eID Interoperability for PEGS

NATIONAL PROFILE DENMARK

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 Danish 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 most significant eIDM system in Denmark is the Danish OCES digital signature based on the OCES standard. OCES is the Danish designation for Public Certificates for Electronic Services ("*Offentlige Certifikater til Elektronisk Service*"). OCES digital signatures are advanced electronic signatures under the notion of the eSignature directive. They are software-based with enforced password-protection, in order to ensure "sole control".

The OCES standard is closely linked to the Danish Central Personal identification number. The personal identification number is a unique identification number for Danish citizens. The personal numbers of all Danish citizens are stored in the CPR-register (a national central register containing information of name, address and register number of all Danish citizens). The legal framework for the use of the personal identification numbers and other information of the CPR-register is laid down in the Act on the Civil Registration System[3].

The Act states that all Danish citizens are provided with a personal identification number. The personal identification number may be handed over to public authorities in compliance with the Danish Act on processing of personal data. Private parties are in general not entitled to request personal identification numbers from the CPR-register. Public authorities who are in possession of personal identification numbers are not entitled to make the personal identification numbers publicly available. CPR numbers are used for identification in all of the public sector and the finance sector.

When applying for an OCES certificate the identity is validated by look-up in the CPR-register and extraction of the person's registered postal address, to which a pin code is sent.

Alternative tokens include the social security card (*sygesikringsbevis*), private sector issued certificates (either software certificates or smart card based), and an identity card for kids under 16. None of these are eID tokens.

Identification information with regard to legal persons is stored in the so called CVR-register (central business register), which identifies legal persons (and natural persons – entrepreneurs) by the so called enterprise (CVR) number.

All of these systems will be discussed in greater detail below.

From a practical perspective, usage and uptake can be summarised as follows:

[3] Consolidation Act no. 140 of 3. March 2004 with later amendments. Available in Danish from http://147.29.40.90/_SHOWF_A775329798/919&A20040014029REGL&0001&000001

eIDM system	Potential user base	Actual penetration	Actual use
OCES digital signature	Estimated at 4 million (around 80% of the population)	Estimated at 800.000 (around 20% of the potential user base)	Public statistics are difficult to get as the usage can not be monitored centrally. There are over a 100 public services though and statistics from central services show a constant increase in usage.
Sygesikringsbevis	Estimated at 4 million	The social security card is distributed to all citizens over 16 years	Only for health purposes.

As a further step in building out the Danish eID infrastructure a public sector federation has been created with the aim of supporting the delivery of existing and new services to citizens and businesses in an integrated manner.

The federation will have its first service – a single signon solution based on the SAML 2.0 standard – in operation in first half of 2008. An important customer to this service is the Danish Citizens Portal that will be upgraded with a citizens individual "My Page" in 2008.

The federation is being established according to a development plan with the following five phases:

Web SSO
Support for Authorisation by proxy and Consent
Government-to-Government SSO, beyond Web
Federated Provisioning
Analysis of feasibility of authorisation using common roles

While the underlying federation architecture can support different authentication credentials and mechanisms, the backbone credential that citizens and employees can use to login to the federation is the OCES Digital Signature.

The underlying federation standard is SAML 2.0. Denmark has created its own SAML 2.0 profile mainly to restrict the various choices in SAML 2.0 and to describe cultural aspect like naming of special Danish attributes. Denmark is participating in efforts in the eGovernment special interest group in Liberty Alliance to define a common eGovernment SAML 2.0 profile.

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

As in other countries the use of eGovernment solutions has rather high political attention in Denmark due to the expected cost savings and citizen service improvements. Several Danish eGovernment applications have been developed in the last years and the number continues to increase. The eGovernment projects are normally vertically integrated, i.e. within the same area of competence, such as tax or social security. EGovernment projects are carried out on a federal, regional or local level.

- Federal eGovernment

Federal eGovernment projects are initiated by Ministries, organisations under Ministries or other federal bodies. The field is coordinated by the Danish Digital Taskforce and a steering committee established under the National eGovernment initiative. Further information about the national eGovernment initiative is found on its website www.e.gov.dk. On this site the initiative is presented in the following way:

"The Danish eGovernment initiative has been initiated by the central government and the regional and local administrations in order to promote and coordinate the transition to eGovernment in the public sector. The Project was from 2001-2005 led by a joint board made up of the permanent secretaries from five ministries, the managing directors of Local Government Denmark and The Danish Regions representing the municipal and regional authorities, respectively, and finally a representative from the municipalities of Copenhagen and Frederiksberg.

