IDABC
European
eGovernment Services

eID Interoperability for PEGS

NATIONAL PROFILE NORWAY

November 2007

This report / paper was prepared for the IDABC programme by:

Author's name: Jos Dumortier - Hans Graux, time.lex

Company's name: Siemens - time.lex

Company's address (optional):

Company's logo (optional)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°3

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/6484/5938

Executive summary

The project eID Interoperability for PEGS aims to propose a solution to the legal, technical and organisational issues related to the creation of an interoperable Pan-European identity management infrastructure. The EU Member States, Candidate Countries and EEA Countries are introducing more sophisticated ways to manage identities in the eGovernment area. Different member states are implementing different structures as their identity management solution. The main challenge for the eID Interoperability for PEGS project is to propose a general architecture that, while taking into account the existence of different models, is able to cope with them by obtaining the final goal of interoperability.

The project should conclude with several different proposals how to build interoperability without affecting member states' own existing infrastructures.

This document describes the current situation regarding the use of electronic authentication means in Norwegian eGovernment applications.

Table of Contents

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY

1.2 Reference Documents

[RD1]	eGovernment in the Member States of the European Union – 5th Edition – May 2006 http://ec.europa.eu/idabc/servlets/Doc?id=24769
[RD2]	European Electronic Signatures Study http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl
[RD3]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD4]	Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, OJ L 175, 15.7.2003, p.45 http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf
[RD5]	DIRECTIVE 2004/18/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_134/l_13420040430en01140240.pdf
[RD6]	IDABC Work Programme Third Revision http://ec.europa.eu/idabc/servlets/Doc?id=25302
[RD7]	DIRECTIVE 2004/17/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

2 Glossary

2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *Entity:* anyone or anything that is characterised through the measurement of its attributes in an eIDM system. This includes natural persons, legal persons and associations without legal personality; it includes both nationals and non-nationals of any given country.

- *eIDM system*: the organisational and technical infrastructure used for the definition, designation and administration of identity attributes of entities. This Profile will only elaborate on eIDM systems that are considered a key part of the national eIDM strategy. Decentralised solutions (state/region/province/commune…) can be included in the scope of this Profile if they are considered a key part of the national eIDM strategy.

- *eIDM token (or 'token')*: any hardware or software or combination thereof that contains credentials, i.e. information attesting to the integrity of identity attributes. Examples include smart cards/USB sticks/cell phones containing PKI certificates, …

- *Authentication*[1]: the corroboration of the claimed identity of an entity and a set of its observed attributes. (i.e. the notion is used as a synonym of "entity authentication").

- *Authorisation*: the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

- *Unique identifiers*: an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context. Examples may include national numbers, certificate numbers, etc.

- *Official registers*: data collections held and maintained by public authorities, in which the identity attributes of a clearly defined subset of entities is managed, and to which a particular legal of factual trust is attached (i.e. which are generally assumed to be correct). This includes National Registers, tax registers, company registers, etc.

[1] For the purposes of this Profile, the notion of authentication is considered to be synonymous with 'entity authentication', as opposed to 'data authentication'. The notion of 'identification should be avoided to avoid confusion.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

- *eSignature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions.

- *Advanced electronic signature*: an electronic signature which meets the following requirements:

  (a) it is uniquely linked to the signatory;

  (b) it is capable of identifying the signatory;

  (c) it is created using means that the signatory can maintain under his sole control; and

  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

  Again, this definition may cover non-PKI solutions.

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[2].

- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

[2] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

2.2 Acronyms

A2A	Administration to Administration
A2B	Administration to Businesses
A2C	Administration to Citizens
CA	Certification Authority
CRL	Certificate Revocation Lists
CSP	Certificate Service Provider
eID	Electronic Identity
eIDM	Electronic Identity Management
IAM	Identity and Authentication Management
IDM	Identity Management
OCSP	Online Certificate Status Protocol
OTP	One-Time Password
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
SA	Supervision Authority
SOAP	Simple Object Access Protocol
SCVP	Server-based Certificate Validation Protocol
SSCD	Secure Signature Creation Device
USB	Universal Serial Bus
TTP	Trusted Third Party
XAdES	XML Advanced Electronic Signature
XML	eXtensible Markup Language
XML-DSIG	XML Digital Signature

3 Introduction

3.1 General status and most significant eIDM systems

The government has decided that the realisation of a round-the-clock public administration is to be based on these main principles:

a) Electronic self-service facilities for citizens and businesses;

b) Development of common ICT components for the public sector; and

c) Establishment of common architectural principles for the public sector.

Electronic coordination in the public sector is still increasing, both horizontally and across the administrative levels (central/local government). The need for coordination between the public and private sectors is showing a growing trend, in parallel with coordination internally within the public sector. In certain contexts, public administration tasks are also dependent on the public sector and private business and industry having coordinated their electronic services. In certain areas of society, administrative authority is delegated to private or semi-private institutions or agencies.

Identity management on a national level is a coordinated administration system applicable all over Norway. We are seeing a transition from local to national identity management in many areas. This trend is driven by financial and political considerations.

There are several public authorities that today use systems to authenticate their users of web-based services. In December 2005 the Ministry of Government Administration and Reform undertook a mapping of 15 public authorities that provide web-based services to private persons domiciled in Norway and businesses. PIN-codes and passwords were the prevailing eID solutions used by these authorities.

Some examples of existing solutions are described below.

3.1.1 Altinn[3]

Altinn is a common Internet portal for public reporting. In 2002 the Norwegian Tax Administration, Statistics Norway, and the Brønnøysund Register Centre joined forces in order to create a common Internet portal for public reporting. The portal was launched in December 2003 under the name Altinn, and has been in full operation throughout 2004. Altinn is a 24/7 solution and is built on a .NET platform, but there is no demand in most cases for the users to change their hardware or software. Regular access to the Internet is usually sufficient. The solution builds on a standard interface based

[3] https://www.altinn.no/cms/1044/altinn/Mer+om+Altinn/Altinn+in+English.htm

on an open standard (XML, SOAP), and integration towards the IT systems for the enterprises is implemented through the help of web services. Altinn is designed for any security level.

Today the Altinn solution uses a combination of a log and authentication for signing on security level 2 and PKI with a smart-card on security level 4, cf. below.

To be able to logon Altinn the user must have a Norwegian personal identification number and a one-time PIN-code. The PIN-code is found either on the form for tax return, sent out by the state, or on the tax withholding card, also sent out by the state. When logging-on the first time the user identifies him-/herself by the personal identification number and the PIN-code. After that the user is asked to submit his/her mobile telephone number and also to choose a password. This will simplify the log-on procedure the next time. When logging-on the next time the user identifies him-/herself by the personal identification number and the password he/she chose. To continue to some services an additional code is sent by SMS to be used in the login process.

The personal log-in procedure is also used for the representation of legal entities, where the person is linked to an authorisation on which entity(-ies) he may represent and in what capacity.

3.1.2 My Page (Min side)

Mypage brings public service offerings together in a web portal. The user will have his own custom page on this portal. The information will be structured thematically, and the services will be grouped and sorted according to the user’s needs. The information and services on Mypage will be provided by agencies and authorities at all levels of public administration, ranging from large central government agencies to small local authorities.

Mypage is divided into two different types of services

(i) Register services; shows what information various agencies have on its users, eg. My Address, My Properties, My Family Doctor and retrieve income tax forms already filed with the tax-authorities.

(ii) Transaction services; allows users to carry out an actual service linked to an agency or local authority, and eg. change the information.

