IDABC
European
eGovernment Services

Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications

NATIONAL PROFILE NETHERLANDS

April 2007

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

Author's name: Arno R.Lodder, Vrije Universiteit Amsterdam

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

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 Nertherlands eGovernment applications.

Table of Contents

1 Documents

1.1 Applicable Documents

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

1.2 Reference Documents

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

  Again, this definition may cover non-PKI solutions.

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[1].

[1] 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

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

3 General eGovernment structure

The Netherlands was amongst the first European countries to start with eGovernment initiatives.[2] Already in 1994 the so called National Action program for the Electronic Highway was launched. In 1998 followed the National Action program for Electronic Government and in 1999 The Digital Delta – Netherlands Online.[3] One example of an early Dutch eGovernment initiative on e-signatures is the electronic income tax declaration, that was already mentioned in the Draft of the European Electronic signatures Directive [RD3].

As the above initiatives illustrate, the most Important eGovernment drivers can be found at a national level. Despite all the plans that were drafted, the actual implementation of those plans did not live to the expectations. One reason has been that the central government is not really in a position to force local governments concerning the use of Information Technology.[4] In recent years, though, at all levels of the government initiatives started, including the electronic communications between government and citizens using electronic signatures. The legislation on electronic communications in the General Administrative Law Act (Algemene Wet Bestuursrecht) enacted in the summer of 2004 has contributed to this development.

In April 2006 the government decided to invest 55 million euro into eGovernment.[5] Parties involved were amongst others the Ministry of Internal Affairs and the Association of Dutch Municipalities (VNG).

At this moment, the end of 2006, at all government levels actual implementation of initiatives on electronic communication between governments and citizens/companies is taking place. In the remainder of this report several examples will be discussed.

To conclude this introductory chapter, a general noteworthy initiative is the e-Citizen Charter defined by the Ministry of Internal affairs. The charter deals with quality requirements for e-government, viz. digital contacts. Each requirement is formulated as a right of a citizen and a corresponding duty of government. It can be found at the website of Burger@Overheid.nl (www.burger.overheid.nl)[6] and contains the following ten principles:

[2] See http://www.e-overheid.nl/e-overheid/geschiedenis/#Nederlandenegovernment

[3] *Kamerstukken* II, 1998/99, 26 643, nr. 1 (see www.overheid.nl/op).

[4] Leenes, Ronald E., "Local e-Government in the Netherlands: From Ambitious Policy Goals to Harsh Reality" (December 2004). Institute of Technology Assessment Working Paper No. ITA-04-04. Available at SSRN: http://ssrn.com/abstract=646701.

[5] http://www.minbzk.nl/onderwerpen/ict_en_de_overheid/administratieve/nieuws_en?ActItmIdt=81256

[6] Burger@Overheid.nl is an independent platform which stimulates the development of e-government from the citizen's point of view. To that end it involves citizens, advises government bodies and monitors progress. Burger@overheid regularly conducts surveys with its own People's Panel, annually grants the Webwise Awards for good practices and at present is developing a so called e-Citizen Charter with quality requirements for e-government. Burger@overheid is an initiative of the Ministry of the Interior. The bureau is part of ICTU, the Dutch implementation organization for ICT in the public sector. A Steering Committee representing citizen's interest groups supervises the proceedings.

1. Choice of Channel

As a citizen I can choose for myself in which way to interact with government.

Government ensures multi channel service delivery, i.e. the availability of all communication channels: counter, letter, phone, e-mail, internet.

2. Transparent Public Sector

As a citizen I know where to apply for official information and public services.

Government guaranties one-stop-shop service delivery and acts as one seamless entity with no wrong doors.

3. Overview of Rights and Duties

As a citizen I know which services I am entitled to under which conditions.

Government ensures that my rights and duties are at all times transparent.

4. Personalised Information

As a citizen I am entitled to information that is complete, up to date and consistent. Government supplies appropriate information tailored to my needs.

5. Convenient Services

As a citizen I can choose to provide personal data once and to be served in a proactive way.

Government makes clear what records it keeps about me and does not use data without my consent.

6. Comprehensive Procedures

As a citizen I can easily get to know how government works and monitor progress. Government keeps me informed of procedures I am involved in by way of tracking and tracing.

7. Trust and Reliability

As a citizen I presume government to be electronically competent.

Government guarantees secure identity management and reliable storage of electronic documents.

8. Considerate Administration

As a citizen I can file ideas for improvement and lodge complaints.

Government compensates for mistakes and uses feedback information to improve its products and procedures.

9. Accountability and Benchmarking

As a citizen I am able to compare, check and measure government outcome.

Government actively supplies benchmark information about its performance.