The Ministry of Science, Technology and Innovation has the main responsibility for infrastructure supporting the eGovernment initiatives.

In December 2005 the joint board was replaced by the "Steering Committee for joint cross-government co-operations". The Steering Committee is served by the Digital Task Force, which is based in the Ministry of Finance.

The guiding idea behind Project eGovernment is that the responsibility for the implementation of eGovernment lies at the decentralised level, but that in several cases, there can be a need for common guidelines and solutions to general problems of a legal, technical, and organizational nature in order to support the transition process. The need for a cross-level effort was stressed in a whitepaper on eGovernment published in May 2001, and the project was agreed on in the annual negotiations with the regional and municipal authorities in June 2001".

The OCES digital signature was one of the projects initiated by the "Steering Committee for joint cross-government co-operations" and is established within the framework of the Ministry of Science, Technology and Innovation.

Likewise is the formation of the Danish public sector federation initiated by the "Steering Committee for joint cross-government co-operations". The federation organisation is hosted by

the Danish Agency for Governmental Management in a collaboration where the Danish National IT and Telecom Agency is responsible for the architecture and standards in the federation..

- Regional eGovernment

After a restructuring reform of the municipalities and regions Denmark consists of 5 regions and app. 100 municipalities (as of January 1, 2007).

The main working area of the regions is the health care sector, including responsibility for the public hospitals. Through their organisation Danish Regions (www.regioner.dk), the regions are running a national healthcare portal (www.sundhed.dk) which includes a number of applications, see section F.

- Local eGovernment

A number of local eGovernment applications are offered by the Danish municipalities. Many of these applications are used by a large number of municipalities and provided through the website www.netborger.dk. This website is owned by the organisation KL which is the organisation of the municipalities (www.kl.dk). The applications of the website are developed and operated by KMD (www.kmd.dk) which is a Danish IT company owned by the municipalities through their organisation KL. KMD is operating on market terms, but has a very strong position in the Danish market for municipality IT-services and applications. As of January 1st 2007 a central entrance to public eGovernment services has been established: www.borger.dk; subsequently all the services mentioned in this paragraph will be available through this portal. From January 2008 a "My Page" will be accessible to all citizens with access via digital signature based on the OCES standard.

In general the OCES signatures and the National eGovernment Initiative provides for a relatively high level of coordination and corporation in the work with Danish eGovernment applications using digital signatures.

3.2.2 National eGovernment cooperation and coordination

See 10.2.1 for information about the national eGovernment cooperation and coordination

3.2.3 Traditional identity resources

Identification towards Danish eGovernment services traditionally relied mostly on the central National Register, which was centralised and digitalised in the beginning of the 1960's. See above for description.

Denmark has no tradition for an identity card of any kind, but has used a combination of the social security card "*sygesikringsbevis*" and driver's license or passport or banking cards.

The National Register contains information for all Danish persons and for persons with residence permit in Denmark. Persons with residence permit are issued a personal identification number along with their permit. The register contains information of the personal identification number, name, address, birth registration, citizenship, relations to the national church, kinship, and marital status. Every day the central National Register is being updated by the local population registers, which have information of citizens living in their municipality. The local population registers receive their information from relevant authorities, such as i.e. the church office or the social authorities. The National Register has a long tradition and population registration was already initiated around 1910. By law citizens are obliged to report to the local population register any change of address and this information is also supplied by local authorities. The information in the central register is therefore very accurate and relied upon by public authorities.

Identification information with regard to legal entities is registered and stored in the so called CVR-register (central business register), which identifies legal persons (and natural persons – entrepreneurs) by the so called enterprise (CVR) number.

The Central Business Register (CVR) is the central register containing primary data on all businesses in Denmark, regardless of economic and organizational structure. CVR also covers both public and private businesses.

In addition, CVR contains detailed information on all limited companies, including fiscal reports, management and financial information and status, etc. All this information is available for purchase and download from the CVR-register website www.cvr.dk.