Access to MyPage will be controlled by a login solution that is common for public services. The login process will follow procedures that prevent unauthorised use of others identity.

The first time you log in you must register the following information before you are granted access to MyPage:

- PIN code from your tax deduction card or PIN code sheet.
- E-mail address/mobile phone number – used to send a temporary password.
- New password – a self-selected password. Must consist of at least eight characters and at least one of them must be a number.

If you have logged in previously, you enter a PIN code and a self-selected password to gain access to MyPage.

My Page uses a SSL-sertificate for the log-on process. The login solution also includes the forwarding of an electronic identity so that users can continue on to another public website without logging in again.

3.1.3 The State Educational Loan Fund

The State Educational Loan Fund[4] (hereinafter referred to as NSELF) has two different authentication solutions. One for logging-on to "Your Page" ("Din side") and one for signing.

- User name and PIN-code for logging on "Your Page" is sent out to all users at a given time. The user can always change the PIN-code, after having logged on the first time. The State Educational Loan Fund does not have access to the PIN-code. It is also possible to log-on to "Your Page" via "My Page", cf. above.

- In connection with granting loans to students NSEF uses a smart-card solution for the signing of the promissory note.[5] The use of an electronic signature is an offer from the NSELF to all students of higher education (i.e. education at university or college level). Normally a promissory note is sent by ordinary mail, to be signed by the student granted the loan prior to the loan being paid. Instead of receiving the promissory note by ordinary mail, it can be sent electronically over the Internet. To be able to sign the promissory note electronically the student only needs a PC with an Internet connection, a smart card and a smart card reader. Three different smart cards can be used, all issued by Buypass AS[6], costing from NOK 60,- (about 7,50 EURO). The three different cards are:

  - "the Buypass" which is a smart card that can be used by all Buypass users. In addition the card can be used together with 3rd party software programs for authentication, signing and encryption (eg. e-mai).
  - "the Lottery-card" which can be used for all games provided by the Norwegian National Lottery[7] games on the Internet, and which can also be used when playing with one of its commissionaires. The smart-card can be used for eID services with other Buypass users.

[4] In Norwegian "Statens Lånekasse for utdanning", www.lanekassen.no

[5] The easiest and fastest way to apply for financial support from the NSELF, is to use the online application. Most applicants can use the online application.

[6] Buypass AS is s owned jointly by the Norwegian National Lottery and Norway post - http://www.buypass.no/kortutstedere.htm

Buypass smart-cards can be upgraded to a qualified certificate, cf. http://www.buypass.no/bedriftslosning/buypass_activate.htm

[7] The Norwegian National Lottery (Norsk Tipping) is Norway's leading games company, wholly-owned by the Norwegian state, cf. www.norsktipping.no

- "the Altinn smart card", which is also the only log-on alternative that provides services on the highest security level in Altinn.

3.1.4 FEIDE

FEIDE[8] is an initiative to create a federated identity management system on a national level for the educational sector. This does not entail merging personal data registers or creating a new central register. It involves converting the organisations' local identity management to a common format, so that each organisation can confirm the identity of its own students and employees in the same way. A FEIDE-affiliated organisation thus gives its students and employees an identity – a FEIDE name – that is valid throughout the sector.

This is a concept based on the principle that every user in the educational sector – pupil, student or employee – receives a user name from their school, college or university, which can be used throughout the sector. The same user name works everywhere, both at the user's own organisation and for shared national services, with the same password or certificate. A central login service is implemented, which checks that the user name and password or certificate agree – in other words, that it is the right person who is logging on. The central login service Moria[9] does not keep the user name and passwords in storage – they exist only at the user's school. Moria receives confirmation from the person's school that the password or certificate matches correctly, and then provides a little data about the person from the school to the service. Each service receives only the personal data that FEIDE considers that it needs and may receive, and receives the data only if the user approves this.

A service that uses the FEIDE login will immediately have all students and staff in the entire sector as potential users. Single Sign-On is supported by Moria on both the user and the service side. Within FEIDE's log-on services Moria conducts more or less the same type of services as Shibboleth. FEIDE also contains the infrastructure to the contracts and defines a common datamodel in the form of an LDAP-form for Nordic educational establishments.

3.1.5 The Internal Revenue Service

The Internal Revenue Service[10] has its own PIN-code solution for tax deduction cards and pre-filled out income tax form, that are distributed to the majority of the population. Total distribution of "TaxPIN" is 3,6 million tax deduction card and 0,36 million "free cards", on a population of 4,66 million. The PIN-code can be used in the tax authorities own portal (www.skatteetaten.no) or in the portal for services to businesses (www.altinn.no). For those using the Altinn portal, they can also use Altinn's own PIN-codes (received by regular mail or SMS). As an indicator on the use of different

[8] Federated Electronic Identity www.feide.no

[9] Moria is an authentication service forWeb-based services. Moria is Open Source and the code is available on SourceForge - http://sourceforge.net/projects/moria/

[10] In Norweigan "Skatteetaten", cf. www.skatteetaten.no

electronic solutions the following information on persons filing their tax return form electronically can be presented:

	30 April 2007	30 April 2006	30 April 2005
Internet	1 538 025	1 400 031	1 255 536
Phone	194 642	217 358	269 542
SMS	365 454	320 459	276 006
Total filed electronically	2 098 121	1 937 848	1 801 084

3.1.6 Norwegian Labour and Welfare Organisation

The Norwegian Labour and Welfare Organisation[11] has a PIN-code solution sent to the user's address registered in the Central Population Registry.

In addition NAV uses different means of authentication to its different services, i.a.

- A user-name and password to file information on employees to the special employe/employees-register.
- In the "My Family Doctor" service the user only has to submit his/her personal identity number, full name and postal code.
- In addition NAV has established several machine-to-machine solutions within the health sector that use PKI-based personal digital signatures on a smart card and entity certificates. A similar solution is established between NAV and all pharmacists, at security level 4, cf. chapter D.1.

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

As of 1 October 2004, the Ministry of Government Administration and Reform is responsible for the government's coordination of ICT policy. The Ministry of Transport and Communications is

[11] Cf. www.nav.no

responsible for telecoms policy and the Ministry of Trade and Industry is responsible for the ICT sectors and for research in the ICT area.

The Norwegian Association of Local and Regional Authorities (KS) is a national member's association for municipalities, counties and public enterprises under municipal or county ownership. All municipalities and counties are members. KS is an employer's and central bargaining organisation, an advisory and consultative body, and acts as a spokesman and advocate vis-à-vis central government on behalf of its members. Even with the principle of independence of the municipalities vis-à-vis the state, the Ministry of Government Administration and Reform has also an overarching coordinating responsibility for the ICT area vis-à-vis the municipal sector. The co-ordination is, inter alia, achieved through the portal My Page (se chapter B above), but there are municipalities, or conglomerates of municipalities, that have their own solutions using different eIDM mechanisms, including the use of BankID.

From the examples shown above one can draw the conclusion that the use of eIDM systems is diverse, but within each system functioning on a national level.

eGovernment projects in Norway are often vertically integrated, i.e. within the same area of competence, such as tax or social security. Nevertheless, steps are being taken towards horizontal integration covering several departments and institutions. One of the purposes of horizontal integration is to share information so as to avoid requesting it twice from citizens or companies. A registry with the Brønnøysund Register Centre achieves this. The register center is, however, now working on a new register (SERES) for semantic interoperability, that will even further ensure that authorities have the same understanding of the semantics of the information, that will further facilitate and ensure that the same information only has to be reported once.

