



# Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications

## NATIONAL PROFILE DENMARK

April 2007



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

Author's name: Henrik Udsen, Copenhagen University

Company's name: Siemens - Lawfort

Company's address (optional):

Company's logo (optional)

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

## **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/6485/5938>

© European Communities, 2007

Reproduction is authorised, except for commercial purposes, provided the source is acknowledged.

## **Executive summary**

The objective of the project is to analyse the requirements in terms of interoperability of electronic signatures for different eGovernment applications and services taking into account the relevant provisions of Directive 1999/93/EC on a Community framework for electronic signatures and their national implementation as well as the report on the Directive and the standardisation activities on the interoperability of electronic signatures.

This document does represent the current situation regarding the use of eSignatures in Danish eGovernment applications.

## Table of Contents

<b>EXECUTIVE SUMMARY</b>	<b>3</b>
<b>TABLE OF CONTENTS</b>	<b>4</b>
<b>1 DOCUMENTS</b>	<b>5</b>
1.1 APPLICABLE DOCUMENTS	5
1.2 REFERENCE DOCUMENTS	5
<b>2 GLOSSARY</b>	<b>5</b>
2.1 DEFINITIONS	5
2.2 ACRONYMS	5
<b>3 INTRODUCTION</b>	<b>5</b>
<b>4 EGOVERNMENT AND ESIGNATURE REGULATIONS</b>	<b>5</b>
4.1 ESIGNATURES REGULATORY FRAMEWORK	5
4.2 EGOVERNMENT REGULATORY FRAMEWORK	5
4.2.1 OCES	5
4.2.2 PERSONAL IDENTIFICATION NUMBER	5
<b>5 EGOVERNMENT APPLICATIONS USING ELECTRONIC SIGNATURES</b>	<b>5</b>
5.1 PUBLIC PROCUREMENT	5
5.1.1 ETHICS	5
5.1.1.1 Application identification	5
5.1.1.2 eSignature details	5
5.1.1.3 Interoperability	5
5.1.1.4 Miscellaneous	5
5.1.2 ASSESSMENT	5
<b>5.2 TAX 5</b>	
5.2.1 TASTSELV BORGER - PERSONAL INCOME TAXES DECLARATIONS	5
5.2.1.1 Application identification	5
5.2.1.2 eSignature details	5
5.2.1.3 Interoperability	5
5.2.1.4 Miscellaneous	5
5.2.1.5 Assessment	5
5.2.2 TASTSELV ERHVERV – VAT AND OTHER COMPANY TAX DECLARATIONS AND PAYMENTS	5
5.2.2.1 Application identification	5
5.2.2.2 eSignature details	5
5.2.2.3 Interoperability	5

5.2.2.4	Miscellaneous	5
5.2.2.5	Assessment	5
<b>5.3</b>	<b>HEALTH CARE</b>	<b>5</b>
5.3.1	SUNDHED.DK – THE NATIONAL HEALTH CARE PORTAL	5
5.3.1.1	Application identification	5
5.3.1.2	eSignature details	5
5.3.1.3	Interoperability	5
5.3.1.4	Miscellaneous	5
5.3.1.5	Assessment	5
<b>5.4</b>	<b>FINANCE</b>	<b>5</b>
5.4.1	VIRK.DK	5
5.4.1.1	Application identification	5
5.4.1.2	eSignature details	5
5.4.1.3	Interoperability	5
5.4.1.4	Miscellaneous	5
5.4.1.5	Assessment	5
5.4.2	WEBREG.DK - REGISTRATION AND CHANGE OF COMPANY INFORMATION	5
5.4.2.1	Application identification	5
5.4.2.2	eSignature details	5
5.4.2.3	Interoperability	5
5.4.2.4	Miscellaneous	5
5.4.2.5	Assessment	5
5.4.3	NEMKONTO	5
5.4.3.1	Application identification	5
5.4.3.2	eSignature details	5
5.4.3.3	Interoperability	5
5.4.3.4	Miscellaneous	5
5.4.3.5	Assessment	5
<b>5.5</b>	<b>JUSTICE</b>	<b>5</b>
5.5.1	ELECTRONIC REGISTRATION OF PROPERTY	5
5.5.1.1	Application identification	5
5.5.1.2	eSignature details	5
5.5.1.3	Interoperability	5
5.5.1.4	Miscellaneous	5
5.5.1.5	Assessment	5
<b>5.6</b>	<b>LOCAL APPLICATIONS</b>	<b>5</b>
5.6.1	NETBORGER.DK	5
5.6.1.1	Application identification	5
5.6.1.2	eSignature details	5
5.6.1.3	Interoperability	5
5.6.1.4	Miscellaneous	5
5.6.1.5	Assessment	5

5.6.2	E-BOKS	5
5.6.2.1	Application identification	5
5.6.2.2	eSignature details	5
5.6.2.3	Interoperability	5
5.6.2.4	Miscellaneous	5
<b>6</b>	<b><u>GENERAL ASSESSMENT</u></b>	<b>5</b>
<b>7</b>	<b><u>OPERATIONAL AND PLANNED APPLICATIONS</u></b>	<b>5</b>
7.1	APPLICATIONS AT THE FEDERAL LEVEL	5
7.2	APPLICATIONS AT THE REGIONAL LEVEL	5
7.3	APPLICATIONS AT THE LOCAL LEVEL	5
<b>8</b>	<b><u>ANNEX A: CONTACT DETAILS OF NATIONAL CORRESPONDENTS</u></b>	<b>5</b>
8.1	PRIMARY CONTACT	5
<b>9</b>	<b><u>ANNEX B: NATIONAL REGULATIONS DETAILS</u></b>	<b>5</b>
<b>10</b>	<b><u>ANNEX C: FILLED-IN QUESTIONNAIRES</u></b>	<b>5</b>
<b>10.1</b>	<b>ETHICS (eTENDER AND PROCUREMENT)</b>	<b>5</b>
10.1.1	APPLICATION IDENTIFICATION	5
10.1.2	eSIGNATURE DETAILS	5
10.1.3	INTEROPERABILITY	5
10.1.4	MISCELLANEOUS	5
10.1.5	ASSESSMENT	5
<b>10.2</b>	<b>TASTSELV BORGER</b>	<b>5</b>
10.2.1	APPLICATION IDENTIFICATION	5
10.2.2	eSIGNATURE DETAILS	5
10.2.3	INTEROPERABILITY	5
10.2.4	MISCELLANEOUS	5
10.2.5	ASSESSMENT	5
<b>10.3</b>	<b>NEMKONTO</b>	<b>5</b>
10.3.1	APPLICATION IDENTIFICATION	5
10.3.2	eSIGNATURE DETAILS	5
10.3.3	INTEROPERABILITY	5
10.3.4	MISCELLANEOUS	5
10.3.5	ASSESSMENT	5
<b>10.4</b>	<b>SUNDHED.DK</b>	<b>5</b>
10.4.1	APPLICATION IDENTIFICATION	5
10.4.2	eSIGNATURE DETAILS	5
10.4.3	INTEROPERABILITY	5

10.4.4 MISCELLANEOUS	5
10.4.5 ASSESSMENT	5
<b>10.5 VIRK.DK</b>	<b>5</b>
10.5.1 APPLICATION IDENTIFICATION	5
10.5.2 ESIGNATURE DETAILS	5
10.5.3 INTEROPERABILITY	5
10.5.4 MISCELLANEOUS	5
10.5.5 ASSESSMENT	5
<b>10.6 NETBORGER.DK</b>	<b>5</b>
10.6.1 APPLICATION IDENTIFICATION	5
10.6.2 ESIGNATURE DETAILS	5
10.6.3 INTEROPERABILITY	5
10.6.4 MISCELLANEOUS	5
10.6.5 ASSESSMENT	5

## 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 <a href="http://ec.europa.eu/idabc/servlets/Doc?id=24769">http://ec.europa.eu/idabc/servlets/Doc?id=24769</a>
[RD2]	European Electronic Signatures Study <a href="http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl">http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl</a>
[RD3]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures <a href="http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf">http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf</a>
[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 <a href="http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf">http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf</a>
[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 <a href="http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_134/l_13420040430en01140240.pdf">http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_134/l_13420040430en01140240.pdf</a>
[RD6]	IDABC Work Programme Third Revision <a href="http://ec.europa.eu/idabc/servlets/Doc?id=25302">http://ec.europa.eu/idabc/servlets/Doc?id=25302</a>
[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 <a href="http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf">http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf</a>
[RD8]	
[RD9]	



## 2 Glossary

### 2.1 Definitions

In the course of this Questionnaire, 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.

- *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.

It should be noted that for the purposes of this questionnaire, only services which rely on eSignatures are relevant, and that the focus is on eGovernment applications offered to citizens and businesses (A2C and A2B, rather than A2A).

- *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. However, PKI solutions are the principal focus of this questionnaire, and non-PKI solutions should only be included if no PKI solutions are in common use. It should also be noted that the questionnaire only examines eGovernment applications in which the eSignature is used to sign a specific transaction, and not where the signature is merely used as a method of authentication of the eSignature holder as defined below.
- *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;
- *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<sup>1</sup>.

---

<sup>1</sup> See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML>

- *Authentication*: 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”). It should be noted that the questionnaire is focused on the use of eSignatures as a method of signing a transaction, and not on their use as a method for authenticating the eSignature holder.
  
- *Relying party*: any individual or organisation that acts in reliance on a certificate (in a PKI solution) or a eSignature.
  
- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

## 2.2 Acronyms

<b>A2A</b> .....	Administration to Administration
<b>A2B</b> .....	Administration to Businesses
<b>A2C</b> .....	Administration to Citizens
<b>CRL</b> .....	Certificate Revocation Lists
<b>eID</b> .....	Electronic Identity
<b>OCSP</b> .....	Online Certificate Status Protocol
<b>PKI</b> .....	Public Key Infrastructure
<b>SCVP</b> .....	Simple Certificate Validation Protocol
<b>SSCD</b> .....	Secure Signature Creation Device
<b>TTP</b> .....	Trusted Third Party

### 3 Introduction

As in other countries the use of eGovernment solutions has a 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](http://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](#) represent 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 decentral level, but that in several cases, there can be a need for common guide lines and solutions to general problems of 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”.

One of the projects of the initiative was the establishment of a national digital signature solution to be used (not exclusively) in eGovernment solutions. This solution, called OCES (Offentlige certifikater til elektronisk service – public certificates for electronic services) digital signatures, is explained in details in section 4.2.1.

The OCES project is established within the framework of the Ministry of Science, Technology and Innovation.

- *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 organization Danish Regions ([www.regioner.dk](http://www.regioner.dk)) the regions are

running a national healthcare portal ([www.sundhed.dk](http://www.sundhed.dk)) which includes a number of applications, see further in section 5.3.1.

- *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 the municipalities and provided through the website [www.netborger.dk](http://www.netborger.dk) (see further section 5.6.1). This website is owned by the organisation KL which is the organisation of the municipalities ([www.kl.dk](http://www.kl.dk)). The applications of the website is developed and operated by KMD ([www.kmd.dk](http://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](http://www.borger.dk), subsequently all the services mentioned in this paragraph will be available through this portal. From Januar 2008 a "my page" will be accessible to all citizens with digital signature based on the OCES standard.

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

## 4 eGovernment and eSignature regulations

### 4.1 eSignatures regulatory framework

European Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures was transposed into Danish legislation through:

- Act no. 417 of 1 October 2000 on Electronic Signatures<sup>2</sup>;
- Executive Order no. 922 of 16 October 2000 on "Reporting of Information to the National Telecom Agency by CAs and system Auditors"<sup>3</sup>;
- Executive Order no. 923 of 16 October 2000 on "Security Requirements etc. for Certification Authorities"<sup>4</sup>;

The definitions of advanced and "qualified" electronic signature under Danish law are very close to the definitions of the European Directive. Advanced and "qualified" electronic signatures cannot be issued to legal persons under Danish law.

For further information of the transposition of the Directive into Danish law see [RD2].

The practical effect of the Danish eSignature Act has been disappointing as no "qualified" electronic signatures are being offered by certification service providers in Denmark. One of the main obstacles has been the requirement for signature holders to meet up and identify themselves in person. Realising that few people would do this the Government initiated the establishing of the above mentioned OCES standard. The OCES signature is a "light version" of the qualified electronic signature with the important difference that the holder of an OCES signature does not have to perform face to face identification. The OCES signature is widely supported by public authorities in their eGovernment solutions and is explained in detail below.

The OCES signature is not covered by the Danish eSignature Act as the OCES signature is not based on a qualified certificate. Neither is the OCES signature covered by any other general eSignature legislation (the eSignature Act focusing on "qualified" electronic signatures is the only general eSignature legislation under Danish law).

---

<sup>2</sup> See [http://147.29.40.91/SHOWF\\_B762442665/1072&A20000041730REGL&0001&000001](http://147.29.40.91/SHOWF_B762442665/1072&A20000041730REGL&0001&000001)

<sup>3</sup> See [http://147.29.40.91/SHOWF\\_B762442665/1072&B20000092205REGL&0002&000001](http://147.29.40.91/SHOWF_B762442665/1072&B20000092205REGL&0002&000001)

<sup>4</sup> See [http://147.29.40.91/SHOWF\\_B762442665/1072&B20000092305REGL&0003&000001](http://147.29.40.91/SHOWF_B762442665/1072&B20000092305REGL&0003&000001)

## 4.2 eGovernment regulatory framework

The legal basis for the introduction of electronic signatures in eGovernment applications can be found in various legislative provisions, specifically allowing the use of “electronic signatures”, “electronic signatures on same security level as OCES signatures” or “digital signatures”.

Furthermore the right to use electronic signatures may follow from a general right to use electronic documents. From 2002-2005 a large “law modernising project”<sup>5</sup> has been carried out by the government under the above National eGovernment Initiative to ensure that such formal requirements do not hinder the use of electronic documents except from the few situations where it has been considered necessary to require paper documents<sup>6</sup>. In addition to these changes of more specific provisions a new provision, § 32a, was inserted in the Administrative Act (*forvaltningsloven*)<sup>7</sup>. § 32a made it possible through administrative decrees to change rules on formal requirements if such rules were a barrier to the use of electronic communication. In this way it became possible to eliminate the legal barriers in a faster and more flexible way not having to go through the parliamentary process of adopting new legislation. In other words this provision allows easy adaptation of the existing legal framework.

Currently the OCES signature is by far the preferred eSignature solution by authorities providing eGovernment applications. The OCES signature will be explained in details below, before discussing how it has been implemented in a number of eGovernment applications. The role of the Personal Identification Number, one of the building blocks of the OCES signature, will also be explained.

### 4.2.1 OCES

In the below scheme the OCES signature is explained in more details. The scheme is based upon the standard application questionnaire (annex C). As many of the applications rely on OCES signatures the descriptions of the specific applications will make references to the OCES standard.

Responsible Organisation	
Organisation Name	<i>National IT and Telecom Agency</i>
Organisation Type	<i>Agency under the Ministry of Science, Technology and Innovation</i>

### Legal and strategically aspects

<sup>5</sup> See [http://www.e.gov.dk/offentlige\\_projekter/lovmodernisering/index.html](http://www.e.gov.dk/offentlige_projekter/lovmodernisering/index.html) (in Danish)

<sup>6</sup> The project was initiated base on recommendations given in report no. 1400, “e-signatur og formkrav i lovgivningen” drafted by a committee appointed by the Ministry of Justice.

