eID Interoperability for PEGS

NATIONAL PROFILE SWEDEN

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 Swedish 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

Sweden does not have a national eIDM system administered by public administration. Rather the issuing of eIDs is done by private entities, mainly banks. The introduction of electronic ID-cards was procured in 2004 leading to framework agreements with the following four providers for eIDs in Sweden:[3]

- BankID (9 different banks)
- Nordea Bank AB
- Steria AB
- TeliaSonera Sverige AB

The agreements are in force until June 2007 (Steria AB) or end of 2007 (for the remaining three providers) and can be prolonged for an additional 6 or 12 (Steria AB) months.

Sweden has had a tradition regarding ID-cards being distributed by private entities. The Post Office and several banks have issued personal identification cards for a long time.[4] Only since 2005 have the police issued national ID-cards to Swedish citizens which can be used for travelling within the Schengen area, which is not the case for the other ID-cards as they do not state the nationality of the card holder. This is mainly due to the fact that e.g. the Post Office does not require Swedish citizenship, but solely a Swedish personal identity number.

Some of the ID-cards issued by banks can be used as carriers for an eID.[5] The eID can, however, also be stored on another smart card or as software on a computer. The ID-card issued by the police follows the standards by ICAO (International Civil Aviation Organization) and contains a chip that can be used in the future to store electronic information, i.e. e-services, as for example the eID. This is, however, left up to the providers within the framework agreement for Swedish eID services.[6] There are no known applications at the moment.

The above mentioned eIDM systems are indirectly linked to the population register (Sw: Folkbokföringssystemet), as one requires a personal identification number in order to obtain an eID. This allows a unique identification of the individual eID holder. The population register is administered by the Swedish National Tax Board (Sw: Skatteverket).

---

[3] See (in Swedish) http://www.e-legitimation.se/

[4] In order to be able to receive an ID-card issued by the Post Office (http://www.svenskkassaservice.se/other_languages/id_cards.html) or any bank, one has to be registered in Sweden and have a personal identification number. Swedish citizenship is, however, not required.

[5] See e.g. (in Swedish) http://www.swedbank.se/sst/inf/out/infOutWww1/0,,113186,00.html and

[6] See (in Swedish) http://www.polisen.se/inter/nodeid=33378&pageversion=1.jsp and http://www.regeringen.se/content/1/c6/05/10/28/6df9fd20.pdf

There are no widely used eIDM systems for legal persons at the moment as an eID is only open to physical persons. Some discussion to this extent have, however, been initiated. Information on legal persons is stored in the Swedish Trade and Industry Register held at the Companies Registration Office (Sw: Bolagsverket).

These systems will be discussed in more detail below.

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

eIDM system	Potential user base	Actual penetration	Actual use
BankID	Estimated at 3,8 million which is the customer rate of the 9 banks co-operating in BankID.	Estimated at 800 000[7]	No public statistics are available for the particular types of eID or particular services.
Nordea	Estimated at 2 million customers in Sweden	Estimated at 330 000	According to the Swedish National Tax Board, however, 2,6 million persons handed in their tax declaration electronically in 2006, electronically meaning via telephone, SMS or Internet (either with a pin code or via an eID).[8]
Steria AB	N/A	N/A	
TeliaSonera Sverige AB	Theoretically the whole Swedish population	Estimated at 250 000	

[7] See (in Swedish) http://www.bankid.com/BankidCom/Templates/NormalPage.aspx?id=44&epslanguage=SV

[8] See (in Swedish) http://www.e-legitimation.se/Elegitimation/Templates/NormalPage.aspx?id=93

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

The Swedish public administration features three levels of government: national, regional (18 counties with county-councils (*landsting*), and 2 regions (*region*) and local (290 municipalities; *kommuner*). Municipalities are responsible for a large number of services, such as housing, roads, schools, child care and water. County councils oversee e.g. health care, but also questions such as building permits and traffic.[9] Obviously, eGovernment services ("e-services") follow this general structure. Legislation is mainly passed on a national level although the counties and municipalities have certain areas of competence.

eGovernment applications are often developed by the individual state, county or municipal authority, and are in that respect "vertical", i.e. within one competence area, such as tax or social security. There are, however, also more general e-government projects that run horizontally across or apply to several or all authorities. For example, a majority of the e-services use the Swedish eIDs (*e-legitimation*) for authentication of the user and (in some cases) for signing by the user. The Swedish eIDs thus work across authority borders and horizontal levels.