3.2.2 National eGovernment cooperation and coordination

The Norwegian government has identified a need to coordinate eGovernmental services, cf. the White Paper on ICT-policy from 2006[12]. The coordination is on several areas and levels, i.a. between the state and municipalities, to establish portals such as Altinn and My Page, to enable the use of the technical solutions (or parts of the technical solutions) of Altinn by other public authorities etc. There is also an identified need for coordination regarding the use of digital signatures (PKI). The Ministry of Government Administration and Reform sent out a letter in 2006, stating that if state authorities are to use digital signatures they must use the signatures identified in the "Requirement Specifications for PKI for the public sector" and, given the fact that the Government cannot order municipalities to do the same, strongly recommended municipalities to also use these e-signatures. (Reference to this letter cf. chapter D.1.)

Making electronic self-service solutions available on the Internet imposes special requirements on the security of electronic communications. Both the sender and the recipient must be sure of whom they are communicating with. In addition, the parties must be able to rely on the contents of what is being

[12] Report nr. 17 (2006-2007) to the Storting (Parliament) – "An information society for all" (St.melr nr. 17 (2006-2007) Eit informasjonssamfunn for alle)

communicated. In response to these challenges, in 2004, a joint Requirements specification for PKI for the public sector was prepared. The strategy sets out in essence three primary measures:

– Establishment of a public approval scheme for providers of *e*ID and e-signatures in the public sector in conformity with the ”Requirements Specification for PKI for the Public Sector”.
– Establishment of a general agreement concerning a joint security portal for the entire public sector, including the municipalities.
– Establishment of a general agreement concerning an enterprise *e*ID and employee *e*ID.

A volontary approval scheme for providers of eID and e-signatures solutions in the public sector in conformity with the ”Requirements Specification for PKI for the Public Sector”, was established, with a statutory basis in the Act on e-signatures. This approval scheme entered into force in December 2005.

The security portal was conceived as a joint login and signature solution for public websites. In July 2005, the State signed a general agreement on security portal services with a commercial supplier. But many of the most relevant suppliers wanted to offer their services directly to the individual national bodies and municipalities. This meant that the security portal services were insufficiently used, which benefited neither of the parties. They therefore agreed in June 2006 to terminate the agreement. In the autumn of 2006, the Ministry of Government Administration and Reform began working on a new strategy for *e*ID and e-signatures for the public sector. The strategy was sent to public hearing in the spring of 2007. Conclusions from this hearing were not publicly available at the time this report was drafted.

The essence of this stategy focuses primarily on:

- The use of a national ID-card (with an eID) as the highest security level for eGovernmental services.
- The establishment of a national joint security portal for the entire public sector (including Altinn and MyPage, and including municipalities) where the national eID and "accepted" private solutions can be verified.

3.2.3 Traditional identity resources

The Central Population Register

Identification towards Norwegian eGovernment services – that need some sort of authentication – is based on the personal identification number from the Central Population Register, and some additional security measure, PIN-code, address etc.

When using a PKI-based solution, there is a reference from the certificate to a catalogue with the holder's national personal identification number.

The Central Population Register is Norway’s authoritative source for a person’s name and date of birth. The unique identifier used in eGovernment services is the personal identification number. The personal identification number is an eleven-digit long number that is assigned by the state to all its inhabitants.[13] The number is unique for each person. The scheme of personal identification numbers was introduced in 1964 and is administrated by the Internal Revenue Service. Everybody who is living in Norway – subsequently not only Norwegian citizens - and who is entered in the Central Population Register is given a personal identification number (or a D-number). Pursuant to the Act on Personal Data a personal identification number can only be used when there is a just reason and it is impossible to ascertain a persons identity by other means such as name, address, date of birth, customer/member number. Public authorities are usually given the right under law to ask for a person's personal identification number.

The Central Population Register does not issue any form of identity card, but issues birth certificates that are usually the seed document when applying for identification cards.

The Directorate of Taxes (*Skattedirektoretet*) keeps the registry updated. Updates are based on information for public authorities (notice of birth or death, and changes regarding civil status) and from the inhabitants themselves, eg. there is a mandatory obligation to give notice when changing addresses.

Both private and public entities use the information in the registry, and they depend on the fact that the information in the registry is correct. However, full access to the registry is limited. Only private entities that have a reporting obligation to the Directorate of Taxes can be granted such access to the registry.

Central Coordinating Register for Legal Entities

The primary task of the Central Coordinating Register for Legal Entities is to coordinate information on business and industry that resides in various public registers, and which is also frequently requested on questionnaires from the public authorities. Instead of having each public authority send their own separate form for a company to answer, the Central Coordinating Register for Legal Entities ensures that all the information is collected in one place. When the Central Coordinating Register for Legal Entities was opened in 1995 it was applauded as one of the most important measures to improve efficiency in public administration in recent years.

The Central Coordinating Register for Legal Entities contains basic data about entities that are under reporting obligations to the Register of Employers, the Value Added Tax Registration List, the Register of Business Enterprises, the Business Register of Statistics Norway, the Corporate Taxation Data Register or the County Governors' Register of Foundations. Others may register voluntarily with the Central Coordinating Register for Legal Entities.

The nine-digit organisation number identifies an entity, making it easier for the authorities to collaborate on information exchange. Pursuant to the Act relating to the Central Coordinating Register for Legal Entities, other state registers are obliged to cooperate with the Central Coordinating Register for Legal Entities and keep their register information updated. A coordinated register notification replaces the registration forms from various authorities that were previously used, ensuring that the

[13] Eg. If you are born on 23 November 1965, your number can be 231165-12345.

necessary information is distributed to those authorities that require registration and notifications of changes.

As all the various authorities use a common register for exchanging information among themselves, complying with the form requirements will become easier for all business operators and others engaged in financial activities. Many associations and others with no registration obligation find it useful to register voluntarily with the Central Coordinating Register for Legal Entities. There is no charge for registration.

The Central Coordinating Register for Legal Entities only contains information that is stipulated by law, and everyone has access to open register information, such as correct name and address, business objective, industry/branch and representative. Key information can be obtained without cost via the Internet and over the phone. For a fee, printouts from the register can also be obtained with the same information.

It is possible to submit a form wholly electronically for the registration of a new legal entity with the register.[14] This requires the use of a digital signature, and can be done by the use of the PIN-codes accepted by Altinn or smart-card solutions cf. above. The solutions for submitting the form electronically, allows several persons to duly sign the documents. Part of if can be “disconnected” eg. for the appointed auditor, and duly signed and submitted separately.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

At the present time the Norwegian government does not issue a physical national Identity Card, with or without an eID. However, the Ministry of Justice has sent out a report on public hearing suggesting that the Police Authorities shall issue a voluntary National Identity Card, also to be used as a "Schengen-card" (a "mini-passport"), with an eID/eSignature on a chip on the card.[15] Pursuant to the report the eID shall contain a “Level 4” certificate, and fulfil the requirement for a Person-High pursuant to the “Requirements Specification for PKI in the Pulic Sector.” (This is a certificate based on a qualified certificate, with additional requirements. Further information on Person-High cf. chapter D.3.]. The hearing of this report was finalised in mid-June 2007. Conclusions from this public hearing were not available at the time this report was drafted.

