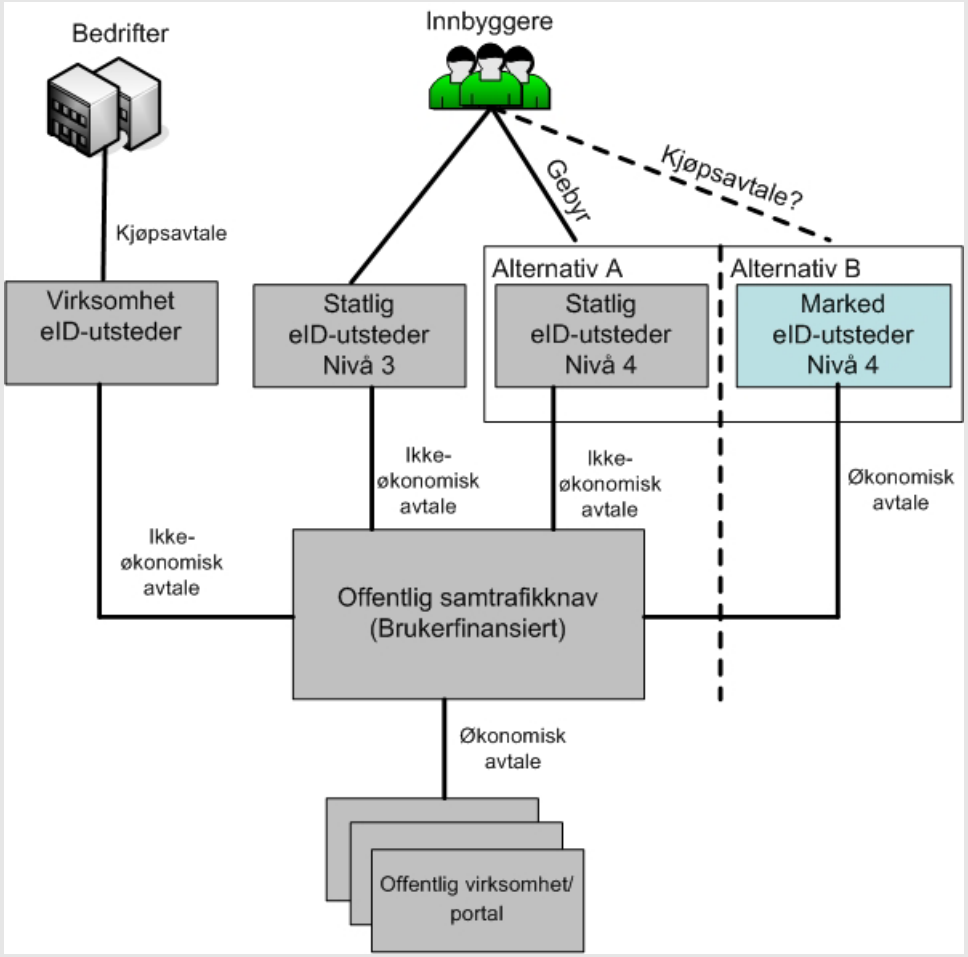
Rollout of enterprise eID

- Enterprise eID realised by PKI-certificates issued to enterprises (different from server certificates); based on certificate class ”Enterprise” according to Common Requirements Specification for PKI in government.
- Brønnøysundregistrene (company files agency) to establish a CA-service for issuance of certificates to all legal persons registered in Norway
- Government agencies will be obliged to obtain their enterprise certificate from this CA
- Non-government entities may do so, but will not be obliged.
- Enterprise certificates to be sold at competitive prices to non-governmental entities.

The government eID interoperability hub

- Government eID interoperability hub to be established for common use by all government agencies (central and local government)
- The interoperability hub to be managed by Brønnøysundregistrene.
- Basic services in the hub:
  - Authentication with common government eID (security level 3 eID and the national identity card)
  - Digital signing with common government eID (webforms and API for signing in local applications)
  - Digital archive (for digitally signed documents)
  - Single sign-on (SAML 2.0) – generic service
- Extended services, depending on demand

The business model proposal



The business model proposal

- Government financed rollout of ”authentication PIN”. No acquisition costs for citizens.
- Citizens shall not pay for the use of eID (either level 3 or 4) for authentication in eGovernment services.
- The citizens will pay a cost-based fee for the acquisition of a national identity card. The card may also be used for authentication in private services, but the costs incurred by that will need to be covered by the service and/or citizens.
- Government agencies shall not need to be invoiced for the validation of government-issued eID.
- Central financing of the interoperability hub, but yearly payments from connected agencies may also be envisaged.