<sup>7</sup> Act no. 571 of 19 December 1985. Available in Danish from [http://147.29.40.91/\\_SHOWF\\_A393870761/311&A20020105030REGL&0001&000001](http://147.29.40.91/_SHOWF_A393870761/311&A20020105030REGL&0001&000001)

<p>The registration (identification) process: how are natural and legal persons (and possibly other entities) identified</p>	<p><i>Natural persons: A person applies for a digital signature by entering personal identification number, postal code and e-mail address on the Certificate Authority's (hereafter CA) webpage. The CA checks the personal identification number in the central personal register and extracts the person's registered postal address, at the same time confirming that the postal code matches the entered postal code. A confirmation e-mail containing an activation link is sent to the specified e-mail address. At the same time a PIN-letter containing an activation-code, necessary for the activation and installation of the digital signature is sent to the registered postal address. Installation of the digital signature is possible by combining the activation link in the confirmation e-mail with the received activation code from the PIN-letter. Activation of the digital signature must happen within four weeks of the application, otherwise the signature is revoked.</i></p> <p><i>In order to boost dissemination of digital signatures, various online and real-time registration- and issuing processes have been added.</i></p> <p><i>Legal persons: A legal person applies for a digital signature by entering the company's business registration number on the CA's webpage. On the basis of this number, the CA retrieves the company name and postal address from the central business register. The applicant then enters the name and e-mail address of the person to be authorized to issue digital signatures for the company and its employees. Also the name of the person authorized to sign for the company must be appointed. The applicant must then print out and sign a contract with the CA regarding issuing of certificates for the company. The contract signed by the authorized person must be sent to the CA by letter or fax. After receiving the necessary document, the CA grants access to a Local Registration Application (LRA). An e-mail is sent to the person authorized to issue certificates, as well as a PIN-letter to the company postal address, containing an activation-code, as described above. Both the e-mail and activation-code are used to issue a certificate to access the LRA. Thereafter the authorized person can issue digital signatures to the company and its employees.</i></p> <p><i>The Certificate policy allows for the regular procedures for certificate applications to be partly or fully deviated from, if other secure procedures regarding identity checks are applied. In particular the above-mentioned online registration- and issuing procedures are examples of this.</i></p>
<p>The scope of the eSignature framework (only natural persons or also legal entities, only nationals or</p>	<p><i>The OCES signature framework applies to both natural and legal entities. OCES signatures can be issued as personal certificates, company certificates and employee certificates.</i></p>

<p>also non-nationals,...)</p>	<p>Accordingly three certificate policies (CPs) exist. The CP's have been translated into English and can be downloaded from <a href="https://www.signatursekretariatet.dk/certifikatpolitikker.html">https://www.signatursekretariatet.dk/certifikatpolitikker.html</a></p>
<p>The legal qualification of the signatures (simple signature, advanced or qualified, with explanations if these notions do not compare cleanly to the terminology of the eSignatures directive) and their validity</p>	<p>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". Company certificates are technically similar to other OCES certificates, but are issued to legal persons. Thus they cannot be referred to as advanced electronic signatures according to the definition of advanced electronic signatures under the Danish eSignature Act.</p>
<p>Rules regarding long term validity of the signatures (including storage of certificates, if any, and signatures)</p>	<p>OCES digital signatures are valid for up to four years and according to the requirements in the CP's, the CA is obliged to keep and be able to make archived information regarding the digital signatures available for a minimum of six years.</p>
<p>Rules regarding liability of the certificate issuer (if any), the service provider and the user</p>	<p>In relation to any person who reasonably relies on the certificate, the CA must assume liability for damages in relation to the general provisions of Danish law. In addition, the CA must assume liability for damages for loss incurred by subscribers and verifiers who have reasonably relied on the certificate, provided that the loss is due to one of the following:</p> <ul style="list-style-type: none"> <li>• that the information specified in the certificate was incorrect at the time of issuing the certificate</li> <li>• that the certificate does not contain all information as required by section 7.3.3 of the CP</li> <li>• failure to revoke the certificate, cf. section 7.3.6 of the CP</li> <li>• lacking or erroneous information relating to the revocation of the certificate, the expiry date of the certificate or whether the certificate is subject to limitation of purpose or amount, cf. sections 7.3.3 and 7.3.6 of the CP or</li> <li>• disregard of section 7.3.1</li> </ul> <p>unless the CA can prove that the CA has not acted negligently or intentionally.</p> <p>The CA prepares its own agreements etc. with its contracting parties. The CA is entitled to attempt 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. Thus, the CA is not entitled to attempt to limit its liability in relation to private citizens who are contracting parties.</p> <p>In addition, the CA is entitled to deny liability in relation to contracting parties who are business operators and public</p>

	<i>authorities for loss as described in s. 11 (3) in Act no. 417 of 31 May 2000.</i>
Rules or laws regarding the creation and functioning of Certification Authorities (CAs)	<p><i>The legal framework of the OCES concept consists of an agreement between the CA and the National IT and Telecom Agency. The three OCES CP's 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.</i></p> <p><i>The requirements of the CP's 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.</i></p>
Rules or laws regarding the existence of a centralised Electronic Certificate Validation Service for eGovernment applications (for example, laws regarding the creation of a Public Validation Platform for national eID cards)	<i>Not applicable</i>
Rules with regard to the hierarchy between multiple signature types used within a Member State (either nationally or cross-border), based on the technical/organisational characteristics of the signature solution	<i>In the OCES framework there is only one level in the hierarchy, due to the fact that all certificates are signed by the root key of the OCES-CA. The OCES CA has been webtrusted and therefore the root certificate has been included in both Microsofts and Mozillas certificate store for trusted authorities.</i>
What is the legal basis (law, decree,...) for this application?	<i>Described above under legal framework</i>
How is liability/responsibility regulated? Does the national legal framework regulate more than the minimum demand of the directive 1999/93 EC?	<i>By general Danish liability rules and regulation. Partly described above in the legal framework.</i>

<p>Which strategies are planned for the future? Should different types of the electronic signature be supported, or are the strategies only related to the wide distribution/extension/circulation of the qualified electronic signature?</p>	<p><i>Regarding OCES the commercial contract with TDC-CA, issuing OCES certificates expires in June 2008. In order to plan the second generation of OCES signatures, an analysis of the future needs and requirements for the digital signature including possible business models and requirements of the future operation of the OCES concept, is therefore taking place at the moment. A European tender is expected to be launched in April 2007.</i></p>
---	---

<b>Technical aspects</b>	
<p>What are the parties involved in the signature process?</p>	<p><i>Signatory (certificate holder), relying party (application/service provider) and CA. Also other relying parties can exist (f.ex. people who are influenced or affected by the signature process)</i></p>
<p>What kind of token or credentials are used (smart cards, software certificates, paper tokens ...)?</p>	<p><i>Software-based digital signatures. Can also be obtained on hardware (such as eToken or smart cards). No matter the media, the issuing refers to the same certificate policy.</i></p>
<p>What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of eSignature?</p>	<p><i>Basic PC-performance requirements. Smart card readers are necessary if the smart card solution is chosen.</i></p>
<p>What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?</p>	<p><i>Installation on Microsoft Windows: Operating system: Windows 98, Me, 2000 and XP Browser: Internet Explorer 5.5 or newer Installation on Mac, Linux etc.: Operating system: No specific requirements other than recent Java distributions (f.ex. Sun 1.3.1 or newer)</i></p>
<p>What are the relevant policies (CPS, certificate policy, signature policy)?</p>	<p><i>OCES 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 <a href="https://www.signatursekretariatet.dk/certifikatpolitikker.html">https://www.signatursekretariatet.dk/certifikatpolitikker.html</a></i></p> <p><i>The CPS from the OCES TDC-CA can be obtained from <a href="http://www.certifikat.dk/repository/TDCCPS40.pdf">http://www.certifikat.dk/repository/TDCCPS40.pdf</a></i></p>
<p>What information is included in the certificate, and what is the role of this information in the functioning of the application?</p>	<p><i>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).</i></p> <p><i>The policy OID field specifies a unique identification of the</i></p>

	<p><i>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.</i></p> <p><i>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.</i></p> <p><i>Note that the serialnumber 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 who by law are entitled to use the CPR or by explicit consent given by the certificate holder.</i></p> <p><i>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.</i></p> <p><i>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.</i></p>
<p>Does the application rely on an existing generic eSignature framework (i.e. a set of commonly agreed standards)? If yes, describe the framework in the country general profile.</p> <p>If no, specify which standards have been implemented in the eSignatures application? Depending on the signature type, this may include standards regarding certificates, signature formats, signature algorithms, token formats, other information security standards, etc.</p>	<p><i>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.</i></p> <p><i>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.</i></p> <p><i>Moreover an Open Source component (OpenSign/OpenLogon – <a href="http://www.openoces.org">www.openoces.org</a>) has been developed. The component offers client side login and web-signing functionalities.</i></p> <p><i>The OCES-CA published a number of technical documents and best practices on how OCES certificates are</i></p>

	<p><i>“examined” in terms of content and semantics, as well as how the integration with CA certificate related services can be achieved.</i></p>
<p>How is the signature verified and how is the verification data processed and stored (directly connecting to the corresponding CA validation service or just through a Validation Service provided by a Validation Authority)?</p>	<p><i>A digital signature is verified directly through the corresponding CA validation service through different validation protocols.</i></p> <p><i>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.</i></p> <p><i>The standard requires certain data to be logged and stored in the validation process, such as:</i></p> <ul style="list-style-type: none"> <li><i>· Time of signature verification</i></li> <li><i>· Result of signature verification:</i> <ul style="list-style-type: none"> <li><i>• Indication that the signature was valid at the time of reception</i></li> <li><i>• Indication that the digital signature associated data is unchanged</i></li> </ul> </li> <li><i>· Time of reception</i></li> <li><i>· State of encryption</i></li> <li><i>· Unique identification of the signature holder (subscriber):</i> <ul style="list-style-type: none"> <li><i>• In terms of OCES personal certificates the PID-nr is considered sufficient identification</i></li> <li><i>• In terms of OCES employee- and company certificates the SerialNumber and CommonName fields are considered sufficient identification.</i></li> </ul> </li> </ul> <p><i>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.</i></p>
<p>What types of validation protocols are used for the electronic certificate validation? (OCSP, CRLs, SCVP...)</p>	<p><i>At the moment CRL’s are the main supported validation protocol. An OCSP-service is also available.</i></p>
<p>How is the long term validity of the certificates dealt with?</p>	<p><i>The above described “proof of validation” standard provides the possibility to ensure long term validation through storing this proof of validation together with the signed data in a secure and tamper-free environment.</i></p> <p><i>Another option would be to store the data together with the original signature, but there is at the moment no time-stamping (and re-time-stamping and signing) or archiving</i></p>

	<p><i>services available in Denmark.</i></p> <p><i>There is so far no legal practice which tries the long term validity of either of the two described scenarios.</i></p>
--	---

<b>Organisational aspects</b>	
<p>Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?</p>	<p><i>The OCES project is established within the framework of the Ministry of Science, Technology and Innovation. Its main aim is to promote the use of digital signatures in Denmark.</i></p> <p><i>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.</i></p> <p><i>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 standardized certificate that will ensure interoperability between CAs.</i></p> <p><i>The National IT and Telecom Agency is responsible for drawing up and maintaining the OCES certificate policies.</i></p> <p><i>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:</i></p> <ul style="list-style-type: none"> <li><i>• citizens in Denmark can obtain digital signatures free of charge (financed by the government for public authorities)</i></li> <li><i>• employee certificates are issued (financed by the government for public authorities)</i></li> <li><i>• corporate certificates are issued</i></li> <li><i>• public authorities may obtain digital signatures on favourable terms</i></li> <li><i>• public authorities can look up in the CPR-register free of charge via a conversion of PID-numbers to</i></li> </ul>

	<p><i>CPR numbers.</i></p> <p><i>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.</i></p>
<p>Who issues/manages credentials (e.g. certificates)? Describe the conditions and the procedure for the issuance of the credentials.</p>	<p><i>At the moment only one CA has an agreement with the National IT and Telecom Agency to issue OCES digital signatures.</i></p> <p><i>See above</i></p>
<p>What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be suspended or revoked?</p>	<p><i>Up to four years.</i></p> <p><i>The subscriber must revoke the certificate if the private key has been compromised or is suspected of having been compromised</i></p> <p><i>The CA must revoke an OCES certificate immediately if the CA has been informed of any of the below-mentioned circumstances:</i></p> <ul style="list-style-type: none"> <li><i>• certainty or suspicion exists that the subscriber's private key has been compromised;</i></li> <li><i>• the private key has been destroyed;</i></li> <li><i>• inaccuracies have been ascertained in the certificate content or other information associated with the subscriber;</i></li> <li><i>• the subscriber wishes to terminate the use of the OCES certificate;</i></li> <li><i>• the subscriber has passed away, or</i></li> <li><i>• the subscriber has been placed under guardianship and has been deprived of his/her legal capacity.</i></li> </ul> <p><i>The CA should revoke a certificate if the CA learns that</i></p> <ul style="list-style-type: none"> <li><i>• the subscriber has lost access to the private key, e.g. as a result of losing the activation code.</i></li> </ul> <p><i>The CA may revoke a certificate if the CA learns that</i></p> <ul style="list-style-type: none"> <li><i>• the rules laid out in this CP have not been met</i></li> <li><i>• the terms from the agreement between the CA and the subscriber have been breached.</i></li> </ul> <p><i>CA breach of the CP does not give the CA the right to revoke a certificate.</i></p>
<p><b>Interoperability aspects</b></p>	

<p>Is the system accessible to non-nationals, and if so, how? If not, can the system be upgraded for cross-border interaction?</p>	<p><i>At the moment only persons with a Danish CPR-number can have an OCES-personal digital signature. The reason being that the registration and identification process is based on a CPR-register. For the same reason only companies registered in the Danish central business register can have an OCES employee- and/or company certificate.</i></p> <p><i>With regards to technology the OCES standard is based on international standards and therefore could be upgraded for cross-border interaction. The challenge lies in the unique identification of the certificateholder.</i></p>
--	--

<b>Miscellaneous</b>	
<p>Are there any statistics on the widespread of the certificates (if not: please provide an estimation)?</p>	<p><i>The OCES signature (Public certificates for electronic services) has existed for 3 years. Around 755.000 certificates (Personal-OCES 625.000, Employee-OCES 125.000, Company-OCES 4.000 (November 2006)) have been issued and almost all municipalities and public institutions have implemented e-services depending on the e-signature.</i></p>
<p>Are there any Government initiatives aimed at providing/encouraging the use of OCES?</p>	<p><i>See above under organisational aspects.</i></p> <p><i>During 2004 it became possible for young people between 15 and 18 to get a digital signature. A solution has been implemented which makes it possible for Danes with protected names and addresses as well as Danes living abroad to get a digital signature by appearing personally at a Danish representation.</i></p> <p><i>One of the National IT and Telecom Agency's tasks in ensuring widespread use of digital signatures is to provide guidance and advice for public authorities and citizens on the implementation and use of digital signatures. For this purpose, a website dedicated exclusively to such information activities has been established: <a href="http://www.digitalsignatur.dk">www.digitalsignatur.dk</a>. The site is visited by about 1000 unique persons a week. To support the knowledge and adoption of digital signatures, a logo for the common public digital signature has been developed, thus creating a common identity for the OCES signature.</i></p> <p><i>A special design was also developed for <a href="http://www.digitalsignatur.dk">www.digitalsignatur.dk</a>. The site offers targeted information for citizens and public authorities. Also available is readily understandable guidance on digital signatures for citizens, and an explanatory video presentation on digital signatures is available.</i></p>

	<p><i>A digital toolbox is available for public authorities. It consists of a number of tools which can be used free of charge in their work to promote digital signatures. Among the items available are logos in various formats, brochures on digital signatures, PowerPoint presentations etc. There are also guidelines on how public authorities can implement digital signatures and the aspects that the authority should consider in this connection.</i></p>
--	--

<b>Assessment</b>	
<p>Please give your own assessment on the implementation and widespread of OCES certificates.</p> <p>Take this opportunity to bring any fruitful information that was not addressed by previous questions.</p>	<p><i>Our assessment is that it takes time to establish an open infrastructure in large scale for digital signatures and to get people to use it. The electronic services are the drivers for the rollout of digital signatures. There has to be benefits for the citizens and companies in using digital signatures. It is in general hard to establish a business case on the development of a PKI-infrastructure, thus public subsidizing 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.</i></p> <p><i>As touched upon above 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.</i></p>

*Ed. Note: It should be noted that the OCES solution does not depend on a smart card or other physical token, and that no major smart card roll-out for the general public is currently planned in Denmark.*

#### 4.2.2 Personal Identification Number

Personal identification numbers are used in the OCES signature process, cf. section 4.2.1.