Simultaneously with the Ministry of Justice’s send-out of its report on a national ID card, the Ministry of Government Administration and Reform sent out a report regarding the strategy of the use of eID

[14] https://www.altinn.no/cms/1044/altinn/Tjenester/Samordnet+registermelding.htm

[15] Cf the report in Norwegian http://www.regjeringen.no/upload/JD/Vedlegg/ID-kort-Sluttrapport.pdf

and eSignature in the public sector on public hearing.[16] One suggestion in the strategy is that the eID in the National Identity Card shall be used in communication with the public administration, at the highest security level. In addition, the Ministry proposed that the government should establish a security portal for the validation of different publicly or privately issued eID's used for governmental services. The closing date of the public hearing was mid-May 2007. Conclusions from the public hearing were not available at the time this report was drafted.

There are, however, various authentication solutions provided and used by the public sector. These solutions vary between the different sectors and the technical requirements, but they can usually also be used by non-nationals living in Norway.

Pursuant to The Regulation on Electronic Communication with and within the Public Sector[17] Section 27 paragraph 1 the Ministry of Government Administration and Reform has been given the task to have the coordination responsibility for the public sector's (at state level) use of security services and products in relation to electronic communication with and within the public administration.

In this capacity the Ministry of Government Administration and Reform sent a letter on 21 September 2006, to all government departments with i.a. the following content:

"A voluntary self-declaration scheme for certification service providers of eID and e-signatures has been established, based on the requirements in the 'Requirements Specification for PKI for the Public Sector'. This is a self-declaration scheme with its statutory basis in a new regulation to the Act on e-signature. The scheme is administered by the National Post and Telecommunication Authority (NPT). NPT shall, based on the information submitted, evaluate whether the certification service provider fulfils the requirements in the public requirement specification for electronic ID and electronic signatures, and thereafter make public a list of providers that fulfil these requirements. The Ministry of Government Administration and Reform has decided that all public authorities that wish to use a PKI-based solution for electronic communication internally or externally with its users, shall demand that the products and services that are acquired for this purpose are self-declared pursuant to the voluntary self-declaration scheme, to that extent it is relevant for the chosen solution. This decision has its statutory basis in the eGovernment Regulation."

At the present time there is no official authentication policy in Norway that defines a strict hierarchy of the different authentication systems in use. However, relevant to this is what the Ministry of Government Administration and Reform stated in its "Strategy on eID and e-signature in the Public Sector" of March 2007:

"***FRAMEWORK FOR AUTHENTICATION AND NON-REPUDIATION IN ELECTRONIC COMMUNICATION WITH AND WITHIN THE PUBLIC SECTOR***

[16] Cf. the report, n Norwegian http://www.regjeringen.no/nb/dep/fad/dok/Horinger/Horingsdokumenter/2007/Horing-forslag-til-strategi-for-bruk-av.html?id=454620

[17] FOR 2004-06-25 nr 988: Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften).

1.1 Background

The public sector has a strategy to pave way for good electronic services to its users (inhabitants and businesses), and also pave way for good electronic interaction between public authorities.

The Regulation on Electronic Communication with and within the Public Sector sets out a requirement that a public authority that chooses to communicate electronically, shall organize its communication in such a way that it ensures necessary confirmation on the parties identity or authorisation, that the data is not involuntary or illegally altered (integrity), protection of the data against unauthorised access (confidentiality), and that it is possible to prove that the activities has taken place and who sent or carried them out (non-repudiation), in accordance with its own security strategy. The public authority shall, however, not set higher requirements than what is necessary in respect of the type of data that is communicated or the activity that is offered to be done electronically.

This document doses not present a complete framework on security, but is only a framework addressing the security services authentication and non-repudiation.

….

3.3 Risk levels

	Risk level 1 **None**	**Risk level 2** **Small**	**Risk level 3** **Moderate**	**Risk level 4** **Large**
Consequence for life and health	There is no danger of loss of life and/or health damage	There may occur minor health damage	There may occur minor health damage	There may occur of loss of life and/or major health damage
Financial loss / extra work / incur increased costs	No financial losses / extra work / incur increased costs	There may occur minor financial losses / extra work / incur increased costs	There may occur moderate financial losses / extra work / incur increased costs	There may occur major financial losses / extra work / incur increased costs
Loss of reputation (standing, trust and	No loss of reputation	Possible damage on	Reputation may be	Reputation may be

integrity)		reputation is considered trivial	weakened for a short period of time	damaged for a longer period of time, possible for ever
Obstruction of justice	No contribution to obstruction of justice	Minimal contribution to obstruction of justice	Moderate contribution to obstruction of justice	It may incur obstruction of justice
Accomplice liability / accessory to violation of the law	Accomplice liability / accessory may not occur.	Accomplice liability / accessory may not occur.	Accomplice liability / accessory may not occur.	Accomplice liability / accessory may not occur.
General problems / inconveniences	No general problems or inconveniences	There may occur some general problems or inconveniences	N/A	N/A

….

4. Security levels

L E V E L	**Requirements Regarding Authentication Factors**	**Issuance to holders**		**Assurance of authentication factors, when storing**	**Requirement to public registration**	**Requirements on non-repudiation**
		Natural persons	**Legal persons**			
1	No requirements	No requirements	No requirements	No requirements	No requirements	No requirements
2	One factor	Mail to registered address at	Mail to registered address. The	Both static and dynamic can be	No requirements	It shall be established routines and

		the Central Population Register	name of the natural person that can sign on behalf the the legal person shall be the first to receive the sending.	copied		logs, that make it reasonably sure that the party you are communicating with stands behind an activity or data
3	To factor, of which one is dynamic	Same requirements as for level 2, with the additional requirement that one ensures in one way or the other that it is the right user	Same requirement as for level 2, with the additional requirement that one ensures in one way or the other that it is the right user	Dynamic can be copied. Static can not be copied	No requirements	It shall be established routines and logs, that make it reasonably sure that the party you are communicating with stands behind an activity or data
4	To factor, of which one is dynamic	The requirements on registration and issuance in accorance with the ”Requirement Specification for PKI for the Public Sector”, Person-High. To meet up in person with ID-documents, at least the first time.	The natural person that can sign on behalf of the legal person, either by meeting up in person, or give a proxy to another that meets up in person. The person meeting up shal present ID-documents, and be checked againt the	Can not be copied.	Shall be declared in accordance with public requirements.	A party to the communication shall be able to verify that the other party stands behind an acitity or data. The party shall not be able by himself to produce or alter such an evidence afterwards.

			Central Coordinating Register for Legal Entities. Requirements in accordance with the ”Requirement Specification for PKI for the Public Sector”, Enterprise.			

Security level 1

This security level gives no security. Used in open communication. There are security solutions that fall within this category, e.g.

- *self-elected password and user name over the net*
- *identification using only a personal registration number*

Security level 2

Examples:

- *Static password, sent to the address registered with the National Registry*
- *Password calculator not protected by a password, at a minimum distributed to the address registered with the National Registry*
- *Lists with one-time passwords, distributed to the address registered with the National Registry*

Security level 3

Examples:

- *Password calculator protected by a PIN-code, where the first PIN-code is sent by a seperate mail*
- *One-time passwords on cellular phone, where the cellular phone is registered with an own registration code distributed to the address registered with the National Registry*
- *Person-Standard pursuant to the ”Requirement Specification for PKI for the Public Sector”,*
- *List with one-time passwords, used together with a static password and user name.*

Security level 4

On this security level only solutions based on PKI can be accepted. Pursuant to the requirements in existing regulation the solutions must be registered with the National Post and Telecommunication

Authority, in accordance with the "Requirement Specification for PKI for the Public Sector", when it comes to Person-High and Enterprise. Examples:

- *A two-factor solution, of which one is dynamic, of which one of the factors or registration factor is delivered personally. It is used a third party to register a log with a connection between activity/data and identity. The log shall be stored with protection against modifications.*
- *A two-factor solution, of which one is dynamic, of which one of the factors or registration factor is delivered personally. It is used a special program that prevents the users to generate false documentation of whom is standing behind data/activity and that prevents the provider to change the log of data/activities and identity.*

…

i) Proposed use of security levels

Risk level 1	à	*Security level 1*
Risk level 2	à	*Security level 2*
Risk level 3	à	*Security level 3*
Risk level 4	à	*Security level 4*

…."