For the past few years several investigations and projects have been undertaken regarding public e-services. Most progress has been noticeable within government applications, while counties and municipalities to a certain extent have lacked the financial resources to implement eGovernment applications. The Swedish Administrative Development Agency, Verva, (*Verket för Förvaltningsutveckling*),[10] has been mainly responsible for coordinating the eID framework, while the different eGovernment applications were developed under the auspices of the various authorities. This is also the case for the regional or local level, as the Swedish Association of Local Authorities and Regions, SALAR (*Sveriges Kommuner och Landsting*, SKL)[11] has mainly focused on electronic public procurement and less on eID applications as such.

3.2.2 National eGovernment cooperation and coordination

The Swedish Administrative Development Agency, Verva is responsible for coordinating the development of central government administration in Sweden and is one of the Government's central advisory agencies. Verva administers *inter alia* the procurement of framework agreements concerning products and services for the entire public sector in the fields of information and communication technologies. Several national eGovernment initiatives are also lead and coordinated by Verva. While regional and local eGovernment initiatives are carried out by the respective regional and local county-

9 See http://www.sweden.se/templates/cs/FactSheet____11493.aspx

10 http://www.verva.se

11 See http://www.skl.se/artikel.asp?C=756&A=180

councils and municipalities, Verva also plays an important role in this regard. For example, Verva offers financing to authorities at state, county and municipality level for the verification of eIDs. Thus authorities that are about to launch e-services can apply to Verva for a one-year "start package" that provides free access to the verification of eIDs.[12]

PTS (the Post- and Telecom Agency, *Post- och Telestyrelsen*)[13] is the Swedish authority responsible for supervising the issuers of qualified certificates to the public. Currently, however, there are no qualified certificates in use in Sweden, and no issuers of such certificates have been registered with PTS. In its role as a supervisory authority PTS is also running an e-signature advisory and discussion group, with representatives from all interested parties.

The National Tax Board (*Skatteverket*)[14] has been one of the first government authorities to develop public e-services based on the eID framework and several services have been available, such as e.g. the possibility to hand in the annual tax declaration electronically. The national Tax Board is also responsible for the population register in Sweden (see more in detail below).

In 2000 the Swedish Government commissioned the National Tax Board to co-ordinate the management of certificates for e-identification and e-signatures within the government administration. The assignment was to be carried out in collaboration with a number of state authorities; the Social Insurance Agency (*Försäkringskassan*), the Patent and Registries Office (*Patent- och Registreringverket*) and The Swedish Agency for Public Management (*Statskontoret*)[15]. This collaboration has become well-known under the name of SAMSET.

The SAMSET project focused on legal matters when introducing electronic authentication and signatures into the administrative processes of public organisations. In this process due focus was furthermore put on questions regarding user dialogue, user interface and users possibilities to understand, manage and trust electronic methods in communication with public authorities. A number of reports (all in Swedish) have been produced in the SAMSET project covering the field from legal investigations to computer icons that can help everyday users to understand the PKI functionalities. The reports can be found on the web site of the National Tax board.[16]

Carelink[17] is a company with stake-holders from *inter alia* county-councils and municipalities, and has worked with PKI within the SITHS-project (Safe IT within the Healthcare Sector). The project focused on personal eIDs for employees linked to their employment status.

---

12 See (in Swedish) http://www.verva.se/web/t/Page 2711.aspx

13 http://www.pts.se

14 http://www.skatteverket.se

15 Statskontoret (The Swedish Agency for Public Management) (http://www.statskontoret.se) was the predecessor of Verva, parts of which was moved into Verva when this agency was formed in January 2006. At the time when Statskontoret was in charge of public procurement and framework agreements for government agencies in the field of information and communication technologies, a framework agreement was signed to enable government authorities and most municipalities and county councils to order services that provide the necessary security for identifications and signature.