10. Involvement and Empowerment

As a citizen I am invited to participate in decision-making and to promote my interests. Government supports empowerment and ensures that the necessary information and instruments are available.http://www.burger.overheid.nl/service_menu/english/who_we_are - top

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 Dutch legislation through:

- Act of 8 May 2003 (Act on electronic signatures), entered into force on May 21, 2003.[7]

- Royal decree of 8 May 2003 defining the requirements for Certification Service Providers, entered into force on May 21, 2003.[8]

- Ministerial regulation of 6 May 2003 on electronic signatures, entered into force on May 21, 2003.[9]

- Guidelines of the Ministry of Economic Affairs on Certification Service Providers, entered into force on May 21, 2003[10]

The Act on electronic signatures determines in the Civil Code the legal status of electronic signatures as well as liability of CSPs. The Telecommunication Act includes definitions of CSPs and the Act on Economic Offences includes penalties on crimes related to CSPs and certificates.

The Dutch legislator did on most points literally follow the definitions of European Directive. The Dutch legislator introduced a general norm for electronic signatures that defined the electronic signature to be legally valid if the method of authentication can be trusted. The level of trust can vary from situation to situation, because it is said that whether an authentication method can be trusted depends on the purpose for which the signature is used, and all other circumstances (Article 3:15d lid BW). The qualified signature is mentioned as a method of authentication that unless proven otherwise is considered trustworthy and as a consequence is seen as legally valid. An electronic signature is defined according to the Directive’s definition of a normal signature.

The Act on electronic signatures foresees that the rules laid down in the Civil Code can also be applied in other domains.[11] The explanatory memorandum of the Act on electronic signatures

[7] Stb. 2003, 1999 (see http://overheid.nl/op). *Aanpassing van Boek 3 en Boek 6 van het Burgerlijk Wetboek, de Telecommunicatiewet en de Wet op de economische delicten inzake elektronische handtekeningen ter uitvoering van richtlijn nr. 1999/93/EG van het Europees Parlement en de Raad van de Europese Unie van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG L 13) (Wet elektronische handtekeningen).*

[8] *Stb.* 2003, 200 (see http://overheid.nl/op). Besluit van 8 mei 2003, houdende de vaststelling van eisen voor het verlenen van diensten voor elektronische handtekeningen,

[9] *Stcrt.* 8 mei 2003, nr. 88, p. 9, see http://www.sdu.nl/staatscourant/ (Regeling van de Staatssecretaris van Economische Zaken van 6 mei 2003, nr. WJZ/03/02263, houdende nadere regels met betrekking tot elektronische handtekeningen.

[10] *Stcr.* 8 mei 2003, p. 10, see http://www.sdu.nl/staatscourant/ Beleidsregel van de Staatssecretaris van Economische Zaken met betrekking tot de aanwijzing van organisaties die certificatiedienstverleners toetsen op de overeenstemming met de bij of krachtens de Telecommunicatiewet gestelde eisen, op grond van artikel 18.16 van de Telecommunicatiewet,

mentions Administrative law and Penal law as examples. However, it is indicated that the articles of the Civil Code can be applied in other domains, unless the nature of the act or the legal relation does not allow such application.

Recently there are also initiatives regarding Criminal Procedural Law.[12] Previously, in the summer of 2004, the Act on electronic governmental communication (Wet elektronisch bestuurlijk verkeer) has been enacted.[13] The additional rules in the General Act on Administrative Law (Algemene Wet Bestuursrecht) are addressed below.

4.2 eGovernment regulatory framework

The legal basis for the introduction of electronic signatures in eGovernment applications can be found in the already mentioned 2004 Act on electronic governmental communication. The general principles of this Act are:

1. The governmental organization communicates electronically, only if it has indicated to be reachable by e-mail or other electronic means;
2. The citizen gets the information in the format it desired (e.g. electronically).

The Act also lays down a general norm[14] on the use of e-signatures, comparable to the one defined in the Civil Code. Again the authentication method is taken as the starting point. The requirements for signing are met if the method used for authentication is sufficient trustworthy. The nature and the content of the communication as well as the purpose for which it was sent have to be taken into account.

Currently, two types of electronic signatures are predominantly used in eGovernment applications:

1. PKI; and, in particular
2. DigiD.

Since the beginning of 2006 GBO.Overheid[15] is responsible for the tactical and operational management and maintenance of generic shared key-services for e-government. This concerns:

- Supportting the management and control of the PKIoverheid system.
- Administration of DigiD, the authentication service;
- An infrastructure for the exchange of data through the government transaction portal (GTP);
- Forum Standardisation;
- Security tasks (GOVCERT.NL and the Policy Authority).

[11] Article 3:15c BW.

[12] Advice by A.R. Lodder & H.W.K. Kaspersen to the Dutch Ministry of Justice on how to amend the Act on Criminal Procedural Law regarding the signing of documents in an electronic environment, October 2006 (eSV? Analyse van artikelen die vanwege het vereiste van ondertekening aan elektronische strafvordering in de weg staan).

[13] *Stb.* 2004, 260 (see www.overheid.nl/op)/

[14] Article 2:17 Awb (General Act on Administrative Law).

[15] http://gbo.overheid.nl/

Both PKI overheid and DigiD are described in more detail below, before discussing how they have been implemented in eGovernment applications. The role of the eNIK (Electronic Identit oCard) will also be commented upon.

For further information, see also http://www.e-overheid.nl/

4.2.1 PKI overheid

The PKI Overheid realizes the Public Key infrastructure, and has been preceded by the National TTP project that started in the late 1990s. Several governmental services make use of the PKI.