3.3.2 Legal framework

The main legal framework for the eID card is laid down in:

- The Act of 15 June 2001 no. 81 on electronic signatures (the eSignature Act)[18]
- The Regulations of 15 June 2001 no. 611 on requirements applicable to issuance of qualified certificates etc.[19]
    - ♦ These regulations contain inter alia a requirement that issuance of qualified certificates shall be done by personal appearance, unless it already exist a relation between the certification service provider and the holder which is based on personal appearance.

[18] Lov 15. juni 2001 nr. 81 om elektronisk signatur (esignaturloven).

[19] Forskrift 15. juni 2001 nr. 611 om krav til usteder av kvalifiserte sertifikater mv.

- The Regulations of 21 November 2005 no. 1296 on voluntary self-declaration scheme for certification service providers.[20]
    - ♦ These regulations set up requirements for certification service providers that want to submit a declaration, that they fulfill the requirements in the "Requirement Specification for PKI for the public sector"; i.e. Person-High, Person-Standard and Enterprise (cf. chapter D.3).

- The Regulations of 25 June 2004 no. 988 on Electronic Communication with and within the Public Sector[21]

Norway has no specific regulations with regard to the process of authentication in general. The Act on electronic signature transposes the provisions of the e-Signatures Directive, but does not state anything about the use/acceptance of different eSignatures/eID. It should, however, be noted that the definition of qualified certificates in the act also applies to authentication. Cf. that the certification class Person-High pursuant to the “Requirements Specification for PKI for the Public Sector” – with a prerequisite of being a qualified certificate – also can be used for authentication.

3.3.3 Technical aspects

As already mentioned above there is at the moment not one prevailing eID solution for eGovernmental services today. It is a many faceted situation, but there is a drive in the Government, especially on the central level, to use eID defined in the “Requirement Specification for PKI for the public service”.[22]

Subsequently I will focus on the three different electronic signatures / eID defined in the above-mentioned requirement, i.e. Personal-High, Personal-Standard and Enterprise.

The Requirement Specification for PKI for the public service is a general, functional specification of the requirements applicable to the procurement of PKI (Public Key Infrastructure) for use in connection with electronic communication with and within the public sector. This requirements specification was drafted in response to a resolution adopted by the Norwegian Government on 17 June 2004, requiring a common specification for electronic ID and signature to be formulated by 15 November 2004. The specification will in turn form the basis for common framework agreements for use by the public sector. The resolution reflects the Government's goal of unlocking the potential that lies in making more public services available in electronic form, allowing the dealings of the citizens,

[20] Forskrift 21. november 2005 nr. 1296 om frivillige selvdeklarasjonsordninger for sertifikatutstedere, §11 første ledd.

[21] Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

[22] http://www.regjeringen.no/en/dep/fad/Documents/rapporter_planer/Rapporter/2005/Requirements-specification-for-PKI-for-the-public-sector.html?id=420380

business and industry of Norway with public sector agencies to be simplified and enhancing the efficiency of public administration. The availability of electronic ID and signature is increasingly seen as a prerequisite for efficient electronic interaction with citizens and the private sector.

As already is clear from the title of the requirements all eIDs defined in the document is based on PKI technology. Each private key is dependent on the use of a PIN-code.

Any certification service provider – public entities or, national entity or non-national private entity – may issue certificates/eID pursuant to these requirements. The validity of the cards is set to a minimum 13 months, but temporary certificates with shorter lifetimes may be permissible.

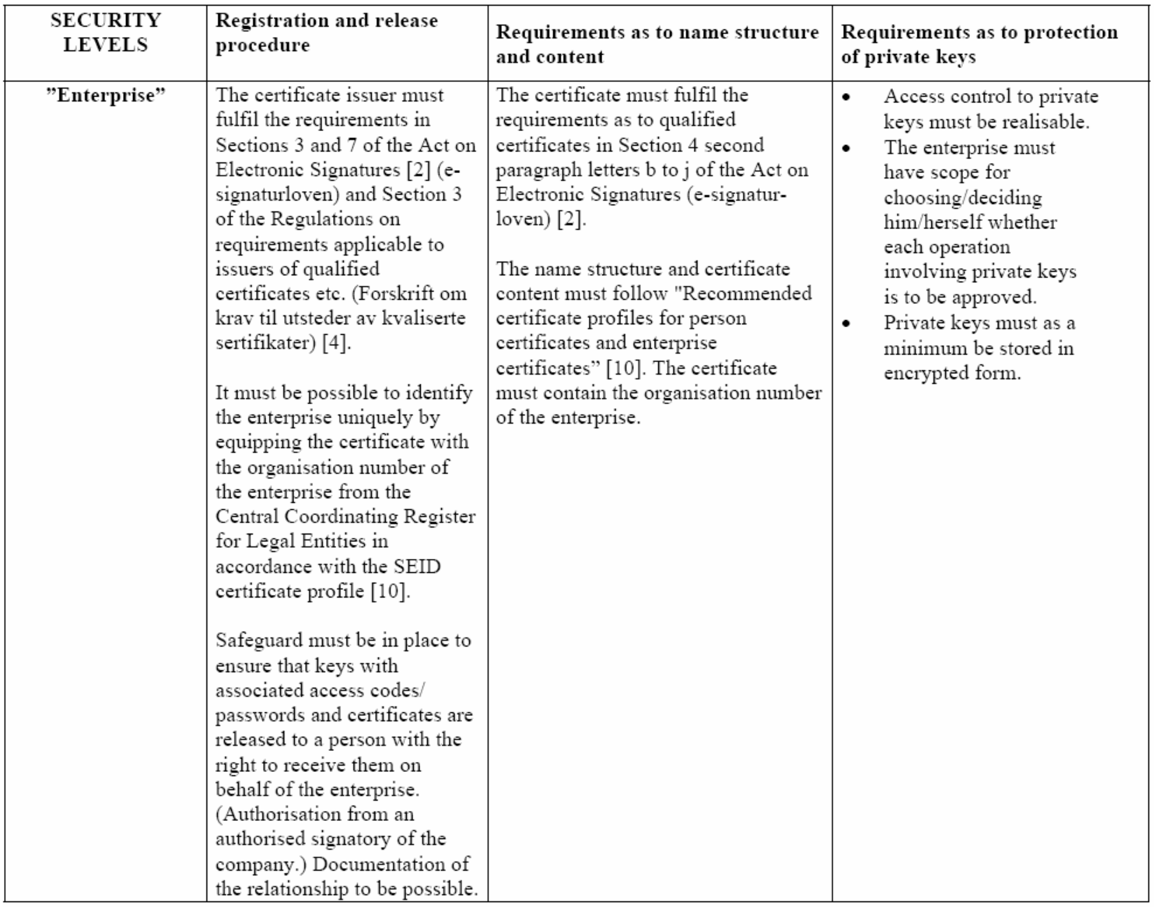
The requirements cover PKI solutions for

(i) authentication/identification,
(ii) signature, and
(iii) encryption (more specifically, PKI will be used for key exchange in connection with encryption).