The CVR register is administered by the Danish Commerce and Companies Agency (DCCA) www.eogs.dk.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

In order to support the strategy of creating an effective and coherent public sector with a high quality of eGovernment and eGovernment services the need for an easily disseminated, publicly recognized digital identity resulted in the development of the OCES standard (Public Certificates for Electronic Services).

The OCES project was established within the framework of the Ministry of Science, Technology and Innovation. Its main aim was to create a public standard for digital signatures and an open, scalable and transparent PKI infrastructure and thus promote the use of digital signatures in Denmark.

In order to issue OCES certificates, a CA must enter into an agreement with the National IT and Telecom Agency (www.itst.dk). In this agreement, the CA undertakes to comply with the terms of the certificate policies drawn up by the Agency. In this connection, the CA undertakes to submit an annual report to the National IT and Telecom Agency. The report implies an external system audit of the CA. The terms governing the annual report have been drawn up on the same principles as those appearing from the Act on Electronic Signatures. At the moment an agreement exists with TDC (largest Danish Telecom provider and operator) as a CA issuing OCES signatures.

In addition to setting the framework for proper operation of the CAs, the certificate policies for OCES digital signatures constitute the basis for a Danish standardised certificate that will ensure interoperability between CAs.

The National IT and Telecom Agency is responsible for drawing up and maintaining the OCES certificate policies. See English version at www.signatursekretariatet.dk/certifikatpolitikker.html.

In preparation for the establishment of an infrastructure for digital signatures, the Ministry of Science, Technology and Innovation entered into a contract with TDC as CA in early 2003. Among other things, this contract signifies that:

- citizens in Denmark can obtain digital signatures free of charge (financed by the government for public authorities)
- employee certificates are issued (financed by the government for public authorities)
- corporate certificates are issued
- public authorities may obtain digital signatures on favourable terms
- public authorities can look up in the CPR-register free of charge via a conversion of PID-numbers to CPR numbers.

All subscribers and service providers must agree to the CP terms and conditions when subscribing. The business model is based on a flat rate receiver payment model, which constitutes ca. 0,5-1€ per certificate per year.

The contract with TDC expires in June 2008 and at the moment an EU-tender for the continuation of the digital signature is being prepared. At the moment there are no plans to use eID cards, but some form of hardware token will eventually be implemented for the OCES digital signature in order to fulfil some of the emerging security and mobility demands. This development is pending the EU-tender.

The OCES certificate policies create a common standard for the content of the OCES certificates, thus all applications receiving OCES certificates can follow the common standards specified in the certificate policies. The certificate policies specify content of the certificates in detail, so an application can depend on predefined content. Moreover procedures for revocation, publication of certificate revocation lists and other technical procedures are being described in the certificate policies. Therefore most eGovernment applications are now developed to support authentication by OCES certificates. The process of identifying oneself is perceived by the user to be identical, no matter which eGovernment application the user accesses. Also private companies can implement web services using the OCES standard.

In preparation for a flexible federation a policy regarding levels of authentication has been created, and confirmed as a public sector recommendation in 2005 following a public hearing.

The policy is adopted from the US Government *E-Authentication Guidance for Federal Agencies*[4]. It establishes and describes the following four levels of identity assurance for electronic transactions requiring authentication:

Level 1: Little or no confidence in the asserted identity's validity.

Level 2: Some confidence in the asserted identity's validity.

Level 3: High confidence in the asserted identity's validity.

Level 4: Very high confidence in the asserted identity's validity.

3.3.2 Legal framework

The legal framework of the OCES concept consists of an agreement between the CA and the National IT and Telecom Agency. The three OCES CPs are part of this agreement. In order to issue OCES certificates, a CA must enter into an agreement with the National IT and Telecom Agency. In this agreement, the CA undertakes to comply with the terms of the certificate policies drawn up by the Agency. In this connection, the CA undertakes to submit an annual report to the National IT and Telecom Agency. The report implies an external system audit of the CA. The terms governing the annual report have been drawn up on the same principles as those appearing from the Act on Electronic Signatures. At the moment an agreement exists with TDC (largest Danish Telecom provider and operator) as a CA issuing OCES signatures.