A national PKI certificate hierarchy has been realised. This national hierarchy consists of 1 root and 2 domains (sub-CAs) each having Certificate Service Providers (CSPs) underneath. GBO.overheid[16] supports the Dutch Minister of Interior and Kingdom Relations with the management and control of the PKIoverheid system.

Each CSP can issue several types of certificates (e.g. authentication, encryption, non-repudiation, service (such as SSL)). Before being allowed as a CSP in the national PKI hierarchy the CSP needs to prove that it complies with ETSI TS 101 456 (European specification for qualified certificates) and additional governmental PKI requirements contained in the Programme of Requirements (*Programma van Eisen*).

The Programme of Requirements is based on Dutch legislation and European standards.

4.2.2 Digital Identity (DigiD)[17]

4.2.2.1 What is DigiD?

DigiD stands for Digital Identity and is a system shared between cooperating governmental agencies, allowing to digitally authenticate the identity of a person who applies for a transaction service via internet. With increasing numbers of public authority offices implementing the DigiD system, it is easy to begin using their range of electronic services after first choosing your own login code (user's name and password) at www.DigiD.nl. In short: DigiD provides users with a personalised login code for the full spectrum of contact with various governmental bodies. Anyone with a Social Fiscal number (SOFI-nummer) can apply for a DigiD.

The Social Insurance Institute (SVB, Sociale Verzekeringsbank), the Centre for Work and Income (CWI, Centrum voor Werk en Inkomen), the Employees' Insurance and Benefits Office (UWV, Uitvoeringsinstituut Werknemersverzekeringen), the Tax Authorities (Belastingdienst) and increasing numbers of local authorities are already connected up to DigiD, with many institutions following their example. An up to date list of participating agencies can be consulted under the section burger / wie doen mee? (citizen / who's joining up?). At the end of November 2006 already 20 % of the Dutch municipalities participated.

4.2.2.2 Examples of services

The number of electronic services available through DigiD is continually increasing. It's already possible to submit online applications to the Social Insurance Institute (SVB) for child benefit allowances and statutory old age pensions as well as digitally signing a tax declaration at the Tax

[16] http://gbo.overheid.nl/

[17] Information taken from http://www.digid.nl/english/, with some modifications.

Authorities (Belastingdienst). You can also contact an increasing number of municipal authorities for internet based services including:

- Requesting a copy of the municipal personal records database
- Applying for various permits
- Notification of a change in address
- Act on the value of real estate
- Paying municipal taxes
- Paying parking fines

4.2.2.3 Levels of authentication

In most cases, user name and password of DigiD offers governmental agencies sufficient assurance of your identity, in addition to the registered address at your municipality, to which the code is send. This is a 'basic' security level, but in certain instances government agencies obviously require additional means of authentication: these are 'medium' or 'high' security levels. This could involve the exchange of (more) sensitive private data. It is the government agency however that decides upon which of these security levels it is necessary to authenticate yourself.

4.2.2.4 SMS authentication

Authentication by SMS is a medium level form of authentication and in addition to your DigiD login code, you will also need a transaction code. Via SMS, DigiD sends this transaction code by SMS to your mobile phone. DigiD will soon extend the medium and high levels of security, using other means of authentication. Depending on the internet service you are using, the government agency will request a basic, medium or high level form of authentication. Since the end of November 2006, the mobile number used must be unique. It appeared that some mobile numbers were registered for up to 5 different DigiDs.

4.2.2.5 Secure transactions

DigiD makes sure that the service it provides is as reliable as possible. After login, a secure connection is safeguarded using Secure Socket Layer (SSL). In addition, DigiD has the reliability of the system tested regularly by an independent professional party. These are just two examples of the security measures employed by DigiD.

4.2.3 In a way beyond DigiD, A Personal Internet Page

Currently pilots are undertaken on a Personal Websites for Citizens.[18] Whereas DigiD provides easy access to a number of different authorities, a Personal webpage should include all information that are stored by the various governmental organizations. So to obtain information of, e.g. a municipality and the Tax authorities it would be no longer necessary to log in twice, but simple going to the Personal Internet Page would suffice to obtain the necessary information.

4.2.4 Commercial CA certificates

The so called commercial ca certificates, which can be used in a number of eGovernment applications, are based on prior physical identification, i.e. the requesting party needs to appear personally before the CA to receive his credentials.

[18] Announced by the Ministry of Internal Affairs March 2006.

The national government so far recognised four private certification authorities that comply with the required standards regarding qualified certificates defined in the Dutch eSignatures Act and which can be used for certain eGovernment applications. As trusted third parties they can deliver PKI based digital certificates for the generation of secure electronic signatures in eGovernment applications.

It should be noted that the four recognised certification authorities can also offer their certificates to foreign entities, and that no generic standards have been put in place to accept certificates issued by other entities. From an interoperability perspective, this means that any user of an application requiring commercial ca certificates is limited to these providers; no other certification service providers qualify.

