IDABC
European
eGovernment Services

eID Interoperability for PEGS

NATIONAL PROFILE THE NETHERLANDS

November 2007

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

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

Company's name: Siemens - time.lex

Company's address (optional):

Company's logo (optional)

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

Disclaimer

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

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

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

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

This paper can be downloaded from the IDABC website:

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

Executive summary

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

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

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

Table of Contents

1 Documents

1.1 Applicable Documents

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

1.2 Reference Documents

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

2 Glossary

2.1 Definitions

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

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

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

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

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

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

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

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

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

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

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

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

  (a) it is uniquely linked to the signatory;

  (b) it is capable of identifying the signatory;

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

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

  Again, this definition may cover non-PKI solutions.

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

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

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

2.2 Acronyms

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

3 Introduction

3.1 General status and most significant eIDM systems

Public administration in the Netherlands traditionally depends principally on the social security number – SSN or "sofi-number") and the public register number (i.e. the administration number used in population register - A-number). However, a programme intended to introduce one single identification number for e-ID purposes is currently being deployed (the Citizen Service Number (BSN - "*Burgerservicenumber*"). The legislation for introducing this Citizen Service Number has passed the House of Representatives (*Tweede Kamer*) in September 2006. Currently (May 2007) this legislation almost passed the Senate (*Eerste Kamer*). A special Act for using this Citizen Service Number in health care has passed the House of Representatives in October 2006. A committee of the Senate has decided after consultation of the Dutch Data Protection Authority to start evaluating this special Act on Citizen Service Numbers only after the general Act has passed the Senate.

Since August 2006 all passports issued contain on a chip some personal information about the holder of the passport. Additionally, the introduction of an electronic identity card by 2007 is being considered.

Obviously, the Citizen Service Number is meant to facilitate the communication between governments and citizens, but may be used by companies under certain conditions. Already in place at the moment is the so-called 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) and after enactment of the Citizen Service Number Act with this number, can apply for a DigiD.

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

The Netherlands was amongst the first European countries to start with eGovernment initiatives.[3] 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.[4] 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.

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 up to the expectations. One reason has been that the central government is not really in a position to force initiatives in local governments concerning the use of Information Technology.[5] 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.[6] Parties involved were amongst others the Ministry of Internal Affairs and the Association of Dutch Municipalities (VNG).

At this moment, at all government levels actual implementation of initiatives on electronic communication between governments and citizens/companies is taking place.

For this Country report particularly relevant is the introduction of the forthcoming and already mentioned Citizen Service Number. In the 1980s the government introduced the Social Security Number (*SOFI-nummer*), and then people feared that this number could be (mis)used for all kind of purposes. Violation of privacy rights was seen as a very serious risk. Therefore, the legislation has

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

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

[5] 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.

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

been very cautious regarding who was allowed to use the SOFI-number and for what purposes. The Citizen Service Number now introduced in fact replaces the SOFI-number. The main difference is that the Citizen Service Number will be more broadly used, including use in the private sector. In the context of these developments it has been a wise decision to draft a separate Act for using this number in Health Care (also because medical personal data belong to a special category of data with special protection (cf. Article 8 of the EU 95/46 Directive on Data protection).

The Dutch Trade Register is compulsory for almost every company, and deals with a number of frequent and important questions.

- Does the company with which I wish to do business actually exist?
- Is the person I am dealing with actually an authorized signatory?
- What has happened to the company I used to do business with a few years ago?

The trade register provides a lot of this kind of information. This section of the website tells you exactly what information is contained in the trade register in the Netherlands.[7]

All the above is related to eGovernment and the use of electronic data, but for this report it is important to indicate the registers that were used to store personal information, and are still in use. Besides the obvious birth, marriage, migration, etc. registers, the main source is the Municipality Basic Administration (*Gemeentelijke Basisadministratie*) that registers everyone living in the Netherlands on a permanent basis (which basically comes down to a stay of 4 months or more). This is the most important registration, which used a so-called A-number as a unique identifier. It is expected that over time the A-number will be replaced by the Citizen Service Number, but at its introduction only the SOFI-number is deleted and replaced by the Citizen Service Number.