The requirements specification does not cover the use of PKI for signing program modules or authentication/key management of processes and computers. Nor does the document define requirements for employee certificates, since it is assumed that in technical terms person certificates will in many cases cover this requirement. In such cases it will, inter alia, be the issuance procedures and rules on authorisation and use within an enterprise that will determine whether or not a person certificate can be used in a professional context. Much of this document can be used by enterprises seeking employee certificates explicitly linking a person to the enterprise. The specification describes a PKI solution for integration with one or more applications. The degree of functionality provided by the application and by the PKI solution will vary depending on the solution proposed by the individual supplier. Accordingly, some requirements may be understood as functionality within the application, whereas for other solution concepts these will be requirements relevant to the PKI solution. Similarly, there may be different solution concepts for the RA function. RA tasks can be performed by the certification service provider, within the user site or within the user's system.

The requirements specification contains three levels of security, two for individuals (Person-High and Person-Standard) and one for enterprises (Enterprise): The security levels and a selection of properties are specified in the table below:

SECURITY LEVELS	Registration and release procedure	Requirements as to name structure and content	Requirements as to protection of private keys
”Person-High”	The certificate must be a qualified certificate and the certificate issuer must fulfil the registration and release procedures that follow from this, including the requirement as to personal attendance.	The name structure and certificate content must follow the requirements in Section 4 of the Act on Electronic Signatures (e-signaturloven) [2] with the clarifications that follow from "Recommended certificate profiles for person certificates and enterprise certificates" [10].	• Access to private keys must as a minimum require two-factor authentication, where one of the factors is something in the physical possession of the user (i.e. cannot be copied electronically). • The user must approve each operation involving private keys by authenticating him/herself • Private keys must never appear in plain text in registers that might be compromised or in other ways provide a basis for unauthorised use.
”Person-Standard"	The certificate issuer must fulfil the requirements in Sections 10 to 16 of the Act on Electronic Signatures (e-signaturloven)[2] and Section 3 of the Regulations on requirements applicable to issuers of qualified certificates etc. (Forskrift om krav til utsteder av kvaliserte sertifikater) [4]. Verification must take place upon registration that the person is found in a Norwegian population register and that the name of the person accords with his or her national identity number. A reasonable degree of certainty must exist that keys and/or associated access codes/passwords and certificates are released to the correct person. Release must either be by postal dispatch to the registered address or electronically based on existing authentication mechanisms providing the same degree of security of correct receipt as a postal dispatch to the registered address.	The certificate must fulfil the requirements applicable to qualified certificates in Section 4 second paragraph letters b to j of the Act on Electronic Signatures (e-signaturloven) [2]. In other respects the name structure and certificate content must follow "Recommend certificate profiles for person certificates and enterprise certificates" [10].	• Access to private keys must require authentication • The user must have scope for choosing/deciding him/herself whether the individual operation involving private keys is to be approved. • Private keys must as a minimum be stored in encrypted form.



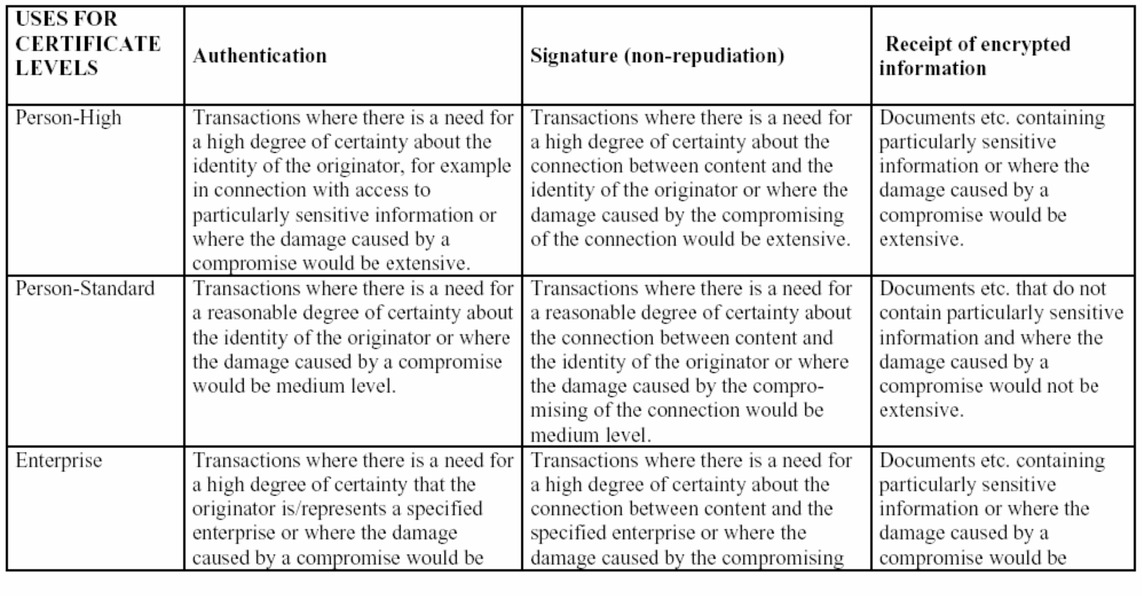
SECURITY LEVELS	Registration and release procedure	Requirements as to name structure and content	Requirements as to protection of private keys
"Enterprise"	The certificate issuer must fulfil the requirements in Sections 3 and 7 of the Act on Electronic Signatures [2] (e-signaturloven) and Section 3 of the Regulations on requirements applicable to issuers of qualified certificates etc. (Forskrift om krav til utsteder av kvaliserte sertifikater) [4]. It must be possible to identify the enterprise uniquely by equipping the certificate with the organisation number of the enterprise from the Central Coordinating Register for Legal Entities in accordance with the SEID certificate profile [10]. Safeguard must be in place to ensure that keys with associated access codes/ passwords and certificates are released to a person with the right to receive them on behalf of the enterprise. (Authorisation from an authorised signatory of the company.) Documentation of the relationship to be possible.	The certificate must fulfil the requirements as to qualified certificates in Section 4 second paragraph letters b to j of the Act on Electronic Signatures (e-signatur-loven) [2]. The name structure and certificate content must follow "Recommended certificate profiles for person certificates and enterprise certificates" [10]. The certificate must contain the organisation number of the enterprise.	• Access control to private keys must be realisable. • The enterprise must have scope for choosing/deciding him/herself whether each operation involving private keys is to be approved. • Private keys must as a minimum be stored in encrypted form.