The four certification authorities are:

Getronics PinkRoccade Nederland BV[19]	6 October 2003	Personal certificates and service certificates
Diginotar BV[20]	2 June 2004	Personal certificates and service certificates
CIBGhttp://www.cibg.nl/[21]	22 December 2004	Personal certificates and service certificates
ESG De electronische signatuur BV [22]	23 August 2006	Personal certificates

Detailed information about the certificates can be found at:

https://www.pkioverheid.nl/over-pkioverheid/certificaten-pkioverheid/

4.3 Enik, national electronic identity card

The government (Ministry of Internal Affairs) is planning introduce an electronic identity card (not replacing the Passport, but co-existing) with the following functionalities:

- An Electronic signature
- Means for electronic identification
- Encrypt communications

The electronic Dutch identity card (eNIK) is a card with a chip which can be requested by all Dutch residents at municipalities just like the passport. Three certificates are used for respectively electronic signature, confidentiality and identity. To be able to use the eNIK, beside the possession of the eNIK and a card reader, the facilities should support an advanced electronic signature.

[19] http://www.pinkroccadecsp.nl/website/

[20] http://www.diginotar.nl/

[21] http://www.cibg.nl/

[22] http://www.de-electronische-signatuur.nl/

The eNIK facilitates all services of the government for which a signature is required, where confidentiality plays an important role and where the identity (of a citizen) must be determined reliably.

The eNIK is not yet introduced. First, it is necessary to set up a control system and an application system. First eNIK are planned to be used earliest in 2007.

The specific applications are still under development.

The eNIK is EAL4+ certified, which is the highest level of the Common Criteria (ISO 15408).

5 eGovernment applications using electronic signatures

There are hundreds of applications by national, regional and local governments in which electronic signatures are used. As has been indicated in the document on the general purpose of this study it is of no use to describe all applications. We will therefore describe two sample applications. The overview in the Chapter on Operational and planned applications is most extensive. Although far from complete. The Questionnaires this country report finishes with will provide the characteristics of the two sample applications.

In the context of this report the interoperability is an important issue, but in order to determine that it is important to assess the general technology underlying the applications. Most public services use either one of the following three electronic signatures types:

First, the use of a normal electronic signature (that is often not really interoperable, due to the fact that people from outside the Netherlands do not possess the information required for identification/authentication such as passport number or local address).

Second the use of DigiD.

Third, the use of PKI.

We refer to the previous chapter for a discussion of these specific electronic signatures. In the remainder of this chapter we single out Public procurement and Tax.

5.1 Public procurement

In 2005 the Dutch Association for Employers (VNO/NCW) has issued a very critical report on procurement entitled *Overheidsopdrachten? Vergeet het maar!*[23]. Over 60 % of the companies considered the demands of government so out of line that they no longer considered the government as a serious client. This report did not focus, however, on e-procurement. Such a procedure is inherently more transparent and may take away existing concerns.

The Consolidated Public Sector Procurement Directive (2004/18/EC) and the Utilities Sector Procurement Directive (2004/17/EC) establishes a new framework for the utilisation of e-communication mechanisms in procurements in the public and utilities sectors. We will discuss briefly the situation of eProcurement in the Netherlands.

A special daily overview of tenders as well as assigned projects is offered via the website www.aanbestedingskalender.nl. This site also supports the sending of information directly to the European Union's Publication Office in Luxembourg, so that three working days later this is published on TED (Tenders Electronic Daily). Municipalities, as well as regional and national government agencies can post their tenders as well as assigned projects on this site. There is no electronic signature used on this site for contracting purposes, the site has a pure informing nature.

In 2006 a new site has been launched, www.tenderned.nl This site co-ordinates on a national level electronic Public Procurement and is in particular interesting for the current study because electronic signatures are used. The site Tenderned is linked to the just mentioned www.aanbestedingskalender.nl. In the description below we will restrict ourselves to Tenderned.nl

Tenderned is a spin-off of an application used for the Dutch Rail road infrastructure (ProRail), www.aanbesteden.prorail.nl. It is an initiative of amongst other The Ministry of Transport, Public Works and Water Management (http://www.verkeerenwaterstaat.nl/english/). In the summer of 2006 ProRail transferred its Public Procurement site to the Ministry of Economic Affairs (www.minez.nl). PIANOo (Dutch abbreviation for: Professioneel en Innovatief Aanbesteden, Netwerk voor Overheids-

[23] Available via http://www.vno-ncw.nl/

opdrachtgevers, see www.ovia.nl) is the organisation within the Ministry of Economic Affairs that manages the site Tendered and aims to fully integrate Tendered with the www.aanbestedingskalender.nl.

Tenderned covers all aspects of Procurement. For instance, Tenderned can be used for goods, services and works, within all sectors, and for all phases of the tendering process.

5.1.1 Application identification

The website requires only one time registration. The website not only allows to upload tenders. It is also possible to ask questions via the web site, and subscribe to a tender. The system also allows "reverse auction".

5.1.2 eSignature details

5.1.2.1 Legal aspects

The signatures should comply with the legal requirements for qualified signatures.