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 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<sup>8</sup>.

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

<sup>8</sup> 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](http://147.29.40.90/_SHOWF_A775329798/919&A20040014029REGL&0001&000001)

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 public available.

## **5 eGovernment applications using electronic signatures**

For an extensive list of eGovernment applications, reference as made to the list in section [7 \(Operational and planned applications\)](#). In the section below only the most significant eGovernment applications and the manner in which they rely on electronic signatures are explained.

### **5.1 Public procurement**

#### **5.1.1 ETHICS**

See also questionnaire in Annex 10

##### **5.1.1.1 Application identification**

National Procurement Ltd. (SKI) is an organisation owned by the state and the local municipalities. The purpose of SKI is to centralise purchases of public organisations in order to achieve as low prices as possible.

SKI is the owner of a system for electronic tenders and procurements called ETHICS (Electronic Tender Handling, Information & Communications System). The system has been in operation since 2000.

ETHICS covers all Phases of a complex tendering process:

- Contract Administration and Legal Requirements
- Market analysis - user Requirements and state-of-the-art Offerings
- Requirements Assessment
- Tender Process Planning and Management Process
- Questionnaire Design Tool
- Execution and Evaluation Process fully supported

##### **5.1.1.2 eSignature details**

###### **5.1.1.2.1 Legal aspects**

Directive 2004/18 is transposed into Danish law by Royal Decree no. 937 of 16 September 2004<sup>9</sup>. The decree basically states that the directive applies. No further regulation on eProcurement and eSignatures are established under Danish procurement law.

---

<sup>9</sup> See [http://147.29.40.91/SHOWF\\_B762442665/1072&B20040093705REGL&0006&000001](http://147.29.40.91/SHOWF_B762442665/1072&B20040093705REGL&0006&000001)

#### **5.1.1.2.2 Technical aspects**

ETHICS is based on leading edge technology from IBM Lotus and integrates through Open Standards with existing office systems, document repositories and common browsers.

The application uses HTML and XML datastructures

ETHICS uses OCES signatures. Technical aspects of the OCES signature are explained in section 4.2.1.

#### **5.1.1.2.3 Organisational aspects**

The parties involved in the signature scheme are bidder/vendor, procurer, SKI (application owner), TDC (issuer of OCES certificates) and Innovation (service provider).

#### **5.1.1.3 Interoperability**

The application is accessible for any one over the internet.

The application supports simultaneously any language supported/accepted by the purchasing entity (tender issuer), i.e. the system presents the information to the end users according to the settings of the end users browser.

No measures have been taken to ensure interoperability with signatures created and/or certificates issued in other countries.

#### **5.1.1.4 Miscellaneous**

No statistics on the use of eSignatures have been provided.

#### **5.1.2 Assessment**

N/A

## **5.2 Tax**

### **5.2.1 TastSelv Borger - Personal income taxes declarations**

See also questionnaire in Annex 10

#### **5.2.1.1 Application identification**

TastSelv Borger is the automated tax process, with the least possible inconvenience to the citizens (which we call the “no touch strategy”). 97 percent of all data regarding the Danish citizens' tax declarations are reported by employers, banks, mortgage institutions, trade unions, social benefits administration etc. to The Central Customs and Tax Administration. The citizens can report corrections or approve their tax return via the Internet. The result in the form of an annual settlement can be seen immediately. If tax overpayments are due to a citizen, they are transferred to his bank account.

#### **5.2.1.2 eSignature details**

##### **5.2.1.2.1 Legal aspects**

According to § 1(3) of the Tax Control Act (Act no. 1126 of 24 November 2005)<sup>10</sup> the Minister of Tax decides whether tax declarations should be signed or admitted in other ways. This clause forms the legal basis for electronic tax declaration applications.

No specific regulation regarding electronic tax applications or eSignatures in tax applications are in place.

##### **5.2.1.2.2 Technical aspects**

All applications in the browser option have been established using standard web browsers as a client, and using standard HTML, Javascript and style sheet. The applications have been coded in Java and run on a number of web servers under Websphere.

An XML interface has been defined for the annual settlement. The purpose is that annual settlement data can be transferred via web services following citizen approval to a bank or another private credit provider for use when citizens apply for loans in banks.

Applets or similar plug-ins are not used, apart from Acrobat Reader for showing the edited annual settlements and the preliminary tax assessments. Consequently, this is a system of thin clients with

---

<sup>10</sup> See [http://147.29.40.91/SHOWF\\_B762442665/1072&A20050112629REGL&0009&000001](http://147.29.40.91/SHOWF_B762442665/1072&A20050112629REGL&0009&000001)

validation, but without business logic. Presentation logic and partly business logic are run on the web servers that retrieve data from and deliver data to the mainframe systems via DB2 call (standard SQL) or IMS transactions.

Encryption is made with 128 bits SSL via a proxy server.

The application uses OCES signatures and/or a simple password solution. Technical aspects of the OCES signature are explained in section 4.2.1.

#### **5.2.1.2.3 Organisational aspects**

The parties involved in the signature scheme are SKAT (application owner), TDC (issuer of OCES certificates), CSC (service provider) and the users.

Relying party are SKAT.

#### **5.2.1.3 Interoperability**

The system is not accessible to non-nationals and no measures have been taken to ensure interoperability with solutions from other countries.

#### **5.2.1.4 Miscellaneous**

In 2005 the application had 3.113.476 logins through password solution and 487.248 logins with OCES signatures. This is an increase in use of OCES of 136% compared to 2004.

#### **5.2.1.5 Assessment**

According to the application owner it has been a problem that the OCES certificate is not mobile.

## **5.2.2 TastSelv Erhverv – VAT and other company tax declarations and payments**

### **5.2.2.1 Application identification**

TastSelv Erhverv is the parallel to TastSelv Borger for enterprises. The application allows enterprises to report and pay VAT and tax online.

### **5.2.2.2 eSignature details**

#### **5.2.2.2.1 Legal aspects**

According to § 1(3) of the Tax Control Act (Act no. 1126 of 24 November 2006) the Minister of Tax decides whether tax declarations should be signed or admitted in other ways. This clause forms the legal basis for electronic tax declaration applications.

No specific regulation regarding electronic tax applications or eSignatures in tax applications are in place.

#### **5.2.2.2.2 Technical aspects**

The application is based on the same technical platform as TastSelv Borger (see above).

#### **5.2.2.2.3 Organisational aspects**

See TastSelv Borger above

#### **5.2.2.3 Interoperability**

The application is accessible to non-nationals who have a SE-number (are paying VAT to Denmark). Non-nationals can only get access by pin-code as OCES signatures are not offered to non-nationals.

#### **5.2.2.4 Miscellaneous**

App. 300.000 enterprises are using the application. 3% use an OCES signature. 97% use simple password solution.

#### **5.2.2.5 Assessment**

N/A

## 5.3 Health care

### 5.3.1 Sundhed.dk – the national health care portal

See also questionnaire in Annex 10

#### 5.3.1.1 Application identification

Sundhed.dk is the joint public health internet portal in Denmark ('sundhed' means health).

For the first time, sundhed.dk brings together the entire Danish health services on the Internet, making this the electronic way for patients, their families, and healthcare professionals to obtain information, communicate and maintain an overview.

#### 5.3.1.2 eSignature details

##### 5.3.1.2.1 Legal aspects

No specific regulation on eSignatures and electronic documents apply to sundhed.dk or the sub applications.

A draft Act (L 50 2005/2006)<sup>11</sup> on changes to the Health Act (Act no. 546 of June 24 2005)<sup>12</sup> will regulate obtaining of personal data in electronic health care systems. See § 1(13) of the draft Act introducing a new § 42 a and § 42 b to the Health Act. The technical requirements will be further specified by the National Board of Health. It is not known whether such requirements will include eSignatures.

##### 5.3.1.2.2 Technical aspects

The application processes XML-based datastructures for National CA, Lab-systems in hospitals, national medicine and patient databases.

The Digital Certificates are used for identifying the users. When Identified by the Portal, the user has access to own data and for Healthcare professionals to patient data. The external systems are Lab-systems in hospitals, national medicine and patient databases.

At the moment there is not any Certificate Signature exchange between systems. The security between systems is handles by a point-to-point private and secure network.

At the moment there are pilot projects (SOSI) validating the exchanges of the signed certificates between systems.

OCES Software certificates are used. Some users copy this certificate to a "Token/Memory stick" and use it like a smart card. However this is not application driven.

---

<sup>11</sup> See <http://www.folketinget.dk/?/samling/20061/MENU/00000002.htm>

<sup>12</sup> See [http://147.29.40.91/SHOWF\\_B762442665/1072&A20050054630REGL&0010&000001](http://147.29.40.91/SHOWF_B762442665/1072&A20050054630REGL&0010&000001)

The application uses OCES signatures. Technical aspects of the OCES signature are explained in section 4.2.1.

#### **5.3.1.2.3 Organisational aspects**

The parties involved in the signature schemes are Sundhed.dk (application owner), TDC (issuer of OCES certificates) and the users of the portal (private citizens and professional health care personnel).

Relying party is the Sundhed.dk

#### **5.3.1.3 Interoperability**

The application is only available to Danish citizens and the application does not provide interoperability with signatures from other countries.

#### **5.3.1.4 Miscellaneous**

App. 110.000 users with own eSignature.

#### **5.3.1.5 Assessment**

According to the application owner OCES provides a simple and secure infrastructure for validating the users. Simple for the citizens to get. The installation process can sometimes be a barrier for the use of Personal Certificates, but sundhed.dk tries to support people in case of problems.

Organisations need support for setting up the right organization for implementing, rolling out and administration employee certificates in own organization. Especially the fact that healthcare professionals need access to data from every bed in a hospital calls for other solutions than the current software based eSignature. The mobility issue is handled differently from hospital to hospital – but several organizations have started to implement a central certificate store – others consider different hardware solutions.

## **5.4 Finance**

### **5.4.1 Virk.dk**

See also questionnaire in Annex 10

#### **5.4.1.1 Application identification**

The stated objective of Virk.dk is to relieve Danish companies of administrative burdens. Virk.dk is an internet portal delivering a number of fully digital solutions for the benefit of the companies as well as the public administration. Virk.dk contains more than 200 e-forms. A number of the forms may be filled out and signed with an OCES signature.

#### **5.4.1.2 eSignature details**

##### **5.4.1.2.1 Legal aspects**

As Virk.dk is a portal with more than 200 e-forms no general rule covers the use of eSignatures in the application. However it might be that some of the forms are covered by specific legislation.

##### **5.4.1.2.2 Technical aspects**

When a user signs the data supplied to an e-form, the signed data is submitted together with an XML instance and a PDF version of the form. Authorities can now retrieve this data on Virk.dk using a common web service.

The fields of the e-form are generated from the data in the repository, taking into account mainly three inputs, all of which are also represented by the corresponding XML Schemas. At first the system will identify the data type of the field for the purpose of validation. Secondly it will identify the unique naming of the fields on the form so that the form can pre-fill an answer that is known to the system from a previous e-form. Finally, it will take into account the grouping structure, so that the form can create the appropriate XML instance document.

This means the data submitted from the form is always consistent with the XML Schemas. Thus, it is easy to build web services and integrate data from different sources.

Authorities can then build integration between Virk.dk and their back office systems, using the common web services based on the XML schemas.

The application uses OCES signatures. Technical aspects of the OCES signature are explained in section 4.2.1.

##### **5.4.1.2.3 Organisational aspects**

The parties involved in the signature scheme are the Danish Commercial and Companies Agency and the private company KRAK (application owners), TDC (issuer of OCES certificates), all government institutions with transactions forms for businesses – currently 39 institutions and the users (companies).

Relying party is the government institutions with transactions forms on Virk.dk.

#### **5.4.1.3 Interoperability**

Non-nationals employed with Danish businesses can use the application. Multinational companies with a Danish Branch can also use the application. Other non-nationals cannot. (Because the identification of the company in the certificate is based on the central business registration number only given to Danish companies)

At present the application does not provide interoperability with signatures from other countries but this is being considered.

#### **5.4.1.4 Miscellaneous**

The number of registered users is app. 15.000.

#### **5.4.1.5 Assessment**

The application owner considers OCES to be stable and secure but with weaknesses in usability, price and usage.

### **5.4.2 Webreg.dk - registration and change of company information**

See also questionnaire in Annex 10

#### **5.4.2.1 Application identification**

Webreg makes it possible to make on-line registration of new companies and changes of company information.

#### **5.4.2.2 eSignature details**

##### **5.4.2.2.1 Legal aspects**

The webreg application is regulated in chapter 11 of the Royal Decree no. 860 of August 10<sup>13</sup> on filing of applications with the Danish Commercial and Company Agency.

According to § 45 of the decree the user must use a digital signature unless the Agency decides otherwise.

#### **5.4.2.2.2 Technical aspects**

The application uses OCES signatures. Technical aspects of the OCES signature are explained in section 4.2.1.

#### **5.4.2.2.3 Organisational aspects**

The parties involved in the signature scheme are the Tax authorities and the Danish Commercial and Companies Agency, TDC (issuer of OCES certificates) and the users.

Relying parties are tax authorities and the Danish Commercial and Companies Agency.

#### **5.4.2.3 Interoperability**

The application does not provide interoperability with signatures from other countries.

#### **5.4.2.4 Miscellaneous**

#### **5.4.2.5 Assessment**

N/A

### **5.4.3 NemKonto**

See also questionnaire in Annex 10

#### **5.4.3.1 Application identification**

All citizens and companies in Denmark have to have an NemKonto Easy Account (Mandatory). An Easy Account is a normal bank account which the citizen/company already has, and designate as their NemKonto Easy Account. All payments from public institutions are being transferred directly to this account via the Easy Account System (EAS).