The following certification service providers issues certificates at the following security levels[23]:

- Buypass AS	Person-Høyt and Enterprise
- Commfides Norge AS	Person-Høyt and Person Standard
- Zebsign AS	Person-Høyt, Peson-Standard and Enterprise

The table below shows the intended use of the various types of certificates:

[23] According to the web-page of the Norwegian Post and Telecommunication Authortiy, 18 June 2007 – www.npt.no (http://www.npt.no/portal/page/portal/PG_NPT_NO_NO/PAG_NPT_NO_HOME/PAG_SIKKERHET_TEKST?p_d_i=-121&p_d_c=&p_d_v=47268)



USES FOR CERTIFICATE LEVELS	Authentication	Signature (non-repudiation)	Receipt of encrypted information
Person-High	Transactions where there is a need for a high degree of certainty about the identity of the originator, for example in connection with access to particularly sensitive information or where the damage caused by a compromise would be extensive.	Transactions where there is a need for a high degree of certainty about the connection between content and the identity of the originator or where the damage caused by the compromising of the connection would be extensive.	Documents etc. containing particularly sensitive information or where the damage caused by a compromise would be extensive.
Person-Standard	Transactions where there is a need for a reasonable degree of certainty about the identity of the originator or where the damage caused by a compromise would be medium level.	Transactions where there is a need for a reasonable degree of certainty about the connection between content and the identity of the originator or where the damage caused by the compromising of the connection would be medium level.	Documents etc. that do not contain particularly sensitive information and where the damage caused by a compromise would not be extensive.
Enterprise	Transactions where there is a need for a high degree of certainty that the originator is/represents a specified enterprise or where the damage caused by a compromise would be	Transactions where there is a need for a high degree of certainty about the connection between content and the specified enterprise or where the damage caused by the compromising	Documents etc. containing particularly sensitive information or where the damage caused by a compromise would be

Common requirements for all three security-levels (unless expressly stated otherwise):

- The certificates shall follow "Recommended certificate profiles for person certificates and enterprise certificates”, unless these are not relevant to the certificate type. If other formats are used any deviations shall be documented (4.1.6)

- The certificates should support user-specified non-critical extensions of the fields. (4.1.10)

- For Personal-Standard and Enterprise storage of keys as encrypted PKCS # 12 objects should be permitted (4.3.4 and 4.4.5).

- The Supplier shall document whether the solutions for presenting and verifying signed data comply with the requirements in CWA 14171 (7.1)

- If the Supplier supplies a signature service, documentation shall be provided of whether the solution complies with the requirements and recommendations in CWA 14170 (7.2).

- All user dialogues, help text and instructions shall be available in the Norwegian language (8.1.1 – 8.1.3).

- What the user sees shall match what she signs. The way in which this principle is satisfied shall be documented (8.1.7).

- Sufficient documentation shall be provided to allow a programmer with general expertise but no knowledge of the interface to utilise it (8.2.2)

- The solution shall not tie the user to a single platform as regards for example operating system or web browser (8.3.1).

- The CSP shall specify the operating systems that the end user may use. This shall include versions and support for “thin Clients”. (Windows XP, Red Hat Linux, Citrixterminal server etc.) The solution shall as a minimum function on the three most commonly used operating systems for end-user environments (Windows, Linux and MAC). (8.3.3)

- Client interoperability (9.4)
  - Certificates should be available for running ”Microsoft Certificate Store”.
  - Operations with private keys should be available for applications using Microsoft CRYPTOAPI or PKCS#11.
  - The S/MIME format shall be used for encrypting e-mail.
  - The solution should support SSL Client certificates.

There are features that are optional pursuant to the Requirements Specifications, i.a. timestamping, notarisation and long term storage beyond 10 years.

For further information on technical aspects please refer to the appended “Requirement Specification for PKI for the public service” (version 1.02 – January 2005) for general requirements. These requirements can be met in various ways, to see how this is done by the certification service providers in more detail please refer to www.npt.no with links to the providers’ certificate policies.[24] The relevant certification policies are appended this questionnaire.

3.3.4 Organisational aspects

The organisation of public services is undergoing a reform to ensure efficient and secure exchange of information, and to increase the number of services available that requires any form of authentication.

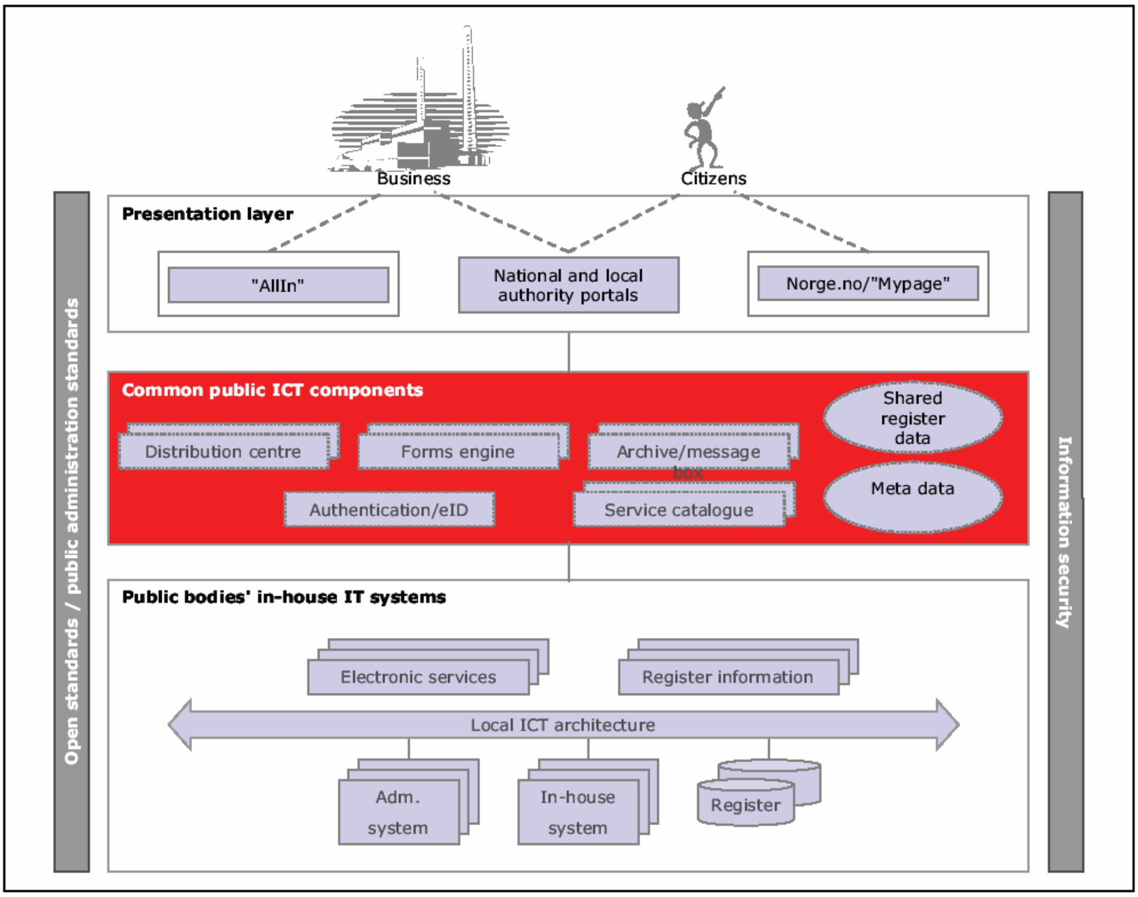
Identification of the citizen is primarily based on his personal identification number. Use of this number is strictly monitored, and subject to prior approval. The same number is i.a. also used by banks and financial institutes to establish the identity of a new client.

3.4 Interoperability

In accordance with the linear responsibility principle, each individual public body is responsible for establishing and developing its own ICT infrastructure in those areas where the public body finds this appropriate. The linear responsibility principle ensures that quality is increased for ICT-based procedure and service provision within each individual sector/enterprise, but poses challenges in terms of the interaction between sector-based and

[24] Cf. link http://www.npt.no/portal/page/portal/PG_NPT_NO_NO/PAG_NPT_NO_HOME/PAG_SIKKERHET_TEKST?p_d_i=-121&p_d_c=&p_d_v=47268

enterprise-based ICT solutions. The Ministry of Government Administration and Reform has a coordinating mandate for the ICT area, but this is limited.