5.1.2.2 Technical aspects

All parties using Tenderned need to use an electronic signature with a smart card or USB token. The subscriptions are signed with a qualified electronic signature. Governmental organisations need to use PKIoverheid. Companies can use any qualified signature. So foreign tenderers can also use the service offered via TenderNed.

5.1.2.3 Organisational aspects

The site has a subscription procedure that is supported by Diginotar, one of the Dutch Qualified Certification Providers. Diginotar provides a secure website for TenderNed for the tendering process in which all acts by tenderers are safely stored, including time stamps.

5.1.3 Interoperability

Any qualified signature issued by a CSP of an EU member state (or a similar level of security from providers outside the EU) suffices for using the services offered by TenderNed.

5.1.4 Miscellaneous

On October 31 2006 the first tender was published on TenderNed.

5.1.5 Assessment

Tenderned is still under development but promises to become a vital part of Public procurement at all governmental levels (national, regional, local) as well as for all interesting parties both inside and outside Netherlands.

5.2 Tax

As already indicated, the possibility of electronic tax declarations was mentioned in the proposal of the Directive 1999/93/EC. Back in the mid 1990s electronic would also mean sending in a diskette containing the filled in tax form, or sending the form by using a Modem. In recent years declaration via the Internet has become more common.

As of January 2005 all companies are obliged to file electronic tax declarations electronically.

For over ten years electronic declaration by citizens is possible, and from 2007 only if the DigiD is used.

5.2.1 Application identification

All electronic forms for tax purposes and other information for citizens can be obtained via the site of the Tax and Customs Administration:

- for citizens via http://www.belastingdienst.nl/zakelijk/aangifte.html
- for businesses via http://www.belastingdienst.nl/particulier/aangifte.html).

Businesses can use their own administrative systems to file the tax declaration or use webforms.

5.2.2 eSignature details

For citizens electronic declaration is not obligatory, but the use of DigiD is required in case of electronic income tax declaration.

Businesses use a personal name/password to log in. They have obtained this information via their Social-Fiscal number and can also use DigiD. If they do not use the internet forms but their own administrative software they can either use digital signatures (e.g. Diginotar is specifically indicated as a CSP where to obtain a digital signature), or a name/password can be asked for.

5.2.2.1 Legal aspects

DigiD is used as a normal electronic signature.

For businesses the used signature is either a normal one, or, in case of businesses using their own administrative software qualified electronic signatures can be used.

5.2.2.2 Technical aspects

Citizens can upload a program to fill in the tax form. After filling in this form and signing the form electronically this form can be uploaded to Tax authority.

Business can either use the website or dedicated software to directly upload.

5.2.2.3 Organisational aspects

The TAX authority is a central player in the development of electronic communications between governments and citizens/businesses, and in particular as regards to the use of electronic signatures in these communications.

DigiD is only available for citizens with a permanent address in the Netherlands.

5.2.3 Miscellaneous

Before the launching of DigiD, the national government considered to use the signatures of the Tax authority in a first step of the development of a general portal for all different governments (one stop shop idea). Hence, for several years over a million citizens declared their income tax via the internet.

5.2.4 Assessment

The TAX authority is at the forefront of the developments of electronic communications using electronic signatures. Up until today there have been only a few false declarations via the internet.

Two such examples can be found in Dutch case law, in the family law domain and in criminal law. In 2001 the Higher Court of Amsterdam decided that the Tax authority wrongly transferred money after an electronic declaration. The case was the following. By using the electronic signatures of his former wife for a provisional tax refund, a man received money back from the Tax authority. His wife he just divorced from only discovered it when in the final declaration she did not get any money back.[24] In 2004 the Court of The Hague sentenced a man to 22 months imprisonment, because he used the electronic signatures of several partners in crime to file false declarations.[25]

In general, the applications provided by the tax authority are successful for almost a decade.

[24] http://www.rechtspraak.nl. Hof Amsterdam 18 december 2001, LJN: AD 8302.

[25] http://www.rechtspraak.nl. Rb. 's-Gravenhage 6 augustus 2004, LJN: AQ6560

6 General Assessment

In recent years the Dutch government, in particular since the enactment of the Act on Electronic Communication with Government in 2004, is offering more and more online services to the public. Whereas a divergent, incoherent package of services can easily originate due to the many players involved, there are several initiatives that aim to set standards or develop applications to be used in all governmental organizations. The DigiD is a good example in this respect. Far over 1 million citizens already applied for this Digital ID that can be used for a number of governmental services both on a national, regional and local level.

Since 2007 electronically based financial reporting by using XBRL (eXtensible Business Reporting Language)[26] allows to easily sent information to the General bureau of Statistics and Chamber of Commerce. At the end of January 2007 the first annual account using XRBL has been sent to the Chamber of Commerce Amsterdam.

Another related development, for now primarily focused on businesses but in the future also to be used by citizens is the Government Transaction Portal (OTP – Overheids Transactie Portaal). This is a website where the One Stop Shop principle is applied. So, in stead of contacting several governmental organisations separately, via the OTP all these organisations can be addressed at once. Electronic signatures play an important role, because in most transactions it is important for the government to know who they are dealing with.