The EAS is a database with account numbers and social security numbers or company numbers.

When a public institution make a payment to a citizen or company, the payment is made to a social security- or company number. The payment then goes from the institution's payment system to the EAS, which attaches an account number, and then to the institutions bank and further on to the citizen/company's bank account.

This way all public payments are made electronically to bank accounts – no checks and cash payments.

Online (at [www.nemkonto.dk](http://www.nemkonto.dk)), it is possible to designate, change or delete an Easy Account for citizens and public institutions. Staff in public institutions with the right user profile can log on to the website and stop payments or search for payments their institution has made. Access is attained by logging on to the website using the OCES signature.

#### **5.4.3.2 eSignature details**

##### **5.4.3.2.1 Legal aspects**

The Nemkonto application is regulated by Executive Order no. 766 of 5 July 2006 on the Nemkonto arrangement<sup>14</sup>.

According to § 26 and § 27 of the decree an “official digital signature” must be used. The term “official digital signature” is not further defined; however the OCES signature supported by the application does without doubt comply with the requirement.

##### **5.4.3.2.2 Technical aspects**

When logging on to the website [www.nemkonto.dk](http://www.nemkonto.dk), the EAS validates the signature with the provider, TDC (private company who has won the tender and provides the digital signature).

The Agency for Governmental Management is responsible for the EAS which is developed by the private software company KMD A/S.

For employees in public institutions using an employee digital signature, the signature is used to identify the user profile of the employee. This is done in the safety system “KSP/CICS”.

The application uses XML Broker and Web Server as external interfaces and SWIFT Customer to Bank Payment XML.

##### **5.4.3.2.3 Organisational aspects**

The parties involved in the signature scheme are EAS (application owner), TDC (issuer of OCES certificates), KMD (service provider) and the users.

Relying party is EAS.

#### **5.4.3.3 Interoperability**

The system is not accessible to non-nationals and no measures have been taken to ensure interoperability with solutions from other countries.

#### **5.4.3.4 Miscellaneous**

The OCES signature is used by app. 40.000 users of the application

#### **5.4.3.5 Assessment**

N/A

---

<sup>14</sup> See [http://www.retsinfo.dk/LINK\\_0/0&ACCN/B20060076605](http://www.retsinfo.dk/LINK_0/0&ACCN/B20060076605)

## **5.5 Justice**

### **5.5.1 Electronic registration of property**

#### **5.5.1.1 Application identification**

Electronic registration of land is planned to be implemented in Denmark in 2008. The legal basis for this is a change to the Danish Registration of Property Act, cf. section 5.6.1.2.1 below.

In order to have a system in place in due time the Danish Court Administration is in the middle of an EU public procurement process. The winner of the tender who will develop the system is expected to be found within long.

Due to the preliminary status of the project it is not possible to provide more detailed answers about the system to come. However it is decided that the system will use OCES signatures but also seek to support other electronic signatures and a similar security level as OCES (including qualified eSignatures).

#### **5.5.1.2 eSignature details**

##### **5.5.1.2.1 Legal aspects**

Act no. 539 of 8 June 2006 on changes to the Registration of Property Act<sup>15</sup> introduces electronic tinglysning. According to § 1(6) of the Act documents should be registered electronically using a digital signature.

The Ministry of Justice may specify technical requirements to electronic documents and eSignatures after having consulted the Ministry of Science, Technology and Innovation. No such specifications are in place yet.

##### **5.5.1.2.2 Technical aspects**

The application will support OCES. On technical aspects of the OCES signature see section 4.2.1.

##### **5.5.1.2.3 Organisational aspects**

Information not available yet

#### **5.5.1.3 Interoperability**

Information not available yet

---

<sup>15</sup> See [http://147.29.40.91/SHOWF\\_B762442665/1072&A20060053930REGL&0012&000001](http://147.29.40.91/SHOWF_B762442665/1072&A20060053930REGL&0012&000001)

#### **5.5.1.4 Miscellaneous**

Information not available yet

#### **5.5.1.5 Assessment**

N/A

## **5.6 Local applications**

### **5.6.1 Netborger.dk**

See also questionnaire in Annex 10

#### **5.6.1.1 Application identification**

Netborger is a portal for a suite of A2B solutions, where local municipalities can offer self-service to their citizens. A large number of applications of the municipalities are offered from the portal (see list in annex 10.5).

The portal by itself provides authentication of the user when needed, and supplies information on Danish municipalities in general.

Self-service are provided thru access to information in legacy systems. This information can be information on rules or application for public services or financial support.

#### **5.6.1.2 eSignature details**

##### **5.6.1.2.1 Legal aspects**

As netborger.dk is an umbrella application with a number of individual applications no general rule covers the use of eSignatures in the application. However it might be that some of the individual applications are covered by specific legislation.

##### **5.6.1.2.2 Technical aspects**

The application uses OCES signatures. Technical aspects of the OCES signature are explained in section 4.2.1. Signing is done using the OpenSource component at [www.OPENOCES.org](http://www.OPENOCES.org).

Furthermore a simple password solution and the common Danish NetBank logon system (NetID) are supported.

##### **5.6.1.2.3 Organisational aspects**

The parties involved in the OCES signature scheme are various application owners, TDC (issuer of OCES certificates), and the users.

Relying parties are the various application owners.

#### **5.6.1.3 Interoperability**

Self-service are only intended for Danish Citizens, and other people living in Denmark.

The authentication server could be extended to accept certificates issued by other CAs. This is not done for the time being.

#### **5.6.1.4 Miscellaneous**

Week 43, 2006: app. 800.000 logins, of which app. 25% are using OCES certificates : 200.000 certificate login

#### **5.6.1.5 Assessment**

N/A

### **5.6.2 E-boks**

#### **5.6.2.1 Application identification**

Secure electronic document archive, where public authorities and companies can deliver documents to citizens/consumers. Documents are achieved thru the website [www.e-boks.dk](http://www.e-boks.dk). In other words documents can be achieved from all computers with an internet access.

#### **5.6.2.2 eSignature details**

##### **5.6.2.2.1 Legal aspects**

The application is not covered by specific provisions.

##### **5.6.2.2.2 Technical aspects**

The application uses OCES signatures. Technical aspects of the OCES signature are explained in section 4.2.1.

Furthermore a simple password solution and the common Danish NetBank logon system (NetID) are supported.

##### **5.6.2.2.3 Organisational aspects**

The parties involved in the OCES signature scheme are e-Boks A/S (application owner), TDC (issuer of OCES certificates), and the users.

Relying party is e-Boks A/S.

#### **5.6.2.3 Interoperability**

According to the application owner the application can be used by non-Danish citizens. However only Danish citizens can have an OCES signature, cf. section 4.2.1.

#### **5.6.2.4 Miscellaneous**

App. 1 million users of the application. According to the application owner 70% uses electronic signatures.

##### **5.6.2.4.1 Assessment**

No specific problems according to the application owner.

## 6 General Assessment

The use of eGovernment applications and the number of eGovernment applications are continuously increasing. It seems as the psychological barrier has been broken and citizens are getting used to communicating with public authorities through eGovernment applications.

Due to cost savings and the future changes in population with fewer people in the working age there is a high political focus on the use eGovernment. Lately the possibility of making use of eGovernment mandatory has been discussed. However this would in most situations require amendments to the existing law.

Electronic signatures are recognized as a key element in achieving success with eGovernment. This is one of the reasons why the Danish Ministry for Science, Technology and Innovation initiated the OCES signature project. The aim of establishing an electronic signature based on open standards free to use by the citizens and used as a public standard eSignature solution in eGovernment applications has to a large extent been achieved.

As can be seen by section 5 of the report the OCES signature is the primary eSignature solution used in eGovernment today.

No qualified eSignatures are offered in Denmark and consequently no eGovernment applications use qualified eSignatures. It appears that for the time being there is no need for qualified eSignatures. The fact that people does not have to identify themselves in person to get an OCES signature (contrary to qualified eSignatures) has not led to any known abuse of eGovernment applications or other applications using OCES signatures. This might change in the future as eGovernment applications are used for more complex and important types of transactions.

The OCES signature does not provide cross border functionality in its current form. In general this applies to the eGovernment applications as such. The reason for this is probably a limited request for such functionality for the time being combined with the fact that many of the applications are providing services only relevant to Danish citizens (tax, health care and the like). More and more demands coming from the implementation of different cross border solutions will increase the need to address this challenge in the future.

The OCES certificate is based on the X509 v.3 standard and is therefore in principle interoperable with any solution that requires X509 based signatures. As mentioned above in 4.2, there are some general challenges regarding interoperability which also applies to the OCES certificate:

- Trust between CAs
- Semantics of the certificate
- Identification of certificate holder

Some initiatives have been promoted in order to internationalize the OCES signature. The OCES CA has "webtrusted" its root keys and they have been included in both Microsoft's and Mozilla's standard root certificate store of trusted certificates .

## 7 Operational and planned applications

Most of the applications mentioned in the tables below have been further elaborated above with information on the actual usage of the applications. It should be noted that the list is not exhaustive.

### 7.1 Applications at the federal level

	Application	Scope	Reference	Contact	Signature
1.	ETHICS	eProcurement and tender application	<a href="http://www.ski.dk">www.ski.dk</a>	<a href="http://www.ski.dk">www.ski.dk</a>	Digital signature
2.	TastSelv Borger	Correction and approval of tax returns	<a href="http://www.skat.dk/SKAT.aspx?oID=349844">http://www.skat.dk/SKAT.aspx?oID=349844</a>	<a href="http://www.skat.dk">www.skat.dk</a> (see also "contact person" in annex 10.1)	OCES (or simple password logon)
3.	TastSelv Erhverv	Electronic filing of VAT and other company tax declarations. Electronic payment of VAT and company tax.	<a href="http://www.skat.dk/SKAT.aspx?oID=199611">http://www.skat.dk/SKAT.aspx?oID=199611</a>	<a href="http://www.skat.dk">www.skat.dk</a>	OCES (or simple password logon)
4.	Virk.dk	Application where all transaction forms that Danish Businesses shall/may forward to Danish Government Institutions are accessible – either as text documents (for print) or as more sophisticated e-forms (where OCES is used).	<a href="http://www.virk.dk">www.virk.dk</a>	<a href="http://www.virk.dk/VirkPortal/site/Kolofon/KontaktVirk.aspx">http://www.virk.dk/VirkPortal/site/Kolofon/KontaktVirk.aspx</a> (see also "contact person" in annex 10.4)	OCES (or simple password logon)

	Application	Scope	Reference	Contact	Signature
5.	Webreg	Webreg makes it possible to make on-line registration of new companies and changes of company information.	<a href="http://www.webreg-portal.dk">www.webreg-portal.dk</a>	See Virk.dk (Webreg is operated as part of Virk.dk)	OCES  (or simple password logon)
6.	State education and loan scheme	Electronic registration of state education loans	<a href="http://www.su.dk">www.su.dk</a>	<a href="http://www.su.dk">www.su.dk</a>	OCES
7.	Nemkonto	All citizens and companies in Denmark have to have a NemKonto Easy Account (Mandatory). An Easy Account is a normal bank account which the citizen/company already has, and designate as their NemKonto Easy Account. All payments from public institutions are being transferred directly to this account via the Easy Account System (EAS).	<a href="http://www.nemkonto.dk">www.nemkonto.dk</a>	<a href="http://www.nemkonto.dk">www.nemkonto.dk</a>  (see also "contact person" in annex 10.2)	OCES
8.	E-registration of property	Electronic registrations of property.	The application is under development	The Court Administration  <a href="http://www.domsstyrelsen.dk">www.domsstyrelsen.dk</a>	OCES
9.	Jobnet	Jobnet is the Danish Employment Service's Internet facility for all jobseekers and employers in	<a href="http://www.jobnet.dk">www.jobnet.dk</a>	<a href="http://www.jobnet.dk">www.jobnet.dk</a>	OCES

	<b>Application</b>	<b>Scope</b>	<b>Reference</b>	<b>Contact</b>	<b>Signature</b>
		Denmark.			
10.	EASY	EASY is the National Board of Industrial Injuries electronic system for filing of claims for work related injuries	<a href="https://easy.ask.dk/easy/">https://easy.ask.dk/easy/</a>	<a href="https://easy.ask.dk/easy/">https://easy.ask.dk/easy/</a>	OCES  (or simple password logon)
11.	Optagelse.dk	Optagelse.dk is a coordinated filing system for applying for admission to educations	<a href="https://www.optagelse.dk/a268/index.jsp">https://www.optagelse.dk/a268/index.jsp</a>	<a href="https://www.optagelse.dk/a268/index.jsp">https://www.optagelse.dk/a268/index.jsp</a>  or the Danish Ministry of Education (application owner)  <a href="http://eng.uvm.dk/">http://eng.uvm.dk/</a>	OCES
12.	Det kongelige bibliotek (The Royal Library)	Selv service application for library users (book reservations, extension of loaning period etc)	<a href="http://www.kb.dk/index-en.htm">http://www.kb.dk/index-en.htm</a>	<a href="http://www.kb.dk/index-en.htm">http://www.kb.dk/index-en.htm</a>	OCES  (or simple password logon)

## 7.2 Applications at the regional level

	Application	Scope	Reference	Contact	Signature
1.	Sundhed.dk		<a href="http://www.sundhed.dk">www.sundhed.dk</a>	<a href="http://www.sundhed.dk">www.sundhed.dk</a>  (see also "contact person" in annex 10.3)	

## 7.3 Applications at the local level

	Application	Scope	Reference	Contact	Signature
1.	Netborger		<a href="http://www.netborger.dk">www.netborger.dk</a>	<a href="http://www.netborger.dk">www.netborger.dk</a>	OCES or simple password solution
2.	Din Boligstøtte (application under Netborger)	Filing of applications for rent subsidy	<a href="http://dinboligstoette.netborger.dk/produkt/paraply/default.asp?p=netborger">http://dinboligstoette.netborger.dk/produkt/paraply/default.asp?p=netborger</a>		See Netborger
3.	Søg børnetilskud (application under	Filing of applications for child benefit	<a href="https://boernetilskud-ansoegning.netborger.dk/default.asp">https://boernetilskud-ansoegning.netborger.dk/default.asp</a>		See Netborger

	Netborger)			
4.	Institutionsopskrivning  (application under Netborger)	Filing of application for child day care	<a href="http://institution-opskrivning.netborger.dk/">http://institution-opskrivning.netborger.dk/</a>	See Netborger
5.	Din ejendom	Information about own real estate property and filing of various applications regarding real estate property	<a href="http://dinejendom.netborger.dk/produkt/forside.asp">http://dinejendom.netborger.dk/produkt/forside.asp</a>	See Netborger

## 8 Annex A: Contact details of National Correspondents

Contact Information of the person(s) completing the questionnaire. The person(s) will be contacted for any queries related to this questionnaire.

### 8.1 Primary Contact

<b>Country</b>	Denmark
<b>Name</b>	Henrik Udsen
<b>Organisation</b>	Copenhagen University

## 9 Annex B: National Regulations Details

National correspondents are required to include references to the legal sources that they have consulted. This includes references to laws, other regulations, and doctrine, in such a manner that a legal expert with knowledge of the national legal system would be able to retrieve the sources.