Common ICT architecture in the public sector.

Pursuant to the Requirements Specifications for PKI for the Public Sector (chapter 9.1) the providers offering Personal-High, Personal-Standard and Enterprise authentication shall be prepared to contribute solutions that will secure interoperability with all suppliers delivering solutions based on this requirements specification. This will as a minimum entail that:

- The application using PKI for authentication and signature needs to use no more than a single Integration Module.
- It is possible to search, validate and utilise certificates issued by several CAs by means of this one Integration Module.
- It is possible to validate signatures based on certificates from several CAs with the aid of this one Integration Module.
- A single agreement can be established to regulate responsibilities and financial factors.

The Requirements Specifications for PKI for the Public Sector states the following:

”Interoperability to be understood in the following context:

> *’Interoperability entails that a certificate recipient (e.g. a user site) wishing to validate a certificate/signature and needing to use certificates from several different issuers shall be able to do so with the aid of solutions that are as expedient as possible for all parties involved.’*

Solutions in this context will entail technical interoperability between the systems of various suppliers and with the systems implemented by a user site, both internally and, if applicable, with end users. Moreover, this entails commercial relationships (agreements) between suppliers and user sites, and between suppliers.

Interoperability will be expected between the suppliers of certificate services used by the public sector, in communications with users and internally. Suppliers shall fulfil the requirements provided for in this specification. Applicable suppliers will either conclude a joint framework agreement with the public sector or be approved for communications with the public sector. In the event of renewals of or announcements of new tenders for the applicable framework agreements or new approvals, new players in the market will have to fulfil the interoperability requirements. Existing suppliers with operational solutions for interoperability will then be expected to make the appropriate arrangements to accommodate this.

The general intentions of the commercial and technical interoperability requirements are:

- *The individual certificate holder should have to relate to as few solutions as possible.*
- *Applications utilising PKI-functionality should have to interact with the minimum number of software modules possible. There should primarily be one single interface: with the PKI supplier with which the user site has an agreement.*
- *The user site should preferably have a single contract partner only.*
- *Competition in the market shall be stimulated.*

The following comments apply to the term “expedient solutions” (see the definition of interoperability above) for interoperability with the public sector:

- *Simplicity:*
  - *The certificate holder shall have to relate to a maximum of one solution per security level.*
  - *The user site shall have to interact with no more than one integration package.*
- *Cost effectiveness:*
  - *It shall be more beneficial in financial terms for the user site to have an interoperability solution than to have individual deliveries from two or more suppliers.*
  - *Cost levels shall be predictable.*
- *Justifiable in commercial terms.*
  - *The certificate holder should have to relate to no more than one contract partner (per security level)*
  - *The user site should have to interact with no more than one contract partner.*
  - *Factors relating to liability, responsibility, rights and obligations on the part of the contract parties in question shall as a minimum be equally well safeguarded with an interoperability solution as with individual agreements.”*

The focus regarding interoperabililty has been mainly a focus of achieving that on a national level. However, there is an ongoing debate in the Government also to achieve interoperability on an international level, i.e. within the EU/EEA. This applies inter alia to the regulations on public procurement, where there is a ongoing project to try to achieve a full scale interoperability covering all EU/EEA.

3.5 eIDM Applications

Cf. above and the presentation of the different eIDM systems for eGovernment services. The Norwegian government has encourage the roll out- of eIDs in the private sector (especially on the high security level), with the aim that these solutions/eIDs also can be used in eGovernmental services.

Several private certificate service providers have already been mentioned. To this it would be appropriate to also mention the BankID. BankID is a solution for authentication and signing on the Internet. It is offered by the banks in Norway and is based on a co-ordinated infrastructure that is developed through the BankID Co-operation, lead by the Norwegian Financial Services Association[25] and the Norwegian Savings Banks Association[26]. Many banks have registered their BankID as a qualified certificate pursuant to the Act on Electronic Signature. The Norwegian Post and Telecommunications Authority, appointed as the surveillance authority pursuant to the Act on Electronic Signatures, has accepted a solution for BankID where the certificate is centrally stored. This solution has been accepted provided that it is ensured that only the holder has access to the private key and it is only the provider that may make use of the key. This means that the certification service provider shall not have access to the private key or the possibility to make a copy of it. Should the private key be compromised, lost etc., the eID can no no longer be used but has to be revoked. Bank ID is used by eGovernmental services, i.a. in municipalities, and in the private sector offering eCommerce services in a B2C solution.

As already mentioned the Government entered into an agreement on security portal services with a commercial supplier in 2005. But due to the fact that many of the most relevant suppliers wanted to offer their services directly to the individual national bodies and municipalities, the agreement was terminated in 2006. One of these suppliers was the BankID-conglomerate.

Due to the failure to achieve a success with such an aim, the Government is now planning on issuing a national ID-card, with an eID. It is explicitly stated in the draft documents that this national ID-card/eID shall also be usable in the private sector; just as the solutions in the private sector, as far as possible, can be used in eGovernmental services. This cross use between the private and public sector will (in principle) only apply to PKI-based eIDs.

[25] http://www.fnh.no/FullStory.aspx?m=708

[26] http://www.sparebankforeningen.no/index.gan?id=797&subid=0

3.6 Future trends/expectations

It should be noted that there is a trend to regulatory bodies that open up for the use of eID/electronic signature to refer to the regulations of 21 November 2005 no. 1296 on a voluntary self-declaration scheme for certification service providers, and the three different types of eID – Person-High, Person-Standard and Enterprise – as further defined in the "Requirements Specification for PKI for the public sector".

As an example the following regulations have a direct reference to the above-mentioned regulations:

- The Regulations of 3 May 2007 no. 476 on a test project on electronic communication with regard to title registration of real estate[27]
- The Regulations of 15 June 2001 nr. 616 on public procurement[28]

This will promote the limitation of security level – issued by public or private entities - and will probably make it easier to achieve interoperability, together with the establishment of a joint security portal for the entire public sector.

The upcoming (probably) national ID-card might very well become the standard for authentication services in eGovernment processes, but only insofar that private eID solutions on the same security level will be accepted in parallel.

In order for the national ID-card to become a success the Norwegian government will have to look on how to extend the functionality of the eID card, especially by encouraging further private sector uptake.

The integration of other existing identification mechanisms (such as the driver's licence) into the eID card is presently a non-issue.

[27] Forskrift 3. mai 2007 nr. 476 om prøveprosjekt for elektronisk kommunikasjon ved tinglysing, § 4

[28] Forskrift 15. june 2001 nr. 616 om offentlige anskaffelser

3.7 Assessment

3.7.1 Advantages:

- There are many good eGovernment solutions, and some services are highly used (filing of tax return) as well as services for special groups (businesses' use of Altinn). This is an indicator that there exists an interest to communicate with the government electronically, provided there is a functioning eID solution.

- The roll out of a national ID card (eID) that is a multi-functional card, also available to non-nationals living in Norway, can facilitate the wish to obtain an increased use of eID on a higher security level.

3.7.2 Disadvantages:

- There are many different authentication solutions used in eGovernment services today, and it will take time before a wholly homogeneous use of authentication solutions is in place.
- There is a need of a stronger co-ordination from the relevant ministries.