The main players on a general level that should be monitored to keep up with new developments are in particular:

- E-overheid, via http://www.e-overheid.nl/
- Government wide Shared Service Organisation for ICT, via http://gbo.overheid.nl/english/
- Public Key Infrastructure, via http://www.pkioverheid.nl/english/
- DigiD, via http://www.digid.nl/english/

Summarizing, in our opinion the Dutch government is really doing well in the field of eGovernment in respect to the communication with citizens/companies and the use of electronic signatures. There are many initiatives, and more and more transactions with the government can take place via the internet.

[26] http://www.xbrlvoorondernemers.nl. On 6 December a special website, www.xbrlvoorondernemers.nl, was launched with
additional information about XBRL for entrepreneurs. The information campaign is a joint initiative of the Ministries of Justice, Finance, Economic Affairs, the Interior and Kingdom Relations, as well as the Chamber of Commerce Netherlands, Statistics Netherlands and the Netherlands Tax and Customs Administrations.

7 Operational and planned applications

Some interesting applications are mentioned on national, regional and local level. This is just a small selection of over hundred, maybe thousand comparable online services.

7.1 Applications at the federal level

	Application	**Scope**	**Reference**	**Contact**	**Signature**
1.	Tax	Online declaration of income taxes by citizens	http://www.belastingdiens.nl/variabel/digid/digid.html	http://www.belastingdienst.nl/	DigID
2.	CWI	Unemployment service	http://www.werk.nl/	http://www.cwinet.nl/	DigID
3.	Mijn IB-Groep	Students using DigiD are able to consult and change all sorts of information related to their scholarship. This also includes consultation of for example all the post the IB- group send the person, the post-office where the student is able to fetch his bus/traincard, the payments made bij the IB-group as well as the debt the student has.	http://www.ibgroep.nl/particulier/Mijn_IBGroep/Waarom.asp	http://www.ibgroep.nl/	DigID
4.	SVB	For the AOW, nabestaanden Anw, kinderbijslag and TOG with an exception for the 65+ regeling is it possible to consult or change your personal data. For the above list with the exeption of	http://www.svb.nl/internet/nl/digitaal_loket/index.jsp	http://www.svb.nl/	DigID

	Application	Scope	Reference	Contact	Signature
		TOG digiD can also be used for a digital request			

7.2 Applications at the regional level

	Application	Scope	Reference	Contact	Signature
	eProvincies	Facilitates and coordinates the use of ICT within provinces, including electronic signatures, in particular DigiD	http://www.e-provincies.nl/smartsite2166.htm	Saskia Kroon. saskia.kroon@ictu.nl T: 070 888 76 99	DigiD
	Digitaal Loket Noord Holland	All kind of information of subsidies, links to all digital desks of Municipalities located in North Holland, and a catalogue of all kind of products/services offered by the Province	http://www.noord-holland.nl/thema/concern/digitaal_loket/index.asp?thema=home	Provincie Noord-Holland Postbus 123 2000 MD Haarlem **Tel.** (023) 514 31 43 **Fax** (023) 514 40 40 **Internet:** www.noord-holland.nl **E-mail:** post@noord-holland.nl	None
	e-subsidie (Province Limburg)	All kind of information of subsidies, including	https://portal.prvlimburg.nl/esubsidie/	Afdeling Coördinatie Werk, Zorg & Cultuur	Digid

	Application	**Scope**	**Reference**	**Contact**	**Signature**
				Tel. 043 - 389 78 00	

7.3 Applications at the local level

	Application	**Scope**	**Reference**	**Contact**
	Tax for dogs	The owners of dogs can file that they possess a dog.	http://www.hellendoorn.nl/gemeente/hondenbelasting.php .	Ir. J.J. van Overbeeke, Lentzinckserve 6, 7441 KE Nijverdal, tel. (0548) mailto:h.van.overbeeke@hellendoorn.nl?SUBJECT=Reactie%20 nl h.van.overbeeke@hellendoorn.nl
	Digitale Balie (digital desk) from Municipality Moerdijk	All kind of Licenses, both applying for and payment. Excerpts from all kind of registers, such as Name/Adress/Date of birth, etc. Includes online payment.	http://www.moerdijk.nl/smartsite.shtml?id=54716	Henk den Moye Keene 9 Klundert 0168-404928 henk.den.duijn@moerdijk.nl

	Digitaal loket (digital desk) Amsterdam, Zeeburg	All kind of Licenses, both applying for and payment. Excerpts from all kind of registers, such as Name/Adress/Date of birth, etc. Includes online payment. For companies special part of the site with additional services	http://www.zeeburg.amsterdam.nl/digitale	Communicatieadviseur digitale Rosanne Kolmer - 020 608 r.kolmer@zeeburg.amsterdam.nl
	Digitaal loket Den Haag (The Hague)	Broad catalogue of services, including parking licenses, local taxes, etc.	http://www.denhaag.nl/smartsite.html?id=22279	**Spui 70**. Post Box 12 600, 2500 DJ Den Haag.