Whenever referring to national regulations or institutions, the correspondents are required to provide the local name as well as an English language translation of the regulation's title.

If available, links to on-line resources (legislation, judicial decisions, governmental websites, and professional organisations) should be included.

National regulation title	National regulation translated title (English title)	Relevant links to on-line resources
Lov om elektroniske signaturer (417/2000)	Act on Electronic Signatures	<a href="http://147.29.40.91/_SHOWF_B762442665/1072&amp;A2000004_1730REGL&amp;0001&amp;000001">http://147.29.40.91/ SHOWF_B762442665/1072&amp;A2000004_1730REGL&amp;0001&amp;000001</a>
Bekendtgørelse om nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen (922/2000)	Executive Order on Reporting of Information to the National Telecom Agency by CAs and system Auditors	<a href="http://147.29.40.91/_SHOWF_B762442665/1072&amp;B2000009_2205REGL&amp;0004&amp;000001">http://147.29.40.91/ SHOWF_B762442665/1072&amp;B2000009_2205REGL&amp;0004&amp;000001</a>
Bekendtgørelse om sikkerhedskrav til nøglecentre mv. (923/2000)	Executive Order on Security Requirements etc. for Certification Authorities	<a href="http://147.29.40.91/_SHOWF_B762442665/1072&amp;B2000009_2305REGL&amp;0003&amp;000001">http://147.29.40.91/ SHOWF_B762442665/1072&amp;B2000009_2305REGL&amp;0003&amp;000001</a>
Forvaltningsloven (571/1985)	The Administration Act	<a href="http://147.29.40.91/_SHOWF_A393870761/311&amp;A20020105_030REGL&amp;0001&amp;000001">http://147.29.40.91/ SHOWF_A393870761/311&amp;A20020105_030REGL&amp;0001&amp;000001</a>
Lov om det centrale personregister (140/2004)	Act on the Civil Registration System	<a href="http://147.29.40.91/_SHOWF_B762442665/1072&amp;A2004001_4029REGL&amp;0005&amp;000001">http://147.29.40.91/ SHOWF_B762442665/1072&amp;A2004001_4029REGL&amp;0005&amp;000001</a>
Bekendtgørelse om fremgangsmåderne ved indgåelse af offentlige vareindkøbskontrakter, offentlige tjenesteydelseskontrakter og offentlige bygge- og anlægskontrakter (937/2004)	Executive Order on coordination of procedures for the award of public works contracts, public supply contracts and public service contracts	<a href="http://147.29.40.91/_SHOWF_B762442665/1072&amp;B2004009_3705REGL&amp;0006&amp;000001">http://147.29.40.91/ SHOWF_B762442665/1072&amp;B2004009_3705REGL&amp;0006&amp;000001</a>
Skattekontrolloven	Tax Control Act	<a href="http://147.29.40.91/_SHOWF_B762442665/1072&amp;A2005011">http://147.29.40.91/ SHOWF_B762442665/1072&amp;A2005011</a>

(1126/2005)		<a href="#">2629REGL&amp;0009&amp;000001</a>
Forslag til ændring af sundhedsloven	Draft Act on changes to the Health Act	<a href="http://www.folketinget.dk/?/samling/20061/MENU/00000002.htm">http://www.folketinget.dk/?/samling/20061/MENU/00000002.htm</a>

## 10 Annex C: Filled-in questionnaires

### 10.1 ETHICS (eTender and procurement)

#### 10.1.1 Application identification

Application/Service Classification	
Application/Service Name	<i>ETHICS</i>
Application/Service Type	<i>A2B (administration to business)</i>
Concerned sector	<i>Public procurement</i>
Application/Service Cross-Border Type	<i>Multilateral</i>
Level of Online Sophistication Type	<i>Stage 4: Transaction: Case handling; decision and delivery (payment)</i>
Intended "clients"	<i>Mandate holders, i.e. Vendors submitting proposals.</i>
Abstract Description	<p><i>Electronic Tender Handling, Information &amp; Communications System, ETHICS, covers all Phases of a complex tendering Process:</i></p> <ul style="list-style-type: none"> <li><i>- Contract Administration and Legal Requirements</i></li> <li><i>- Market analysis - user Requirements and state-of-the-art Offerings</i></li> <li><i>- Requirements Assessment</i></li> <li><i>- Tender Process Planning and Management Process</i></li> <li><i>- Questionnaire Design Tool</i></li> <li><i>- Execution and Evaluation Process fully supported</i></li> </ul> <p><i>ETHICS is based on Best Practices - jointly developed by the Danish National Procurement Ltd. and constantly trimmed to leading edge technology.</i></p> <p><i>ETHICS is compliant with the EU Directives for Public</i></p>

	<p><i>Procurement and with World Bank recommendations.</i></p> <p><i>ETHICS is based on intuitive user interfaces and ease-of-use.</i></p> <p><i>ETHICS is based on leading edge technology from IBM Lotus and integrates through Open Standards with existing office systems, document repositories and common browsers.</i></p>
Identification of Application/Service Entities	<i>Described above.</i>
Procedural Details	<i>Describe the major procedures of the application/service</i>
Current status	<i>Operational for over 6 years</i>
Expected future developments	<i>Further functional enhancement to support Tender procedures and integration with existing Government operated applications (currently in Slovakia).</i>

<b>Responsible Organisation</b>	
Organisation Name	<i>Inno:vasion</i>
Organisation Type	<i>Private company.</i>
Date of questionnaire	12/06/2006

<b>Application/Service System Details</b>	
Communications Information	<i>The internet</i>
External interface	<i>Any browser and currently Adobe Acrobat (other form filling tools will be support in the near future.</i>
Data structures processed by the application	<i>HTML and XML data structures</i>

### 10.1.2 eSignature details

<b>Legal and strategically aspects</b>	
Does the system rely on a simple /	<i>Public Private Key Infrastructure (PKI)</i>

advanced / qualified / other signature?	<i>based on X.509 ver. 3</i>
Is the signature required/recommended?	<i>Yes, required for signing proposals and contracts.</i>
Which strategies are planned for the future? Should different types of the electronic signature be supported, or are the strategies only related to the wide distribution/extension/circulation of the qualified electronic signature?	
What is the legal basis (law, decree,...) for this application?	<i>EU directives for public procurement.</i>

<b>Technical aspects</b>	
What are the parties involved in the signature process?	<i>Bidder/vendor, contractor, procurer, ASP provider.</i>
What kind of token or credentials are used (smart cards, software certificates, paper tokens ...)?	<i>Personal certificates (software certificates)</i>
What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of eSignature?	<i>None</i>
What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?	<i>Any browser and currently Adobe Acrobat.</i>
What information is signed by the user and what is the objective of the signature?	<i>Commit proposals (by locking documents after they have been signed) and to prove their origin.</i>
Is this an application with multiple signatures for the same data and, if yes, what is the relationship between the signatures?	<i>Yes, when signing contracts.</i>
What are the relevant policies (CPS, certificate policy, signature policy)?	<i>OCES certificates</i>
How are the signature/certificate presented to the application?	<i>Adobe Acrobat</i>

What information is included in the certificate, and what is the role of this information in the functioning of the application?	<p><i>Name of person</i></p> <p><i>Issuer</i></p> <p><i>Issue date</i></p> <p><i>Expiry date</i></p> <p><i>Tender name</i></p> <p><i>Etc.</i></p>
Does the application rely on an existing generic eSignature framework (i.e. a set of commonly agreed standards)?	<i>Yes (OCES)</i>
How is the signature verified and how is the verification data processed and stored (directly connecting to the corresponding CA validation service or just through a Validation Service provided by a Validation Authority)?	<i>The verification process is currently done manually.</i>
What types of validation protocols are used for the electronic certificate validation? (OCSP, CRLs, SCVP...)	<i>CRL</i>
How is the long term validity of the signatures (including long-term archiving of certificates and signatures) ensured?	<i>Not applicable. During the tender procedure the issued certificates are only used for a short period of time.</i>

<b>Organisational aspects</b>	
Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?	<i>Public/private purchaser and vendor/supplier.</i>
Who are the relying parties <sup>16</sup> ? Describe the context?	<i>People authorized to sign for the institution or firm</i>
Who issues/manages credentials (e.g. certificates)? Describe the conditions and the procedure for the issuance of	

<sup>16</sup> « Relying Party » :shall mean an individual or organisation that acts in reliance on a Certificate or a eSignature

the credentials.	
What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be suspended or revoked?	<i>In a tender procedure it's typically one half year. For the contract between 2 to 4 years.</i>

### 10.1.3 Interoperability

Interoperability aspects	
Is the system accessible to non-nationals, and if so, how? If not, can the system be upgraded for cross-border interaction?	<i>The system is accessible for any one over the internet.  The system supports simultaneously any language supported/accepted by the purchasing entity (tender issuer), i.e. the system present the information to the end users according to the settings of the end users browser.</i>
What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?	<i>None</i>

### 10.1.4 Miscellaneous

Miscellaneous	
Are there any statistics on the actual use of electronic signatures for this application (if not: please provide an estimation)?	<i>Yes</i>
Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application;	<i>No</i>
Are there any Government initiatives aimed at providing/encouraging the use of eID/ eSignature *for this specific eGovernment application* (e.g. through an awareness programme)?	<i>Not specially</i>

### 10.1.5 Assessment

Assessment	
Please give your own assessment on the way how eSignature have been implemented in the concerned application (strengths, weaknesses).  Take this opportunity to bring any fruitful information that was not addressed by previous questions.	<i>Excellent. The system has been in operation for over 6 years and we've been able to process signed proposals from many different type of vendors without any training, i.e. from small firms consisting of only a few employees to large international companies.</i>

## 10.2 TastSelv Borger

### 10.2.1 Application identification

Application/Service Classification	
Application/Service Name	<i>TastSelv Borger</i>
Application/Service Type	<i>A2C (administration to citizen)</i>
Concerned sector	<i>Tax</i>
Application/Service Cross-Border Type	<i>None</i>
Level of Online Sophistication Type	<i>Stage 4: Transaction: Case handling; decision and delivery (payment)</i>
Intended "clients"	<i>natural persons; nationals; end-users and/or mandate holders ...</i>
Abstract Description	<i><b>TastSelv Borger</b> is the automated tax proces, with the least possible inconvenience to the citizens (which we call the "no touch strategy"). 97 percent of all data to the Danish citizens' tax declarations are reported by employers, banks, mortgage institutions, trade unions, social benefits administration etc. to The Central Customs and Tax Administration. The citizens can report corrections or approve their tax return via the Internet. The result in the form of an annual settlement can be seen immediately. If tax overpayments are due to a citizen, they are transferred to his bank account.</i>
Identification of Application/Service Entities	<i>All data to the Danish citizens' tax declarations</i>
Procedural Details	<i>Data are reported by third parties to the tax administration. The data are used to calculate a suggested result of the annual tax statement. If the taxpayer doesn't agree in the accuracy of the reported data, he can report a change to the specific data.</i>
Current status	<i>Operational</i>
Expected future developments	<i>From 2008 we expect not to issue a tax declaration to 60 - 70 % of the Danish taxpayers, because they will only</i>

	<i>receive the calculated result (which they can change if necessary).</i>
--	--

Responsible Organisation	
Organisation Name	<i>SKAT (The central tax and customs administration)</i>
Organisation Type	<i>National</i>
Date of questionnaire	<i>30/10/2006</i>

Application/Service System Details	
Communications Information	<i>You cannot have all this information in your questionnaire</i>
External interface	<p><i>All applications in the browser option have been established using standard web browsers as a client, and using standard HTML, Javascript and style sheet. The applications have been coded in Java and run on a number of web servers under Websphere.</i></p> <p><i>An XML interface has been defined for the annual settlement. The purpose is that annual settlement data can be transferred via web services following citizen approval to a bank or another private credit provider for use when citizens apply for loans in banks.</i></p> <p><i>Applets or similar plug-ins are not used, apart from Acrobat Reader for showing the edited annual settlements and the preliminary tax assessments. Consequently, this is a system of thin clients with validation, but without business logic. Presentation logic and partly business logic are run on the web servers that retrieve data from and deliver data to the mainframe systems via DB2 call (standard SQL) or IMS transactions.</i></p> <p><i>Encryption is made with 128 bits SSL via a proxy server.</i></p>
Data structures processed by the application	<i>You cannot have all this information in your questionnaire</i>

### 10.2.2 eSignature details

Legal and strategically aspects	
Does the system rely on a simple /	<i>Login has been established with a TASTSELV code (the tax administration has its own issuing of pincodes) or a digital</i>

advanced / qualified / other signature?	<p><i>signature.</i></p> <p><i>The OCES (national digital signature in Denmark) is an advanced but not a qualified signature.</i></p> <p><i>The TASTSELV code is a simple password solution.</i></p> <p><i>These logins give access to a joint menu structure, from where the taxpayer is given access to all e-services behind the access control, and from where it is possible to navigate between the different elements of the menu structure.</i></p> <p><i>Access control is based on entry of a password for the digital signature or keying in of the person's personal ID number and a TASTSELV code.</i></p>
Is the signature required/recommended?	<i>See above</i>
Which strategies are planned for the future? Should different types of the electronic signature be supported, or are the strategies only related to the wide distribution/extension/circulation of the qualified electronic signature?	<i>We will continue to make the access as easy as possible for the taxpayers to the website.</i>
What is the legal basis (law, decree,...) for this application?	<i>The data collection is based on law (The tax control act), but The specification of reporting methods and tools is not based on law but is decided by the tax administration.</i>

<b>Technical aspects</b>	
What are the parties involved in the signature process?	<p><i>Issuing of OCES signatures and PKI: TDC (telecom agency)</i></p> <p><i>Issuing of TASTSELV code: SKAT</i></p> <p><i>Certificate holder: citizen</i></p>
What kind of token or credentials are used (smart cards, software certificates, paper tokens ...)?	<i>Please explain. If OCES certificates are used: Personal certificates, employee certificates and/or company certificates – Software certificates/pincodes</i>
What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of eSignature?	<i>The OCES certificate is so far only a software certificate as far as the TastSelv Borger application is concerned. But we will implement hardware requirements when necessary/applicable.</i>
What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?	<i>No specific software requirements are needed.</i>

What information is signed by the user and what is the objective of the signature?	<i>The signature is used to sign the correction of the taxreturn, the preliminary assessment and to gain access to data in the digital archive. The signature also gives single sign-on acces to SKAT, SU-styrelsen and Økonomistyrelsen.</i>
Is this an application with multiple signatures for the same data and, if yes, what is the relationship between the signatures?	<i>No.</i>
What are the relevant policies (CPS, certificate policy, signature policy)?	<i>OCES</i>
How are the signature/certificate presented to the application?	<i>In a java applet.</i>
What information is included in the certificate, and what is the role of this information in the functioning of the application?	<i>OCES</i>
Does the application rely on an existing generic eSignature framework (i.e. a set of commonly agreed standards)?	<i>Yes – OCES</i>
How is the signature verified and how is the verification data processed and stored (directly connecting to the corresponding CA validation service or just through a Validation Service provided by a Validation Authority)?	<i>OCES certificates</i>
What types of validation protocols are used for the electronic certificate validation? (OCSP, CRLs, SCVP...)	<i>OCES certificates</i>
How is the long term validity of the signatures (including long-term archiving of certificates and signatures) ensured?	<i>?</i>