16 See http://www.skatteverket.se/etjanster/samset/

17 http://www.carelink.se

The 24/7 Delegation, (*24-timmarsdelegationen*) was assigned by the Swedish government in 2003 to promote the development of e-services within the public sector. The Delegation's progress report, "E-services for All" (SOU 2004:56), recommended the eID as a common security solution for e-services in the public sector. The Delegation also proposed a number of actions to stimulate the development of e-services.[18] The functions of both the 24/7 Delegation as well as the e-Committee (*e-nämnden*)[19] were transferred into Verva at the beginning of 2006.

A private initiative worth mentioning is the WPKI Non-Profit Association. It is a non-profit organisation that tries to establish a well-functioning infrastructure for mobile e-IDs by developing technical and administrative specifications describing how the mobile terminal SIM cards should be designed to host the mobile e-ID and identifying the interfaces between the stake holders' mobile operator, e-ID issuer (RA/CA) and relying party.[20]

3.2.3 Traditional identity resources

The Swedish population register contains data on who lives in the country and where they live. The information stored includes *inter alia* name, place of birth, citizenship, civil status, spouse, children, parents, guardian(s) and adoption, address, property, parish and municipality in which you are registered, immigration to and emigration from Sweden, address abroad, death and place of burial. The register is held by the National Tax Board and is updated regularly by other public agencies, which means a person only has to notify the National Tax Board on changes of address, immigration and emigration, names of newborn children and certain name changes.[21] The place of registration has an impact on several citizen rights, such as the right to vote, where to pay taxes and the right for certain social benefits, such as housing allowance. Each person in the register is given a unique number, a personal identity number, consisting of the date of birth of a person, a birth number, and a check digit.[22]

The population registration in Sweden has originally been administered by the church. The oldest preserved church registers date from the early 17th century. Since 1 July 1991 the National Tax Board is in charge of the population register. The local tax offices deal with the administration of the data in the registers, while the National Tax Board is the chief authority and provides for legal and administrative support.

---

18 For a list with reports (in Swedish) see http://www.verva.se/web/t/PublicationList____3037.aspx, the report "E-identification for secure e-services" is available in English http://www.verva.se/web/t/Publication____1358.aspx

19 Some reports on eID can be found (in Swedish) at http://www.verva.se/web/t/PublicationList____3036.aspx

20 See http://www.wpki.net/index_eng.html

21 See http://www.skatteverket.se/download/18.b7f2d0103e5e9ecb08000127/717b03.pdf

22 See http://www.skatteverket.se/blanketterbroschyrer/broschyr/info/717b.4.39f16f103821c58f680008017.html

The information in the population register is shared with other public agencies via the Navet system or the Swedish population and address register (SPAR);[23] both of which are regulated by specific statutes, mentioned below.[24]

The population register contains information on name, personal identity number and co-ordination number, place of birth (in Sweden or abroad), citizenship, civil status, spouse, children, parents, guardian(s) and adoption, address, property, parish and municipality in which you are registered, immigration to and emigration from Sweden, address abroad, as well as death and place of burial.

Information on legal entities is, depending on the type of the company, kept in several different registers, administered by the Companies Registration Office, *Bolagsverket*). Limited companies are, e.g., registered in the Limited Companies Register (*Aktiebolagsregistret*), trading partnerships, limited partnerships and sole traders in the Business Register (*Handelsregistret*).[25] The different registers can all be accessed via the Swedish Trade and Industry Register at the Companies Registration Office.[26]

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

The eID framework

The first framework agreement on eID in Sweden dates from 2001. In 2004 a new call for tenders was issued leading to framework agreements with the previously mentioned four providers for eIDs in Sweden. The current agreements are valid until June 2007 (Steria AB) or end of 2007 (remaining four providers).

According to the framework agreements the offered services may include the following applications[27]:

- personal eID (*Personlig e-legitimation*)
- personal eID for certain groups (*Personlig e-legitimation för riktad grupp*), e.g. employees or groups of customers.