The requirements of the CPs are very similar to the requirements of the Danish Act on electronic signatures (which transposes the eSignature Directive into Danish law). An important difference concerning liability is that the CA within the OCES concept has the possibility to limit its liability in the relationship that exists between the CA and its contracting parties to the extent that such joint contracting parties are business operators or public authorities, but not at all in relation to private people as contracting parties.

OCES digital signatures are advanced electronic signatures under the notion of the eSignature directive. They are software-based with enforced password-protection, in order to ensure "sole control".

3.3.3 Technical aspects

OCES digital signatures can be issued as personal certificates, company certificates and employee certificates. Accordingly three certificate policies (CP) exist. The CPs have been translated into English and can be downloaded from https://www.signatursekretariatet.dk/certifikatpolitikker.html

[4] The US policy regarding E-Authentication Guidance for Federal Agencies is communicated in memorandum M-04-04 from the Office of Budget and Management, December 16, 2003

The CPS from the OCES TDC-CA can be obtained from http://www.certifikat.dk/repository/TDCCPS40.pdf

OCES digital signatures are software-based digital signatures. They can also be obtained on hardware (such as eToken or smart cards). No matter the media, the issuing refers to the same certificate policy.

In the OCES framework there is only one level in the hierarchy, due to the fact that the root key of the OCES-CA signs all certificates. The OCES CA has been webtrusted and therefore the root certificate has been included in both Microsoft's and Mozilla's certificate store for trusted authorities.

On a technical level the OCES certificates comply with the ETSI TS 101 862, X509v3, RFC 2459 and RFC 3039 specifications. The CPs require the certificates to follow the Danish specification for qualified certificates (DS 844) (Qc statements in the certificate cannot specify that the certificate is qualified, though).

The policy OID field specifies a unique identification of the CP under which a given certificate has been issued. The policy OID is found in the field 'certificatePolicies' in the Certificate. In order to distinguish different certificate types from one another, the application can parse on the policy OID field.

The subject certificate field specifications can be seen in detail in the relevant CP for personal-, employee- and company-certificates in section 7.3.3. (https://www.signatursekretariatet.dk/certifikatpolitikker.html)

Note that the serial number field for personal certificates contains a person specific identification number (PID), which uniquely refers to a person's central personal identification number. Conversion can be achieved through a CA service, which maps the PID and CPR numbers and which is accessible only to authorities that by law are entitled to use the CPR or by explicit consent given by the certificate holder.

The CA offers a special web-service, where the PID-nr in the certificate-field can be converted to the certificate holder's central personal number (CPR). This service is only available for public authorities or if the certificate holder explicitly has given his consent.

In employee certificates the serial number field contains the concatenation of the company's central business number and an employee identification number. The concatenation is used by digital signature related applications to uniquely identify an employee in a given company.

For company certificates the serial number field contains the company's business registration number, which can be concatenated with different qualifiers, denominating different departments in the company. These numbers can be used by applications to uniquely identify a given company or department of a company.

Applications receiving OCES certificates follow the standards specified in the certificate policies. The certificate policies specify content of the certificates in detail, so an application can depend on predefined content. Moreover procedures for revocation, publication of certificate revocation lists and other technical procedures are being described in the certificate policies.

An Open Source component (OpenSign/OpenLogon – www.openoces.org) has been developed. The component offers client side login and web-signing functionalities.

The OCES-CA has published a number of technical documents and best practices on how OCES certificates are "examined" in terms of content and semantics, as well as how the integration with CA certificate related services can be achieved.

A digital signature is verified directly through the corresponding CA validation service through different validation protocols.

In terms of storage of the signature verification result, a recommended "standard" for "proof of validation" has been developed in order to maintain evidential value of digital signature based transactions.

The standard requires certain data to be logged and stored in the validation process, such as:

- Time of signature verification
- Result of signature verification:
  - Indication that the signature was valid at the time of reception
  - Indication that the digital signature associated data is unchanged
- Time of reception
- State of encryption
- Unique identification of the signature holder (subscriber):
  - In terms of OCES personal certificates the PID-nr is considered sufficient identification
  - In terms of OCES employee- and company certificates the SerialNumber and CommonName fields are considered sufficient identification.

The standard was initially developed for secure e-mail validation at gateway-based central solutions, but also serves as inspiration for web-based applications and services.