#### Organisational aspects

Which institutions, providers, etc. are involved in the signature scheme, and

*Apart from SKAT also SU-styrelsen and Økonomistyrelsen and the service provider CSC is involved.*

how do they relate?	
Who are the relying parties <sup>17</sup> ? Describe the context?	<i>As above</i>
Who issues/manages credentials (e.g. certificates)? Describe the conditions and the procedure for the issuance of the credentials.	<i>OCES certificates</i>
What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be suspended or revoked?	<i>OCES certificates</i>

---

<sup>17</sup> « Relying Party » :shall mean an individual or organisation that acts in reliance on a Certificate or a eSignature

### 10.2.3 Interoperability

Interoperability aspects	
Is the system accessible to non-nationals, and if so, how? If not, can the system be upgraded for cross-border interaction?	No
What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?	No

### 10.2.4 Miscellaneous

Miscellaneous																					
Are there any statistics on the actual use of electronic signatures for this application (if not: please provide an estimation)?																					
<table border="1"> <thead> <tr> <th>Optællinger på indkomstår 13/3-2/5</th> <th>2004</th> <th>2005</th> <th>Udvikling</th> <th>Udvikling i %</th> </tr> </thead> <tbody> <tr> <td>Antal login PIN</td> <td>2.765.020</td> <td>3.113.476</td> <td>348.456</td> <td>13%</td> </tr> <tr> <td>Antal login DS</td> <td>206.662</td> <td>487.248</td> <td>280.586</td> <td>136%</td> </tr> <tr> <td>Antal login i alt</td> <td>2.971.682</td> <td>3.600.724</td> <td>629.042</td> <td>21%</td> </tr> </tbody> </table>		Optællinger på indkomstår 13/3-2/5	2004	2005	Udvikling	Udvikling i %	Antal login PIN	2.765.020	3.113.476	348.456	13%	Antal login DS	206.662	487.248	280.586	136%	Antal login i alt	2.971.682	3.600.724	629.042	21%
Optællinger på indkomstår 13/3-2/5	2004	2005	Udvikling	Udvikling i %																	
Antal login PIN	2.765.020	3.113.476	348.456	13%																	
Antal login DS	206.662	487.248	280.586	136%																	
Antal login i alt	2.971.682	3.600.724	629.042	21%																	
<table border="1"> <thead> <tr> <th>Optællinger på indkomstår 13/3-2/5</th> <th>2004</th> <th>2005</th> <th>Udvikling</th> <th>Udvikling i %</th> </tr> </thead> <tbody> <tr> <td>Antal personer med login PIN</td> <td>1.148.182</td> <td>1.259.289</td> <td>111.107</td> <td>10%</td> </tr> <tr> <td>Antal personer med login DS</td> <td>64.379</td> <td>172.379</td> <td>108.000</td> <td>168%</td> </tr> <tr> <td>Antal personer med login i alt</td> <td>1.212.561</td> <td>1.431.668</td> <td>219.107</td> <td>18%</td> </tr> </tbody> </table>		Optællinger på indkomstår 13/3-2/5	2004	2005	Udvikling	Udvikling i %	Antal personer med login PIN	1.148.182	1.259.289	111.107	10%	Antal personer med login DS	64.379	172.379	108.000	168%	Antal personer med login i alt	1.212.561	1.431.668	219.107	18%
Optællinger på indkomstår 13/3-2/5	2004	2005	Udvikling	Udvikling i %																	
Antal personer med login PIN	1.148.182	1.259.289	111.107	10%																	
Antal personer med login DS	64.379	172.379	108.000	168%																	
Antal personer med login i alt	1.212.561	1.431.668	219.107	18%																	
<p>The first scheme is total number of logins (PIN=password - DS = digital signature). The second scheme is number of persons with a login.</p> <p>Hermed tal på anvendelsen af digital signatur ifm. login til SKATs TastSelv-Borger i selvangivelses indberetningsperioden (13. marts til den 2. maj).</p> <p>Forklaring:</p> <p>Login PIN = TastSelv-kode            Login DS = digital signatur            "Servicefællesskabet" = samarbejdet mellem SKAT, SU-styrelsen og Økonomistyrelsen om bl.a. fælles login via DS.</p> <p>Grafen herover viser login til SKATs TastSelv Borger i den nævnte periode.</p>																					

Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application;	
Are there any Government initiatives aimed at providing/encouraging the use of eID/ eSignature *for this specific eGovernment application* (e.g. through an awareness programme)?	Yes. ("Det offentlige – brug os på nettet")

### 10.2.5 Assessment

Assessment	
<p>Please give your own assessment on the way how eSignature have been implemented in the concerned application (strengths, weaknesses).</p> <p>Take this opportunity to bring any fruitful information that was not addressed by previous questions.</p>	<p>The implementation wasn't good enough. We are already making improvements on the implementation. But worst of all is the fact that the OCES certificate is not mobile but so far is only a software solution for the private users.</p>

## 10.3 NemKonto

### 10.3.1 Application identification

Application/Service Classification	
Application/Service Name	NemKonto-systemet (EasyAccount System)
Application/Service Type	A2A, A2B and A2C
Concerned sector	All payment systems in the entire public sector (state, regions and municipalities).
Application/Service Cross-Border Type	None.
Level of Online Sophistication Type	Stage 3: Two-way Interaction: Processing of forms inclusive authentication
Intended "clients"	All Danish citizens, companies and staff in public institutions handling payments.
Abstract Description	<p>All citizens and companies in Denmark have to have an NemKonto Easy Account (Mandatory). An Easy Account is a normal bank account which the citizen/company already has, and designate as their NemKonto Easy Account. All payments from public institutions are being transferred directly to this account via the Easy Account System (EAS).</p> <p>The EAS is a database with account numbers and social security numbers or company numbers.</p> <p>When a public institution make a payment to a citizen or company, the payment is made to a social security- or company number. The payment then goes from the institution's payment system to the EAS, which attaches an account number, and then to the institutions bank and further on to the citizen/company's bank account.</p> <p>This way all public payments are made electronically to bank accounts – no checks and cash payments.</p>
Identification of Application/Service Entities	Citizens, companies and staff in public institutions.
Procedural Details	<p>Online (at <a href="http://www.nemkonto.dk">www.nemkonto.dk</a>), it is possible to designate, change or delete and Easy Account for citizens and public institutions. They attain access by logging on to the website using their digital signature (eSignature).</p> <p>Staff in public institutions with the right user profile can log on to the website and stop payments or search for payments their institution has made.</p>

Current status	Operational in all public institution by Nov. 7 <sup>th</sup> 2006.
Expected future developments	None planned. But we are working on giving the private sector access to the system.

Responsible Organisation	
Organisation Name	The Danish Agency for Governmental Management
Organisation Type	National.
Date of questionnaire	25/10/2006

Application/Service System Details	
Communications Information	Website where either citizens/companies or staff in public institutions log on.
External interface	XML Broker and Web Server
Data structures processed by the application	SWIFT Customer to Bank Payment XML

### 10.3.2 eSignature details

#### OCES

Legal and strategically aspects	
Does the system rely on a simple / advanced / qualified / other signature?	Web access to the system requires a regular OCES signature for citizens and companies; and an OCES employee digital signature ("Medarbejdersignatur") for staff in public institutions.
Is the signature required/recommended?	Required.
Which strategies are planned for the future? Should different types of the electronic signature be supported, or are the strategies only related to the wide distribution/extension/circulation of the qualified electronic signature?	The Danish OCES Signature is required and there are no plans of changing this or supporting other types of signatures.
What is the legal basis (law, decree,...) for this application?	It is mandatory for all Danish citizens and companies to have an Easy Account. Citizens have to options of designating which account they want as an easy account

	<p>online (using the OCES). The two other options are designating it through their bank or public institution.</p> <p>For public institutions it is mandatory (last chance is nov. 7<sup>th</sup>, 2006) to send all payments through the EAS. If the wish to stop or search for a payment they <i>can</i> log on to the website (using their OCES). If they want to change an Easy Account for a company or citizen they <i>have to</i> log on to the website (using their OCES) in order to do this.</p>
--	--

<b>Technical aspects</b>	
<p>What are the parties involved in the signature process?</p>	<p>When logging on to the website <a href="http://www.nemkonto.dk">www.nemkonto.dk</a>, the EAS validates the signature with the provider, TDC (private company who has won the tender and provides the digital signature).</p> <p>The Agency for Governmental Management is responsible for the EAS which is developed by the private software company KMD A/S.</p> <p>For employees in public institutions using an employee digital signature, the signature is used to identify the user profile of the employee. This is done in the safety system "KSP/CICS".</p>
<p>What kind of token or credentials are used (smart cards, software certificates, paper tokens ...)?</p>	<p>For citizens: Personal OCES certificates. For companies: Company OCES certificates. For employees in public institutions: Employee OCES certificates.</p> <p>All software certificates.</p>
<p>What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of eSignature?</p>	<p>No hardware requirements.</p>
<p>What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?</p>	<p>The digital signature has to be requested from the provider TDC and installed on a personal computer.</p> <p>Requirements: Standard pc and internet.</p>
<p>What information is signed by the user and what is the objective of the signature?</p>	<p>For citizens:</p> <p>Identifying who they are, information about their Easy Account is shown, and the possibility for the citizen to change or deleting their Easy Account.</p>

	<p>For companies:</p> <p>Identifying who they are and information about their Easy Account is shown.</p> <p>For public institutions:</p> <p>Information about who they are, which institution they work in. This is linked to the safety system KSP/CICS which matches the OCES information with their user profile. According to this it is possible to look up, delete or change Easy Accounts for citizens and companies, stop and search for payments.</p>
Is this an application with multiple signatures for the same data and, if yes, what is the relationship between the signatures?	No, one signature per user.
What are the relevant policies (CPS, certificate policy, signature policy)?	
How are the signature/certificate presented to the application?	The website contains a link saying: "Log on using digital signature". A window opens and asks the user to select his/hers signature, and then asks for the password.
What information is included in the certificate, and what is the role of this information in the functioning of the application?	
Does the application rely on an existing generic eSignature framework (i.e. a set of commonly agreed standards)?	Yes.
How is the signature verified and how is the verification data processed and stored (directly connecting to the corresponding CA validation service or just through a Validation Service provided by a Validation Authority)?	
What types of validation protocols are used for the electronic certificate	

validation? (OCSP, CRLs, SCVP...)	
How is the long term validity of the signatures (including long-term archiving of certificates and signatures) ensured?	

<b>Organisational aspects</b>	
Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?	<p>TDC, the private company who provides the digital signature.</p> <p>National IT and Telecom Agency who has the contract with TDC.</p> <p>For NemKonto:</p> <p>Agency for Governmental Affairs and KMD.</p>
Who are the relying parties <sup>18</sup> ? Describe the context?	KMD updates the EAS according to the action the citizen or public institution has performed on the website.
Who issues/manages credentials (e.g. certificates)? Describe the conditions and the procedure for the issuance of the credentials.	
What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be suspended or revoked?	OCES

---

<sup>18</sup> « Relying Party » :shall mean an individual or organisation that acts in reliance on a Certificate or a eSignature

### 10.3.3 Interoperability

Interoperability aspects	
Is the system accessible to non-nationals, and if so, how? If not, can the system be upgraded for cross-border interaction?	No.  So far the law behind the system only apply to payments made form Danish public institutions made to Danish citizens and companies located in Denmark. It is, though, possible for people having a Danish social security number with a Danish OCES signature to access the system from outside of Denmark.
What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?	None.

### 10.3.4 Miscellaneous

Miscellaneous			
Are there any statistics on the actual use of electronic signatures for this application (if not: please provide an estimation)?	<b>Month</b>	<b>Citizen/company</b>	<b>Staff in public institution</b>
	08-2005	9.471	689
	09-2005	9.136	2.071
	10-2005	36.764	6.912
	11-2005	27.569	19.449
	12-2005	14.820	42.657
	01-2006	15.365	54.091
	02-2006	9.707	48.001
	03-2006	17.627	49.635
	04-2006	13.118	34.578
	05-2006	8.202	41.799
	06-2006	6.082	35.182
	07-2006	6.122	28.992
08-2006	7.481	33.762	
09-2006	6.492	34.761	
Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application;	We had to close down for the possibility for companies to designate their Easy Account online. The reason is, that in many (especially large) companies there is no control with which employee has the access to the company's signature. In order to prevent an employee from changing the Easy Account for the whole company, we closed down this option.		

<p>Are there any Government initiatives aimed at providing/encouraging the use of eID/ eSignature *for this specific eGovernment application* (e.g. through an awareness programme)?</p>	
--	--

### 10.3.5 Assessment

<b>Assessment</b>	
<p>Please give your own assessment on the way how eSignature have been implemented in the concerned application (strengths, weaknesses).</p> <p>Take this opportunity to bring any fruitful information that was not addressed by previous questions.</p>	<p>One bad thing: It has been quite a problem, that Danish citizens outside of Denmark could not retrieve an OCES signature.</p>

## 10.4 Sundhed.dk

### 10.4.1 Application identification

Application/Service Classification	
Application/Service Name	The Danish National eHealth Portal
Application/Service Type	A2A: Government to Hospital's, GP's, Pharmacies and other healthcare professionals. A2C: Citizens to Government, Hospital's, GP's, Pharmacies and other healthcare professionals.
Concerned sector	eHealth and shared care for Public healthcare and citizens.
Application/Service Cross-Border Type	If cross-borders means between countries this is None. The portal is for Denmark only.
Level of Online Sophistication Type	Stage 3
Intended "clients"	Government, Hospital's, GP's, Pharmacies and other healthcare professionals, Citizens.
Abstract Description	Sundhed.dk is the joint public health internet portal in Denmark ('sundhed' means health).  For the first time, sundhed.dk brings together the entire Danish health services on the Internet, making this the electronic way for patients, their families, and healthcare professionals to obtain information, communicate and maintain an overview.
Identification of Application/Service Entities	<b>Features - citizens</b> Features available for citizens: - Directory of names and addresses - Contact information - E-services (booking, prescription renewal, consultation)

	<ul style="list-style-type: none"> <li>- Health appointment calendar</li> <li>- Comparison of prices, quality and accessibility</li> <li>- E-commerce (pharmacies)</li> <li>- Information about prevention and treatment</li> <li>- Contact information</li> <li>- Medical information (eg. information about treatments)</li> <li>- Waiting list information from hospitals</li> <li>- Preventive medicine</li> <li>- Health laws and regulations</li> <li>- Access to own health data</li> <li>- Cross-sectorial personal electronic medicine profile</li> <li>- Patients' medical history (since 1977)</li> <li>- Shared care: Pregnancy Records</li> <li>- Online Donor Registration and access to own data</li> </ul> <p><b>Features - health professionals</b></p> <p>Features available for health care professionals:</p> <ul style="list-style-type: none"> <li>- Information for GPs</li> <li>- Patient appointment calendar</li> <li>- Web access to laboratory data</li> <li>- ICPC search of diagnoses from GP's electronic healthcare program (Linkportal)</li> <li>- Other data</li> <li>- Patient records (medicine records, medical records etc.)</li> <li>- Waiting list information from hospitals</li> <li>- Secure e-mail communication</li> <li>- Encyclopedias (Cochrane etc.)</li> <li>- Regional information</li> <li>- Contact information (authorities, departments, health personnel)</li> <li>- Visitation information from hospitals/regions</li> <li>- Preventive medicine</li> <li>- Health laws and regulations</li> <li>- Laboratories and consultants</li> <li>- Regional health reports</li> </ul>
--	--

Procedural Details	The user logs in to the portal using a Digital Certificate provided by the Danish government (OCES). There is one type of certificates for Citizens to access own information and one type for healthcare professionals to access patient data.
Current status	The Portal was launched in December 2003. Ever since more features have been added to the Portal Every 3 month.
Expected future developments	Support optimization of the Healthcare sector by supporting eHealth and shared care facilitating communication between sectors and access to own and patient data.