The Municipality Basic Administration is hosted by each Municipality, but connected by a national secured network in order to prevent citizens being registered in two registers or none at all. The Municipality Basis Administration is used by a number of organizations (both Public and Private sector) that are either mentioned in the Municipality Basic Administration Act or are given special permission. As it names suggest the Municipality Basis Administration contains information on Name, Date of Birth, Gender, Place of living, Nationality, etc. The Municipality Basic Administration is the national authentic source for personal data.

[7] See http://www.kvk.nl/sectie/sectie.asp?sectieID=102

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

DigiD[8]

DigiD is a government initiative that aims to improve and simplify government internet services. DigiD is implemented by 'GBO.Overheid' (*Gemeenschappelijke Beheerorganisatie*) and the Dutch Tax Authorities.

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.

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.

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 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

[8] Information at www.digid.nl

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.

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. The first eNIK are planned to be used at the earliest in 2007.

3.3.2 Legal framework

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

- Act on the Citizen Service Number - *Wet algemene bepalingen burgerservicenummer* (Kamerstukken 30.312), as of April 2007 approved by the House of Representatives, at a final stage of the discussion in the Senate.
- Act on the use of the Citizen Service Number in Health Care - *Wet gebruik burgerservicenummer in de zorg* (30.380), as of April 2007 approved by the House of Representatives, at an initial stage of the discussion in the Senate.
- Act of 9 June 1994 on the Municipality Basic Administration (*Wet van 9 juni 1994, houdende regels ter zake van de gemeentelijke basisadministratie van persoonsgegevens, laatstelijk gewijzigd* Stb. 2007, 76)

Other relevant legislation includes:

- Act of 8 May 2003 (Act on electronic signatures), entered into force on May 21, 2003.[9]

[9] 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).*

- Royal decree of 8 May 2003 defining the requirements for Certification Service Providers, entered into force on May 21, 2003.[10]
- Ministerial regulation of 6 May 2003 on electronic signatures, entered into force on May 21, 2003.[11]
- Guidelines of the Ministry of Economic Affairs on Certification Service Providers, entered into force on May 21, 2003[12]

3.3.3 Technical aspects

DigiD

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.

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.

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

[10] *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,

[11] *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.