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

Primary Contact	
Country	The Netherlands
Name	Arno R. Lodder
Organisation	Vrije Universiteit

8.2 Alternative Contact

Country	
Name	
Organisation	

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
Wet van 8 mei 2003 houdende Aanpassing van Boek 3 en Boek 6 van het Burgerlijk Wetboek, de Telecommunicatiewet en de Wet op de economische delicten inzake elektronische handtekeningen ter uitvoering van richtlijn nr. 1999/93/EG van het Europees Parlement en de Raad van de Europese Unie van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG L 13) (Wet elektronische handtekeningen)	Act of 8 May 2003 (Act on electronic signatures), entered into force on May 21, 2003.	Stb. 2003, 1999 (see http://overheid.nl/op)
Besluit van 8 mei 2003, houdende de vaststelling van eisen voor het verlenen van diensten voor elektronische handtekeningen	Royal decree of 8 May 2003 defining the requirements for Certification Service Providers, entered into force on May 21, 2003.	*Stb.* 2003, 200 (see http://overheid.nl/op).
Regeling van de Staatssecretaris van Economische Zaken van 6 mei 2003, nr. WJZ/03/02263, houdende nadere regels met betrekking tot elektronische handtekeningen.	Ministerial regulation of 6 May 2003 on electronic signatures, entered into force on May 21, 2003.	*Stcrt.* 8 mei 2003, nr. 88, p. 9, see http://www.sdu.nl/staatscourant/
Beleidsregel van de Staatssecretaris van Economische Zaken met betrekking tot de aanwijzing van organisaties die certificatiedienstverleners toetsen op de	Guidelines of the Ministry of Economic Affairs on Certification Service Providers, entered into force on May 21, 2003	*Stcr.* 8 mei 2003, p. 10, see http://www.sdu.nl/staatscourant/

overeenstemming met de bij of krachtens de Telecommunicatiewet gestelde eisen, op grond van artikel 18.16 van de Telecommunicatiewet		
Wet van 29 april 2004, houdende aanvulling van de Algemene wet bestuursrecht met regels over verkeer langs elektronische weg tussen burgers en bestuursorganen en daarmee verband houdende aanpassing van enige andere wetgeving (Wet elektronisch bestuurlijk verkeer)	Act on Electronic communication with governments, entered into force on June 30, 2004	Stb. 2004, 214 See http://overheid.nl/op

10 Annex C: Filled-in questionnaires

Below two important initiatives are elaborated upon. For the purpose of this study it seems, however, most interesting to contact the people behind the general underlying technology used in most governmental applications. The general contacts are:

DigiD
Postbus 993
7301 BE Apeldoorn
(0800) 023 04 35

Technical details:

Marc Gerrits, 070-8887950

PKI overheid

Ir. R. Lachman
Adviseur Beheer en Relatiemanagement
GBO.OVERHEID
PKIoverheid
Wilhelmina van Pruisenweg 104
Postbus 84011
2508 AA Den Haag
Tel: +31(0) 70 8887 950
Fax:+31(0) 70 8887 882
mailto: rajesh.lachman@gbo.overheid.nl

10.1 Electronic Public Procurement: TENDERNED

10.1.1 Application identification

Application/Service Classification	
Application/Service Name	TenderNed
Application/Service Type	A2B
Concerned sector	All
Application/Service Cross-Border Type	All foreign tenderers can use the system
Level of Online Sophistication Type	Stage 3: Two-way Interaction: Processing of forms inclusive authentication
Intended “clients”	All contracting authorities (Directive 2004/18/EG), all ‘special sectors” (Directive 2004/17/EG) and all tenderers.

Abstract Description	The system supports contracting authorities (and special sectors) and tenderers all phases of contracting from publication of notices till contracting.
Identification of Application/Service Entities	
Procedural Details	Filing tenders and subscribing to tenders
Current status	Pilot phase, it is operational for a dozen contracting entities.
Expected future developments	The system will be fully operational in 2008. One module of this system will become compulsory, namely the publication of notices.

Responsible Organisation	
Organisation Name	PIANOo, [Network for Contracting Authorities] part of Ministry of Economic Affairs
Organisation Type	National level
Date of interview	31/01/2006

Application/Service System Details	
Communications Information	Web based
External interface	Any web browser
Data structures processed by the application	All material that needs to be provided in case of tenders, including the signing of the contracts and a Virtual Company Document

10.1.2 eSignature details

Legal aspects	
Does the system rely on a simple / advanced / qualified / other signature?	Qualified
Is the signature required/recommended?	Required for contracting authorities and for tenderers.
Which strategies are planned for the	The nature of the information exchanged in Tender

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?	procedures is considered confidential, therefore secured websites and qualified signatures are used.
What is the legal basis (law, decree,…) for this application?	A forthcoming National Procurement Act
How is liability/responsibility regulated? Does the national legal framework regulate more than the minimum demand of the directive 1999/93 EC?	No