---

[23] See http://www.skatteverket.se/download/18.b7f2d0103e5e9ecb08000127/717b03.pdf

[24] Of particular relevance are the Act on the national register of personal addresses (SFS 1998:527) (Sw: Lag (1998:527) om det statliga personadressregistret SPAR) and the Act on the processing of personal data for the purpose of keeping the national register of persons (SFS 2001:182), (Sw: Lag (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet)

[25] See http://www.bolagsverket.se/in_english/register_and_change/index.html

[26] See https://snr3.bolagsverket.se/snrgate/default.jsp

[27] See (in Swedish) http://www.avropa.nu/upload/Bilagor/Aktuella/RAO-Elektronisk%20identifiering-2004/eID%202004%20-%20Vägledning%20till%20ramavtalen%201.0.pdf

- web server authentication (*Webbserverlegitimation*), including both server certificates and function certificates.
- eIDs for electronic authority stamps (*E-legitimation för myndighetens elektroniska stämpel*) in order to verify authenticity of documents.
- eIDs for certain functions (*Tjänstelegitimation*), e.g. within a company employees can be identified.

The only application offered by all providers is the personal eID. The agreement includes both software and hardware solutions concerning the way the private key is stored. The private key is especially important for secure identification and signature.

As there are at least four different providers of eIDs in Sweden, public authorities as well as private entities interested in engaging the advantages of the eID framework have to be able to employ validity checks for all four eID types. In order to do that the framework agreements offer commercial software that can be utilised. Public administrations can also use the Infra Service (*Infratjänst*)[28] that was procured earlier.

As the services are not centrally handled by a governmental authority, it is difficult to estimate the number of eIDs issued.[29] Regarding prices several differences can be noticed as well. Most of the banks issue eIDs for free to their customers, some of the providers (e.g. TeliaSonera) charge ca. 50 EUR for a smart card eID solution.[30] There are also different age limits for acquiring an eID. For obtaining an eID from Nordea, e.g., one has to be at least 16 years old, TeliaSonera requires customers to be 18 years old.

The different solutions all offer two certificates, one for authentication and one for signing.[31]

Entities that are able to procure within the framework agreements include all state authorities, 20 counties and regions, 229 municipalities, social security authorities, as well as 26 public organisations.[32]

Personal security codes

Besides using an eID, individuals can also submit their tax return via the Internet, an SMS message or a telephone call using their personal security code. The SMS and telephone alternatives only allow people to approve the information in their pre-printed self-assessment form sent to them earlier by the tax authority. In case somebody wants to make deductions for travel to and from work or other changes to the tax return, she/he has to use an eID or the personal security code and access the form

---

28 See http://www.avropa.nu/templates/ramavtalsomrade____75.aspx

29 Some estimated numbers were, however, presented earlier in the report.

30 See http://www.telia.se/privat/katalog/VisaProdukt.do?channelId=-76442&tabId=0&OID=1537014385&type=PRODUCT

31 See more below under technical

32 See http://www.avropa.nu/templates/ramavtalsomrade____224.aspx

online. An eID further allows changes in or adding of information and filling in and submitting supplement forms such as for sole traders or for earnings from residential property rental.

3.3.2 Legal framework

Swedish legislation does not stipulate any basic requirements for eIDs. The Act on Qualified Electronic Signatures (*Lag (2000:832) om kvalificerade elektroniska signaturer*)[33] deals with electronic signatures in general and does not refer to eIDs specifically. The different regulations by authorities concerning the provided e-services (see below) refer in many cases to the use of an eID, but without defining the eID requirements.

The reason for the lack of definition of the eID in Swedish laws and regulations is that the Swedish eIDs are commercial products that have been selected in a public procurement process. The requirements presented in this public procurement process represent the policy essence of the services and certificates used. The requirements were derived from, in principle, the CA-policy presented in ETSI TS 101 456.[34]

The personal identity number is a unique identification number for Swedish citizens, appearing on the eID and its microchip. The legal framework for the issuing of the personal identity number is laid down in the Population Registration Act (SFS 1991:481) (Sw: Folkbokföringslag (1991:481)). Section 18 of the Population Registration Act stipulates that each person registered in the Swedish population registration system receives a personal identity number.