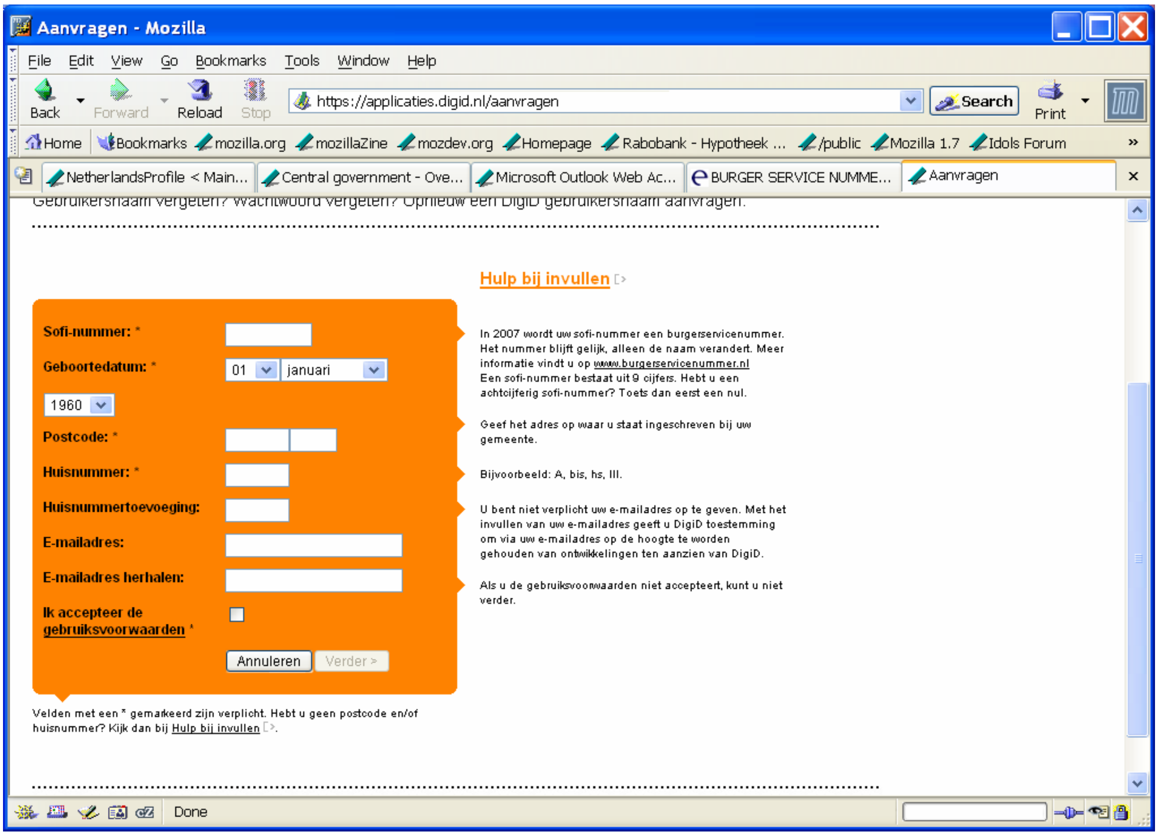
[12]*Stcr.* 8 mei 2003, p. 10, see http://www.sdu.nl/staatscourant/ Beleidsregel van de Staatssecretaris van Economische Zaken met betrekking tot de aanwijzing van organisaties die certificatiedienstverleners toetsen op de overeenstemming met de bij of krachtens de Telecommunicatiewet gestelde eisen,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

the system tested regularly by an independent professional party. These are just two examples of the security measures employed by DigiD.

The specific applications of Enik, the national electronic identity card, are still under development. The eNIK is EAL4+ certified, which is the highest level of the Common Criteria (ISO 15408).

3.3.4 Organisational aspects

The DigiD is issued online via http://www.digid.nl/. The entering of the basic information suffices, after which the name/password is sent to your home address.


Aanvragen - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
https://applicaties.digid.nl/aanvragen
Search
Print
Home Bookmarks mozilla.org mozillaZine mozdev.org Homepage Rabobank - Hypotheek ... /public Mozilla 1.7 Idols Forum
NetherlandsProfile < Main... Central government - Ove... Microsoft Outlook Web Ac... BURGER SERVICE NUMME... Aanvragen
Gebruikersnaam vergeten? Wachtwoord vergeten? Opnieuw een DigiD gebruikersnaam aanvragen.
Hulp bij invullen
Annuleren
Verder >
Done

Sofi-nummer: *	
Geboortedatum: *	01 januari 1960
Postcode: *	
Huisnummer: *	
Huisnummertoevoeging:	
E-mailadres:	
E-mailadres herhalen:	
Ik accepteer de gebruiksvoorwaarden *	□

In 2007 wordt uw sofi-nummer een burgerservicenummer. Het nummer blijft gelijk, alleen de naam verandert. Meer informatie vindt u op www.burgerservicenummer.nl Een sofi-nummer bestaat uit 9 cijfers. Hebt u een achtcijferig sofi-nummer? Toets dan eerst een nul.

Geef het adres op waar u staat ingeschreven bij uw gemeente.

Bijvoorbeeld: A, bis, hs, III.

U bent niet verplicht uw e-mailadres op te geven. Met het invullen van uw e-mailadres geeft u DigiD toestemming om via uw e-mailadres op de hoogte te worden gehouden van ontwikkelingen ten aanzien van DigiD.

Als u de gebruiksvoorwaarden niet accepteert, kunt u niet verder.

Velden met een * gemarkeerd zijn verplicht. Hebt u geen postcode en/of huisnummer? Kijk dan bij Hulp bij invullen.

DigiD is not only used in the communication Government-Citizens but also for example companies can use the DigiD for services at the Chamber of Commerce.