<b>Responsible Organisation</b>	
Organisation Name	The Danish National eHealth Portal (Danish Government)
Organisation Type	Government : National and Regional
Date of questionnaire	18/11/2006

<b>Application/Service System Details</b>	
Communications Information	<p>The Digital Certificates are used for identifying the users. When Identified by the Portal, the user have access to own data and for Healthcare professionals to patient data. The external systems are Lab-systems in hospitals, national medicine and patient databases.</p> <p>At the moment there is not any Certificate Signature exchange between systems. The security between systems is handles by a point-to-point private and secure network.</p> <p>At the moment there are pilot projects (SOSI) validating the exchanges of the signed certificates between systems.</p>
External interface	To National CA, Lab-systems in hospitals, national medicine and patient databases.

Data structures processed by the application	XML-based datastructure for National CA, Lab-systems in hospitals, national medicine and patient databases.
--	---

#### 10.4.2 eSignature details

Legal and strategically aspects	
Does the system rely on a simple / advanced / qualified / other signature?	<p>The Digital Certificates are used for identifying the users. When Identified by the Portal, the user have access to own data and for Healthcare professionals to patient data. The external systems are Lab-systems in hospitals, national medicine and patient databases.</p> <p>At the moment there is not any Certificate Signature exchange between systems. The security between systems is handles by a point-to-point private and secure network.</p> <p>At the moment there are pilot projects (SOSI) validating the exchanges of the signed certificates between systems.</p>
Is the signature required/recommended?	<p>The Digital Certificates are used for identifying the users. When Identified by the Portal, the user have access to own data and for Healthcare professionals to patient data. The external systems are Lab-systems in hospitals, national medicine and patient databases.</p> <p>At the moment there is not any Certificate Signature exchange between systems. The security between systems is handles by a point-to-point private and secure network.</p> <p>At the moment there are pilot projects (SOSI) validating the exchanges of the signed certificates between systems.</p>
Which strategies are planned for the future? Should different types of the electronic signature be supported, or are the strategies only related to the wide distribution/extension/circulation of the qualified electronic signature?	<p>At the moment there are pilot projects (SOSI) validating the exchanges of the signed certificates between systems. This is based on a national standard for Web Service Certificate based identification In different levels;</p> <ul style="list-style-type: none"> <li>- level a : username and password</li> <li>- level b : Company/organization certificate</li> <li>- level c : Personal certificates</li> <li>- etc.</li> </ul>

What is the legal basis (law, decree,...) for this application?	Danish law for privacy.
---	-------------------------

<b>Technical aspects</b>	
What are the parties involved in the signature process?	The Digital Certificates are used for identifying the users. The National CA and the Portal are involved.
What kind of token or credentials are used (smart cards, software certificates, paper tokens ...)?	Software certificates provides by the National CA. Some users copy this certificate to a "Token/Memory stick" and is used like a smart card.  OCES are used: Personal and employee.
What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of eSignature?	Standard PC with access to the Internet.
What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?	Standard Internet Browser.
What information is signed by the user and what is the objective of the signature?	The Digital Certificates are used for identifying the users.  At the moment there are pilot projects (SOSI) validating the exchanges of the signed certificates between systems.
Is this an application with multiple signatures for the same data and, if yes, what is the relationship between the signatures?	The Digital Certificates are used for identifying the users.  At the moment there are pilot projects (SOSI) validating the exchanges of the signed certificates between systems.
What are the relevant policies (CPS, certificate policy, signature policy)?	OCES
How are the signature/certificate presented to the application?	Call to the National CA using Web Services.  Standard handling of an Internet Browser.

What information is included in the certificate, and what is the role of this information in the functioning of the application?	OCES
Does the application rely on an existing generic eSignature framework (i.e. a set of commonly agreed standards)?	OCES
How is the signature verified and how is the verification data processed and stored (directly connecting to the corresponding CA validation service or just through a Validation Service provided by a Validation Authority)?	OCES
What types of validation protocols are used for the electronic certificate validation? (OCSP, CRLs, SCVP...)	OCES
How is the long term validity of the signatures (including long-term archiving of certificates and signatures) ensured?	OCES  (Revocation list at the CA is validated every time a user loges into the system. The CA revoke the Certificates automatically every 2 years)

<b>Organisational aspects</b>	
Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?	The Digital Certificates are used for identifying the users. So only the National CA is involved.  At the moment there are pilot projects (SOSI) validating the exchanges of the signed certificates between systems. For this pilot 2 hospitals(in Ribe and in Copenhagen) and the Danish Medicine Agency are involved.
Who are the relying parties <sup>19</sup> ? Describe the context?	Government, Hospital's, GP's, Pharmacies and other healthcare professionals, Citizens.

<sup>19</sup> « Relying Party » :shall mean an individual or organisation that acts in reliance on a Certificate or a eSignature

Who issues/manages credentials (e.g. certificates)? Describe the conditions and the procedure for the issuance of the credentials.	OCES
What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be suspended or revoked?	OCES

### 10.4.3 Interoperability

Interoperability aspects	
Is the system accessible to non-nationals, and if so, how? If not, can the system be upgraded for cross-border interaction?	At the moment you need an OCES certificate provided by the Danish National CA.  Though the application is an Internet application and can call other national CA's using OCES.
What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?	OCES

### 10.4.4 Miscellaneous

Miscellaneous	
Are there any statistics on the actual use of electronic signatures for this application (if not: please provide an estimation)?	Approx. 110.000 registered users with Certificates.
Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application;	No  Though a lot of legal issues with regards to consent – what consent are needed for a Healthcare professional to access a patient's data and what kind of IT checks and logging are needed.
Are there any Government initiatives aimed at providing/encouraging the use of eID/ eSignature *for this specific eGovernment application* (e.g. through an awareness programme)?	Yes.  The initiatives are primarily targeted at the health care professionals. A full implementation of OCES between the GP's is a part of the agreement between the Danish GP's and the Danish Healthcare Authorises.  There is also a national decision within the Danish regions to implement OCES as the primary way of identifying healthcare professionals in local EPR and national databases.  The activities is supported by various sundhed.dk specifikk awareness initiatives e.g. doctors conferences, newsletters to hospitals, GP's, dentists etc.  Sundhed.dk have no citizen focused OCES-campaigns, since the message about OCES is integrated in the PR activities following up the launch of new services on sundhed.dk.

#### 10.4.5 Assessment

Assessment	
<p>Please give your own assessment on the way how eSignature have been implemented in the concerned application (strengths, weaknesses).</p> <p>Take this opportunity to bring any fruitful information that was not addressed by previous questions.</p>	<p>Simple and secure infrastructure for validating the users. Simple for the citizens to get. The installation process can sometimes be a barrier for the use of Personal Certificates, but sundhed.dk try to support people in case of problems.</p> <p>Organisations need support for setting up the right organization for implementing, rolling out and administration employee certificates in own organization. Especially the fact that healthcare professionals need access to data from every bed in a hospital calls for other solutions than the current software based eSignature. The mobility issue is handled differently from hospital to hospital – but several organizations have started to implement a central certificate store – others consider different hardware solutions.</p>

## 10.5 Virk.dk

### 10.5.1 Application identification

Application/Service Classification	
Application/Service Name	<i>Virk.dk – a government portal for Danish businesses</i>
Application/Service Type	<i>A2B regarding information B2A regarding transactions etc. A2A regarding transactions from portal to relevant Government institution.</i>
Concerned sector	<i>Basically the key concept behind Virk.dk is that all transaction forms that Danish Businesses shall/may forward to Danish Government Institutions are accessible – either as text documents (for print) or as more sophisticated e-forms (where OCES is used).</i>
Application/Service Cross-Border Type	<i>None</i>
Level of Online Sophistication Type	<i>All of the 4 stages described underneath:</i> <ul style="list-style-type: none"> <li>• <i>Stage 1: Information: Online info about public services</i></li> <li>• <i>Stage 2: Interaction: Downloading of forms</i></li> <li>• <i>Stage 3: Two-way Interaction: Processing of forms inclusive authentication</i></li> <li>• <i>Stage 4: Transaction: Case handling; decision and delivery (payment)</i></li> </ul>
Intended “clients”	<i>Businesses</i>
Abstract Description	<i>Please see the describing enclosure</i>
Identification of Application/Service Entities	<i>Please see the describing enclosure</i>
Procedural Details	<i>Please see the describing enclosure</i>
Current status	<i>The Portal is currently preparing an invitation to tender</i>
Expected future developments	<i>The Portal is currently preparing an invitation to tender.</i>

**Responsible Organisation**

Organisation Name	<i>The main responsibility and financial benefactor is the Danish State, but organizational the portal is defined by a board constituted by public and private parties. On a daily basis the portal is run by a secretariat under The Danish Commerce and Companies Agency (Ministry of Economic and Business Affairs).</i>
Organisation Type	<i>National</i>
Date of questionnaire	27/10/2006

Application/Service System Details	
Communications Information	<i>Please see the describing enclosure</i>
External interface	<i>Internet Portal</i>
Data structures processed by the application	<i>Please see the describing enclosure</i>

### 10.5.2 eSignature details

Legal and strategically aspects	
Does the system rely on a simple / advanced / qualified / other signature?	<i>OCES</i>
Is the signature required/recommended?	<i>Yes</i>
Which strategies are planned for the future? Should different types of the electronic signature be supported, or are the strategies only related to the wide distribution/extension/circulation of the qualified electronic signature?	<i>No</i>
What is the legal basis (law, decree,...) for this application?	<i>We have more than 200 e-form on the portal, for most the are no specific user-rights but for others there are.</i>

Technical aspects	
What are the parties involved in the signature process?	<i>Portal owners and TDC (OCES provider)</i>

What kind of token or credentials are used (smart cards, software certificates, paper tokens ...)?	<i>OCES: employee certificates and company certificates</i>
What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of eSignature?	<i>Internet Access</i>
What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?	<i>Please see OCES</i>
What information is signed by the user and what is the objective of the signature?	<i>Various Transaction forms</i>
Is this an application with multiple signatures for the same data and, if yes, what is the relationship between the signatures?	<i>Can be: in some of the e-forms a signature is necessary from both Business and for instance a chartered accountant. When transaction is completed by the Business, the transaction is signed by the portals company certificate and the receiving institutions signs a receipt with their company certificate.</i>
What are the relevant policies (CPS, certificate policy, signature policy)?	<i>OCES</i>
How are the signature/certificate presented to the application?	<i>OpenSign and OpenLogin</i>
What information is included in the certificate, and what is the role of this information in the functioning of the application?	<i>OCES</i>
Does the application rely on an existing generic eSignature framework (i.e. a set of commonly agreed standards)?	<i>OCES</i>
How is the signature verified and how is the verification data processed and stored (directly connecting to the corresponding CA validation service or just through a Validation Service provided by a Validation Authority)?	<i>OCES</i>

What types of validation protocols are used for the electronic certificate validation? (OCSP, CRLs, SCVP...)	OCES
How is the long term validity of the signatures (including long-term archiving of certificates and signatures) ensured?	

Organisational aspects	
Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?	<i>All government institutions with transactions forms for businesses – currently 39 institutions</i>
Who are the relying parties <sup>20</sup> ? Describe the context?	One among the 450.000 Danish businesses, the Portal, and on of the 39 government institutions
Who issues/manages credentials (e.g. certificates)? Describe the conditions and the procedure for the issuance of the credentials.	OCES
What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be suspended or revoked?	OCES

### 10.5.3 Interoperability

Interoperability aspects	
Is the system accessible to non-nationals, and if so, how? If not, can the system be upgraded for cross-border interaction?	Non-nationals as being employees in Danish businesses – Yes.  Multinational Companies with a Danish Branch – Yes.  Otherwise – No.
What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?	We are participating in a working-group looking at this issue – primarily regarding the financial sector.

<sup>20</sup> « Relying Party » :shall mean an individual or organisation that acts in reliance on a Certificate or a eSignature

#### 10.5.4 Miscellaneous

Miscellaneous	
Are there any statistics on the actual use of electronic signatures for this application (if not: please provide an estimation)?	About 33.000 Danish Companies currently holds a signature, in these companies a total of about 115.000 employees holds a signature. In addition there is about 4000 company certificates around.
Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application;	Lots – but most are concerning the end-users administration and control of user-rights and written authorities.
Are there any Government initiatives aimed at providing/encouraging the use of eID/ eSignature *for this specific eGovernment application* (e.g. through an awareness programme)?	Many – currently we are marketing an application wich presumes OCES, the target-group is the 35.000 biggest Danish companies in terms of employees. And I am sure more initiatives will follow.