At the moment CRLs are the main supported validation method. An OCSP-service is also available.

3.3.4 Organisational aspects

As mentioned above, a private CA that has an agreement with and has been approved by the National IT and Telecom Agency issues OCES digital certificates. Other CAs could enter into such an agreement, be approved and thus issue OCES certficates.

See above for detailed description.

All Danish citizens can apply for an OCES digital signature via the website of the CA. There is no charge to have an OCES digital signature as the Danish government pays the expense through the commercial contract described above.

3.4 Interoperability

As mentioned above the validation of the identity is based on the national central personal register. Thus only citizens with a CPR number can get an OCES digital signature. A foreigner with permanent residence in Denmark will be issued with a CPR number and can therefore have an OCES signature. Also a Danish person living abroad can have a digital signature, but only if the person has a CPR number and a Danish Passport containing this number.

A procedure for the possibility for non-nationals living outside of Denmark to have an OCES signature has not yet been developed; there is however a need, so eventually this issue will be addressed.

Technically it is possible for a service provider in another country that supports the SAML 2.0 standard to be part of the Danish federation and to receive an assertion of authentication based on the user logging in with OCES Digital Signature. However, it has not been analyzed which agreements, user mapping capabilities etc. would be needed to make this work for real-life solutions.

3.5 eIDM Applications

Electronic services for OCES digital signatures include:

Log-on with digital signatures:
- 5 pensions fond
- 90 public authorities - more than 150 services
- 25 private companies

Implemented Employee signatures:
- 22 public administrations

Secure e-mail:
- 400 public authorities
- 20 private companies

Examples of electronic services using digital signatures:
- Sundhed.dk – the public sector's health portal

- The National Tax Authority
- The State Education Fund
- The City of Copenhagen
- Borger.dk – A portal for citizen used by all local authorities
- TDC On-line – online telecom resource (potential 700,000 users)
- "danmark" – the private Danish health insurance company (1.7 million customers)
- "Virk.dk" – the common public sector portal for companies (potential 250.000 companies)
- ATP - the Danish supplementary labour market pension fund (1.9 million customers)
- The Ministry of Education: Central Education Admission Portal (60,000 people per year)
- "Eboks" private electronic mailbox

Danish key applications are described in detail in the IDABC Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications.

The Danish public sector federation expects to have approximately 25 service providers with a larger number of applications in production in 2008. Some of the applications will be existing applications that support OCES Digital Signature today while others will be new applications that do not develop their own login-functionality (beyond what is needed for emergency backup)

3.6 Future trends/expectations

A tender for the next generation digital signature in Denmark is about to be launched as the contract with the present CA (TDC A/S) expires in June 2008. An analysis on possibilities for the continuation and development of the OCES concept has been carried through and recommendations for tender requirements have been defined. Tender announcement is expected in May 2007.

3.7 Assessment

The Danish approach has a number of advantages and challenges, which can be briefly summarised as follows.

3.7.1 Advantages:

- Roll-out is fairly smooth and very cost-effective as there is no requirement for physical presence and no requirements for special hardware or software;
- There is no cost for the user;
- A common standard encourages easy and cost-effective development of eGovernment services.

3.7.2 Challenges:

- It takes time to establish an open infrastructure on a large scale for digital signatures and to get people to use it;
- Electronic services which add value for the user are the drivers for the rollout of digital signatures;
- It is important to get the private sector involved;
- Public/private partnerships are important for development;
- Accessibility to non-nationals: the Danish system is largely built for Danish nationals and residents in Denmark with a need to interact with the Danish public authorities. To increase interoperability the question of how to identify people on a European level must be analysed;
- In order to maintain trustworthiness, the OCES digital signature must constantly be upgraded and developed to meet new security threats;
- Creating mobility for the digital signature;
- The more practical use of digital signatures, the more need for development of additional interfaces and services from the CA;

It is in general hard to establish a business case for the development of a PKI-infrastructure, thus public subsidising is necessary. After a slow start for the OCES-project the rollout rate at the moment is now satisfactory, but new value-adding services must continuously be developed in order to create and maintain a market for digital signatures.

The largest challenge with regards to international interoperability lies in trust between issuers, unique identification of subscribers as well as content and semantics of certificates.