3.4 Interoperability

To my knowledge as of yet there are no measures on interoperability yet, but as far as higher level authentication procedures are required (or allowed), any electronic signature complying with the requirements of qualified electronic signatures can be used, so including users from abroad.

3.5 eIDM Applications

Some interesting applications are mentioned below, on the national, regional and local level. This is just a small selection of over hundred, maybe thousand comparable online services. Before that and in more detail the initiative of the Tax Authority is discussed, for this has been one of the main driving forces behind eIDM.

The Tax authority is a central player in the development of electronic communications between governments and citizens/businesses. 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 their tax declarations electronically. For over ten years electronic declaration by citizens is possible, and from 2007 only if the DigiD is used.

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.

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.

Applications at the federal level

	Application	Scope	Reference
1.	Tax	Online declaration of income taxes by citizens	http://www.belastingdienst.nl/variabel/digid/digid.html
2.	CWI	Unemployment service	http://www.werk.nl/
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	http://www.ibgroep.nl/particulier/Mijn_IBGroep/Waarom.asp

	Application	Scope	Reference
		student is able to fetch his bus/traincard, the payments made bij the IB-group as well as the debt the student has.	
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 TOG digiD can also be used for a digital request	http://www.svb.nl/internet/nl/digitaal_loket/index.jsp

Applications at the regional level

	Application	Scope	Reference
	eProvincies	Facilitates and coordinates the use of ICT within provinces, including electronic signatures, in particular DigiD	http://www.e-provincies.nl/smartsite2166.htm
	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
	e-subsidie (Province Limburg)	All kind of information on subsidies	https://portal.prvlimburg.nl/esubsidie/

Applications at the local level

	Application	Scope	Reference
	Dog ownership taxes	The owners of dogs can register their ownership	http://www.hellendoorn.nl/gemeente/hondenbelasting.php.
	Digitale Balie (digital desk)	All kind of Licenses, both applying for and	http://www.moerdijk.nl/smartsite.shtml?id=5471

	from Municipality Moerdijk	payment. Excerpts from all kind of registers, such as Name/Adress/Date of birth, etc. Includes online payment.	6
	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
	Digitaal loket Den Haag (The Hague)	Broad catalogue of services, including parking licenses, local taxes, etc.	http://www.denhaag.nl/smartsite.html?id=22279

3.6 Future trends/expectations

Fears of breaches of privacy are in the current times not so often heard, but given today's power of technology the introduction of the Citizen Service Number combined with the possible use of it by private players, caution seems necessary. The current legal framework can partly guarantee this, but the developments should be closely monitored in order to establish the direct and indirect effects of the above measures. The influence of the Citizen Service Number in terms of eIDM in general, and of its use as unique identifier by all kind of applications cannot be underestimated. It is e.g. hoped that access to internet services will not be linked to either DigiD or the Citizen Service Number. In Korea the obligation to subscribe to Massive Multiplayer Online Role-playing games with the Social Security Number led to the theft of over 200.000 identities. The judge penalized the companies for lack of security, but identity theft clearly constitutes a serious risk these days.

A Dutch example has been the breaking into Medical Files[13] (Spaink 2005), when over 1 million personal medical files appeared to be easily accessible by unauthorized parties. This is one reason why the introduction of the Electronic Medical file did not take place by January 2006 as was originally intended, and why it still has not been introduced. So, although the initiatives open up many opportunities for the communication with the government as well as for more effectively managing data bases with personal information, adequate security measures should be put in place.

Another 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

[13] K. Spaink, Medische geheimen, Nijgh en van Ditmar, see also www.tnty.nl

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/

3.7 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 the prime example of eIDM that pushed the developments. With the forthcoming introduction of the Citizen Service Number, electronic Identity management will operate both with a legal framework and based on a well accessible authentic source. Over 1 million citizens have already applied for the Digital ID that can be used for a number of governmental services both on a national, regional and local level.

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 eIDM. There are many initiatives, and more and more transactions with the government can take place via the internet. However, the need for adequate security measures should not be overlooked.