#### 10.5.5 Assessment

Assessment	
<p>Please give your own assessment on the way how eSignature have been implemented in the concerned application (strengths, weaknesses).</p> <p>Take this opportunity to bring any fruitful information that was not addressed by previous questions.</p>	<p>Strengths: Stable and secure</p> <p>Weaknesses: Usability, price, usage</p>

## 10.6 Netborger.dk

### 10.6.1 Application identification

Application/Service Classification																																		
Application/Service Name	<p><i>Provide the Application/Service Name:</i></p> <p><i>Netborger.dk</i></p>																																	
Application/Service Type	<p><i>Provide the Application/Service Type: A2A (administration to administration), A2B (administration to business) or A2C (administration to citizen) (Provide all that apply)</i></p> <p><i>Netborger is a portal for a suite of A2B solutions, where local municipalities can offer self-service to their citizens.</i></p> <p><i>The portal by itself provides authentication of the user when needed, and supplies information on Danish municipalities in general.</i></p>																																	
Concerned sector	<p><i>Public procurement, tax, social security, employment, financial management, justice, education, transportation and logistics, customs...</i></p> <p><i>Public service, including information and application of various issues handled by the municipality.</i></p>																																	
Application/Service Cross-Border Type	<p><i>Provide the Application/Service Cross-Border Type: (None, Bilateral or Multilateral)</i></p> <p><i>Multilateral</i></p>																																	
Level of Online Sophistication Type	<p><i>Provide the Level of Online Sophistication Type as defined by eGovernment indicators for benchmarking eEurope (22/02/2001):</i></p> <ul style="list-style-type: none"> <li>• <i>Stage 1: Information: Online info about public services</i></li> <li>• <i>Stage 2: Interaction: Downloading of forms</i></li> <li>• <i>Stage 3: Two-way Interaction: Processing of forms inclusive authentication</i></li> <li>• <i>Stage 4: Transaction: Case handling; decision and delivery (payment)</i></li> </ul> <p><i>Several applications are provided through the portal. These are different stages.</i></p> <table border="1"> <thead> <tr> <th>Stage</th> <th>Applikationsnavn</th> <th>URL</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>Ansøgning om folkepension</td> <td><a href="https://pensionsguiden.netborger.dk">https://pensionsguiden.netborger.dk</a></td> </tr> <tr> <td>2</td> <td>BBR-Tjek</td> <td><a href="http://bbr-tjek.netborger.dk">http://bbr-tjek.netborger.dk</a></td> </tr> <tr> <td></td> <td>Beregn børnetilskud til forældre under uddannelse</td> <td><a href="http://boernetilskud-uddannelse.netborger.dk">http://boernetilskud-uddannelse.netborger.dk</a></td> </tr> <tr> <td>4</td> <td>Betal din kommune</td> <td><a href="http://betaldinkommune.netborger.dk/def:">http://betaldinkommune.netborger.dk/def:</a></td> </tr> <tr> <td></td> <td>BetalingsService</td> <td><a href="http://betalingservice.netborger.dk/produ">http://betalingservice.netborger.dk/produ</a></td> </tr> <tr> <td></td> <td></td> <td><a href="http://budgetmodul.netborger.dk/budget/">.asp</a></td> </tr> <tr> <td>3</td> <td>Budgetmodul</td> <td><a href="http://budgetmodul.netborger.dk/budget/">http://budgetmodul.netborger.dk/budget/</a></td> </tr> <tr> <td></td> <td>Byggesagsguiden</td> <td><a href="http://byggesagsguiden.netborger.dk/proce">http://byggesagsguiden.netborger.dk/proce</a></td> </tr> <tr> <td></td> <td></td> <td><a href="http://dinbarselsorlov.netborger.dk">.asp</a></td> </tr> <tr> <td>3</td> <td>Din Barselsorlov</td> <td><a href="http://dinbarselsorlov.netborger.dk">http://dinbarselsorlov.netborger.dk</a></td> </tr> </tbody> </table>	Stage	Applikationsnavn	URL	3	Ansøgning om folkepension	<a href="https://pensionsguiden.netborger.dk">https://pensionsguiden.netborger.dk</a>	2	BBR-Tjek	<a href="http://bbr-tjek.netborger.dk">http://bbr-tjek.netborger.dk</a>		Beregn børnetilskud til forældre under uddannelse	<a href="http://boernetilskud-uddannelse.netborger.dk">http://boernetilskud-uddannelse.netborger.dk</a>	4	Betal din kommune	<a href="http://betaldinkommune.netborger.dk/def:">http://betaldinkommune.netborger.dk/def:</a>		BetalingsService	<a href="http://betalingservice.netborger.dk/produ">http://betalingservice.netborger.dk/produ</a>			<a href="http://budgetmodul.netborger.dk/budget/">.asp</a>	3	Budgetmodul	<a href="http://budgetmodul.netborger.dk/budget/">http://budgetmodul.netborger.dk/budget/</a>		Byggesagsguiden	<a href="http://byggesagsguiden.netborger.dk/proce">http://byggesagsguiden.netborger.dk/proce</a>			<a href="http://dinbarselsorlov.netborger.dk">.asp</a>	3	Din Barselsorlov	<a href="http://dinbarselsorlov.netborger.dk">http://dinbarselsorlov.netborger.dk</a>
Stage	Applikationsnavn	URL																																
3	Ansøgning om folkepension	<a href="https://pensionsguiden.netborger.dk">https://pensionsguiden.netborger.dk</a>																																
2	BBR-Tjek	<a href="http://bbr-tjek.netborger.dk">http://bbr-tjek.netborger.dk</a>																																
	Beregn børnetilskud til forældre under uddannelse	<a href="http://boernetilskud-uddannelse.netborger.dk">http://boernetilskud-uddannelse.netborger.dk</a>																																
4	Betal din kommune	<a href="http://betaldinkommune.netborger.dk/def:">http://betaldinkommune.netborger.dk/def:</a>																																
	BetalingsService	<a href="http://betalingservice.netborger.dk/produ">http://betalingservice.netborger.dk/produ</a>																																
		<a href="http://budgetmodul.netborger.dk/budget/">.asp</a>																																
3	Budgetmodul	<a href="http://budgetmodul.netborger.dk/budget/">http://budgetmodul.netborger.dk/budget/</a>																																
	Byggesagsguiden	<a href="http://byggesagsguiden.netborger.dk/proce">http://byggesagsguiden.netborger.dk/proce</a>																																
		<a href="http://dinbarselsorlov.netborger.dk">.asp</a>																																
3	Din Barselsorlov	<a href="http://dinbarselsorlov.netborger.dk">http://dinbarselsorlov.netborger.dk</a>																																

	<p>4 Din Boligstøtte <a href="http://dinboligstoette.netborger.dk">http://dinboligstoette.netborger.dk</a></p> <p>4 Din Borgerkonto <a href="http://dinborgerkonto.netborger.dk">http://dinborgerkonto.netborger.dk</a></p> <p>3 Din Skattesag <a href="http://dinskattesag.netborger.dk">http://dinskattesag.netborger.dk</a></p> <p>3 dinejendom2g <a href="http://dinejendom.netborger.dk/produkt/fo">http://dinejendom.netborger.dk/produkt/fo</a> <a href="http://ejendomsfakta.netborger.dk/produk">http://ejendomsfakta.netborger.dk/produk</a></p> <p>1 Ejendomsfakta <a href="http://ejendomsfakta.netborger.dk/produk">http://ejendomsfakta.netborger.dk/produk</a> <a href="http://ejendomsfakta.netborger.dk/produk">asp</a></p> <p>2 e-service forsider <a href="http://e-services.borgerservice.dk/produkt/default">http://e-</a> <a href="http://e-services.borgerservice.dk/produkt/default">este=ligestilling</a></p> <p>1 Familieydelsesberegner <a href="http://www2.netborger.dk/beregning/famil">http://www2.netborger.dk/beregning/famil</a> <a href="http://www2.netborger.dk/beregning/famil">beregning.aspx</a></p> <p>4 FAS c/s Internet <a href="http://maalertjek.netborger.dk/default.asp">http://maalertjek.netborger.dk/default.asp</a></p> <p>3 Flytteguiden <a href="http://flytteguiden.netborger.dk">http://flytteguiden.netborger.dk</a></p> <p>1 Institutionsfakta <a href="http://institutionsfakta.netborger.dk/">http://institutionsfakta.netborger.dk/</a></p> <p>1 KommuneFakta <a href="http://kommunefakta.netborger.dk">http://kommunefakta.netborger.dk</a></p> <p>3 Opskriv dit barn <a href="http://institution-opskrivning.netborger.dk">http://institution-opskrivning.netborger.dk</a></p> <p>2 Pasningsguiden <a href="http://pasningsguiden.netborger.dk">http://pasningsguiden.netborger.dk</a></p> <p>2 Pensionsguide <a href="http://pensionsguiden.netborger.dk">http://pensionsguiden.netborger.dk</a></p> <p>3 Placering på venteliste <a href="http://institution-placering.netborger.dk/">http://institution-placering.netborger.dk/</a> <a href="http://www2.borgerservice.dk/privatoekon">http://www2.borgerservice.dk/privatoekon</a></p> <p>1 Privatøkonomisk test <a href="http://www2.borgerservice.dk/privatoekon">/</a></p> <p>1 Selvbetjening <a href="http://www.netborger.dk/blanketter_v1/de">http://www.netborger.dk/blanketter_v1/de</a> <a href="http://www2.netborger.dk/selvbetjening/de">http://www2.netborger.dk/selvbetjening/de</a></p> <p>1 Selvbetjening 2 <a href="http://www2.netborger.dk/selvbetjening/de">x</a></p> <p>3 Syge- og barseldagpenge <a href="http://dagpenge-anmodning.netborger.dk/">http://dagpenge-anmodning.netborger.dk/</a></p> <p>3 Sygesikring <a href="http://sygesikring.netborger.dk/">http://sygesikring.netborger.dk/</a></p> <p>3 Søg børnetilskud <a href="http://boernetilskud-ansoegning.netborger">http://boernetilskud-ansoegning.netborger</a></p> <p>4 Udmeld dit barn <a href="http://institution-udmeldelse.netborger.dk/">http://institution-udmeldelse.netborger.dk/</a></p> <p>3 Vurderingsfortegnelsen <a href="http://vurdering.netborger.dk/">http://vurdering.netborger.dk/</a></p> <p>3 Økonomisk friplads <a href="http://institution-fripladsansoegning.netbo">http://institution-fripladsansoegning.netbo</a></p>
Intended "clients"	<p><i>Provide intended "clients": natural and/or legal persons; nationals and/or non-nationals; end-users and/or mandate holders ...</i></p> <p><i>The citizens of the municipality</i></p>
Abstract Description	<p><i>Give an abstract description of the application:</i></p> <p><i>Self-service are provided thru access to information in legacy systems. This information can be information on rules or application for public services or financial support</i></p>
Identification of Application/Service Entities	<p><i>Identify the important entities of the application/service</i></p> <p><i>Besides access to public and private information, the portal consists of a portal server, where access to the application servers are provided. The logon is done on a Common Logonserver, which provides single sign on for the user to this portal and other public portals. The webserver access legacy systems to provide</i></p>

	<i>the relevant information.</i>
Procedural Details	<i>Describe the major procedures of the application/service</i>
Current status	<i>Precise the current status of the described application (planned, specification phase, development phase, operational)</i> <i>Operational</i>
Expected future developments	<i>Describe the application's owner intentions.</i> <i>Indented to become the entrance to the public sector in Denmark, concerning self service for all citizen.</i>

Responsible Organisation	
Organisation Name	<i>Provide the name of the responsible organisation:</i> <i>LGDK - Local Authority Interest Association</i>
Organisation Type	<i>Provide the type of organisation: whether it is National, Regional or Local</i> <i>National</i>
Date of questionnaire	xx/xx/2006

Application/Service System Details	
Communications Information	<i>Identify the System's (important to the Application/Service) Communications components</i> <i>NA.</i>
External interface	<i>Identify the System's External Interface</i> <i>Webserver</i>
Data structures processed by the application	<i>Identify the data structures processed by the Application/Service</i> <i>NA.</i>

### 10.6.2 eSignature details

Legal and strategically aspects	
Does the system rely on a simple / advanced / qualified / other signature?	<i>Please explain</i> <i>Services support the OCES certificate.</i>

	<p><i>Signing are done using the OpenSource component at <a href="http://www.OPENOCES.org">www.OPENOCES.org</a></i></p> <p><i>Futhermore the CommonPinCode are supportet, together with the common Danish NetBank logon system.</i></p>
Is the signature required/recommended?	<p><i>Please explain</i></p> <p><i>Nonrepudiation can be achieved using different technologies. Digital signature are one. Another are system proof, where logging of user actions can be sufficient proof.</i></p>
Which strategies are planned for the future? Should different types of the electronic signature be supported, or are the strategies only related to the wide distribution/extension/circulation of the qualified electronic signature?	<p><i>Support for further ID tokens will be needed. ie Support for SAML v2, for support of federated identity.</i></p>
What is the legal basis (law, decree,...) for this application?	<p><i>Provide regulation short description and reference to on-line resources</i></p> <p><i>A variety of Danish legislation.</i></p>

<b>Technical aspects</b>	
What are the parties involved in the signature process?	<p><i>Please explain</i></p> <p><i>The webserver holding the portal.( Need identification of the user)</i></p> <p><i>The common logon server (Requests the certificate.).</i></p> <p><i>The Certificate issuer ( revocation list etc.)</i></p>
What kind of token or credentials are used (smart cards, software certificates, paper tokens ...)?	<p><i>Please explain. If OCES certificates are used: Personal certificates, employee certificates and/or company certificates</i></p> <p><i>Personal certificates, employee certificates and company certificates are supported.</i></p>
What are the hardware requirements on the client side (e.g. smartcard	<p><i>Please explain</i></p> <p><i>No hardware requirements.</i></p>

reader/USB tokens) for the use of eSignature?	
What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?	<i>Please explain</i> <i>No software requirements.</i>
What information is signed by the user and what is the objective of the signature?	<i>Please explain</i> <i>Applications for financial support. The application are storing the signed application for future reference.</i>
Is this an application with multiple signatures for the same data and, if yes, what is the relationship between the signatures?	<i>Please explain</i> <i>No</i>
What are the relevant policies (CPS, certificate policy, signature policy)?	<i>No answer needed if the application solely relies on OCES certificates</i> <i>OCES</i>
How are the signature/certificate presented to the application?	<i>Please explain</i> <i>The application only sees the subject serial number which contains the unik ID.</i>
What information is included in the certificate, and what is the role of this information in the functioning of the application?	<i>No answer needed if the application solely relies on OCES certificates</i> <i>OCES</i>
Does the application rely on an existing generic eSignature framework (i.e. a set of commonly agreed standards)?	<i>If yes (OCES) no further answer is needed. OCES</i> <i>If no, specify which standards have been implemented in the eSignatures application? Depending on the signature type, this may include standards regarding certificates, signature formats, signature algorithms, token formats, other information security standards, etc.</i>
How is the signature verified and how is the verification data processed and stored (directly connecting to the corresponding CA validation service or just through a Validation Service provided by a Validation Authority)?	<i>No answer needed if the application solely relies on OCES certificates</i> <i>OCES</i>
What types of validation protocols are used for the electronic certificate validation? (OCSP, CRLs, SCVP...)	<i>No answer needed if the application solely relies on OCES certificates</i>

	OCES
How is the long term validity of the signatures (including long-term archiving of certificates and signatures) ensured?	System logfiles.

Organisational aspects	
Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?	<i>Only application specific parties should be described</i> OCES
Who are the relying parties <sup>21</sup> ? Describe the context?	OCES
Who issues/manages credentials (e.g. certificates)? Describe the conditions and the procedure for the issuance of the credentials.	<i>No answer needed if the application solely relies on OCES certificates</i> OCES
What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be suspended or revoked?	<i>No answer needed if the application solely relies on OCES certificates</i> OCES

---

<sup>21</sup> « Relying Party » :shall mean an individual or organisation that acts in reliance on a Certificate or a eSignature

### 10.6.3 Interoperability

Interoperability aspects	
Is the system accessible to non-nationals, and if so, how? If not, can the system be upgraded for cross-border interaction?	<p>Self-service are only intended for Danish Citizens, and other people living in Denmark.</p> <p>The authentication server could be extended to accept certificates issued by other CAs.</p>
What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?	<p>OCES</p> <p>The OCES certificates are using the definitions for Qualified certificates specified by Danish Standard U27, which follows the EU regulation for Qualified certificates.</p>

### 10.6.4 Miscellaneous

Miscellaneous	
Are there any statistics on the actual use of electronic signatures for this application (if not: please provide an estimation)?	<p>Week 43, 2006: app. 800.000 logins, of which app. 25% are using OCES certificates : 200.000 certificate login.</p>
Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application;	<p>No</p>
Are there any Government initiatives aimed at providing/encouraging the use of eID/ eSignature *for this specific eGovernment application* (e.g. through an awareness programme)?	<p>OCES</p>

### 10.6.5 Assessment

Assessment	
Please give your own assessment on the way how eSignature have been implemented in the concerned application (strengths, weaknesses).	<p>OCES</p>

Take this opportunity to bring any fruitful information that was not addressed by previous questions.	
---	--