Technical aspects	
What are the parties involved in the signature process?	The Government that published the tender as well as interesting parties
What kind of token or credentials are used (smart cards, software certificates, paper tokens …)?	Smart cards and USB tokens
What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of eSignature?	A reader when smart cards are used
What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?	Just standard signature software: Software drive, SafeSign, Java VM
What information is signed by the user and what is the objective of the signature?	Several documents has to be signed: - Contracting authorities: Notices, 'Eigen verklaring' (Own Certificate), Contracts - Tenderers: tender Objective of the signature is a high degree of authenticity.
Is this an application with multiple signatures for the same data and, if yes, what is the relationship between the signatures?	No
What are the relevant policies (CPS, certificate policy, signature policy)?	Standard
How are the signature/certificate	Through a secure site provided by Diginotar, one of the

presented to the application?	Dutch Qualified Certification Providers.?? Niet goed m.i.
What information is included in the certificate, and what is the role of this information in the functioning of the application?	Who is responsible for signing
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. 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.	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?	

Organisational aspects	
Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?	Diginotar, Gemnet CSP, ESG: providers of electronic signatures, certified by OPTA.
Who are the relying parties[27]? Describe the context?	

[27] « 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.	OPTA
What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be suspended or revoked?	

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?	Yes, if a foreign tenderer has a qualified electronic signature, the system will be made accessible for this tenderer.
What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?	

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)?	100-200
Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application;	Yes, installing software at the client pc limits a quick roll-out
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)?	

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.	Strengths: legally equal with written signature Weaknesses: the implementation within an existing network and the duration of acquiring a qualified signature.

10.2 Tax-on-Web

10.2.1 Application identification

Application/Service Classification	
Application/Service Name	Elektronische aangifte
Application/Service Type	A2B and A2C
Concerned sector	Tax
Application/Service Cross-Border Type	Several forms can be downloaded for foreign tax payers (in English and German) and an Electronic Signature Registration Form for Non-Resident Taxpayers exist. You can use this form to notify the Tax and Customs Administration of your electronic signature (the form is in Dutch, but speaks more or less for itself).
Level of Online Sophistication Type	Stage 4: Transaction: Case handling; decision and delivery (payment)
Intended "clients"	Natural and legal persons both income tax for citizens and business
Abstract Description	Tax authority offers form for various tax declarations, such as income tax, dividend tax, VAT return
Identification of Application/Service Entities	Tax authorities and citizens/businesses
Procedural Details	Citizens: Either the uploading of a filled in form or the filling in of a web-based form For companies either webbased forms or uploading information from their own administrative systems
Current status	Operational
Expected future developments	There has been some confusion about what information can be provided to consultants that fill in forms for their clients, in particular information of privacy sensitive nature. New procedures are developed to prevent misuse of personal information.

Responsible Organisation	
Organisation Name	Tax authority

Organisation Type	National
Date of interview	xx/xx/2006

Application/Service System Details	
Communications Information	*Web based*
External interface	*Web interface, or in some cases information is directly uploaded from the internal system of businesses*
Data structures processed by the application	*XML and XBRL*

10.2.2 eSignature details

Legal aspects	
Does the system rely on a simple / advanced / qualified / other signature?	DigiD is simple, the name password combination companies use to log in is also simple. For companies using their own admistrative software (or their consultants) it is possible to make use of qualified signatures
Is the signature required/recommended?	For citizens DigiD is required. For business a qualified signature is optional
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?	Different types
What is the legal basis (law, decree,…) for this application?	National Tax law, as well as the general Civil Law and Administratieve law sections on electronic signatures
How is liability/responsibility regulated? Does the national legal framework regulate more than the minimum demand of the directive 1999/93 EC?	No

Technical aspects	
What are the parties involved in the signature process?	The form are signed by citizens or by companies. Both can make use of consultants. The government does not sign

	yet.
What kind of token or credentials are used (smart cards, software certificates, paper tokens …)?	Depends on the signature. See also general description of DigiD above. In case qualified signatures are used, any type is allowed (so smart cards, software certificates)
What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of eSignature?	Standard software
What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?	Standard software
What information is signed by the user and what is the objective of the signature?	Form of the Tax authority. The signature is meant to identify the signer and to use the signed form as means of proof in case of later disputes.
Is this an application with multiple signatures for the same data and, if yes, what is the relationship between the signatures?	No
What are the relevant policies (CPS, certificate policy, signature policy)?	
How are the signature/certificate presented to the application?	Via secures websites, as well as secure administrative software
What information is included in the certificate, and what is the role of this information in the functioning of the application?	Note that the certificate is only used voluntary. DigiD contains general identifying information as the name, address, SO-FI number, etc.
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. 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.	Yes, DigiD

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)?	Via the DigiD-site
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?	

Organisational aspects	
Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?	The tax authority and PKIoverheid (provides authentication means such as DigiD)
Who are the relying parties[28]? Describe the context?	
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?	

[28] « 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?	Yes, there are special forms for non-nationals and they can apply for an electronic signatures, see http://www.belastingdienst.nl/english/
What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?	

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)?	Far over a million each year
Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application;	The role of consultants filling in forms online is not regulated satisfactory yet
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

10.2.5 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.	Good roll-out, with years of experience