Furthermore the use of the personal identity number is regulated in several different national laws, such as the Personal Data Act (SFS 1998:204) (*Personuppgiftslag* (1998:204))[35] and in special data protection legislation, such as the Act on the national register of personal addresses (SFS 1998:527) (*Lag (1998:527) om det statliga personadressregistret SPAR*) and the Act on the processing of personal data for the purpose of keeping the national register of persons (SFS 2001:182), (*Lag (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet*).[36]

In addition, legislation for the different e-government applications has been amended in order to include the possibility for identification or signing through eIDs. In most cases legislation does not

---

33 See http://www.pts.se/Archive/Documents/SE/Qualified%20Electronic%20Signatures%20Act%20_SFS%202000_832_English%20translation.pdf

34 Information received from Mr Göran Ribbegård, goran.ribbegard@verva.se, 31 October 2006.

35 See http://www.datainspektionen.se/in_english/personal_data.shtml

36 Some more examples can be found in Sören Öman, *Implementing Data Protection in Law*, in Peter Wahlgren (ed), Scandinavian Studies in Law, Volume 47 – IT Law, Stockholm Institute for Scandinavian Law, Stockholm, 2004, at 389-403.

distinguish between authentication and signing. Many applications, however, mainly require authentication and no signing process as such yet.

Chapter 4 Section 4 of the Act on Tax Return and Income Statements (SFS 2001:1227) (*Lag (2001:1227) om självdeklarationer och kontrolluppgifter*), for example, allows for the personal income tax declaration to be in electronic form. The wording "electronic document" implies that the content and signer of the document can be verified via a certain technical process. In this case the requirement for a signature as laid down in Chapter 4 Section 3 can be considered fulfilled. The government or the delegated authority may regulate further when the tax return can be handed in as an electronic document.

This additional regulation can be found in Regulation SKVFS 2006:1 by the Swedish National Tax Board (*Skatteverkets föreskrifter om e-tjänsten Inkomstdeklaration*). Section 12 of this regulation stipulates that the income tax declaration can be handed in electronically by means of an eID or by use of a personal security code. Depending on the technical solution an individual can amend or only approve the self-assessment form it has previously received from the National Tax Board (see Sections 13-18 Regulation SKVFS 2006:1).

The Act on self-services via the Internet within the administration of social security (SFS 2004:115) (*Lag (2004:115) om självbetjäningstjänster via Internet inom socialförsäkringens administration*) deals with the possibility for individuals to use self-services in order to supply information, hand in applications or notifications, dispose over rights and perform other legal actions within the frame that is stipulated in regulations by the government or the delegated authority. According to its Section 3 an individual submitting information shall use an electronic signatures as stipulated in Section 2 of the Swedish Qualified Electronic Signatures Act.

The Regulation RFFS 2004:4 by the Swedish Social Insurance Agency on self-services via the Internet within the administration of social security (*Riksförsäkringsverkets föreskrifter (RFFS 2004:4) om självbetjäningstjänster via Internet inom socialförsäkringens administration*)[37] allows electronic means and the use of self-services in questions concerning parent's allowance and pension due to age. The use of certificates and electronic signatures is necessary for withdrawal from parent's allowance, assurance for parent's allowance and temporary parent's allowance and application for pension due to age, according to Section 2 in Regulation RFFS 2004:4.

The new Swedish Companies Act (SFS 2005:551) (*Aktiebolagslag (2005:551)*) that entered into force on 1 January 2006 explicitly mentions in Section 13 the signing of documents using an electronic signature. According to this Section any document that has to be signed may, if not otherwise stipulated, be signed with an advanced electronic signature as defined in the Swedish Act on Qualified Electronic Signatures.

The Companies Ordinance (SFS 2005:559) (*Aktiebolagsförordning (2005:559)*) furthermore stipulates that an application for registration according to the Swedish Companies Act or Chapter 12 Section 8 of the Co-operative Societies' Act (SFS 1987:667) (*Lag om ekonomiska föreningar (1987:667)*) or a report based on the Companies Act, can be submitted electronically in accordance with the regulations issued by the Swedish Companies Registration Office. A report or application shall be

[37] In Swedish available at http://lagrummet.forsakringskassan.se/risextern/

signed by a member of the Board of Directors or one of the executive officers. If this is done electronically the document has to be signed with an electronic signature in accordance with the regulations issued by the Swedish Companies Registration Office.

3.3.3 Technical aspects

The different eID solutions have several things in common: they all are based on PKI technology and they all incorporate two certificates: one for authentication and one for signing.

Existing solutions include the storing of eIDs on smart cards or as files on the hard disk; some issuers offer both options. The conformity of the smart card based eIDs with the requirements of Annex III of the European Directive 1999/93/EC has not been officially assessed, and it is therefore not certain that they can be considered as "Secure Signature Creation Devices" in the sense of the Directive. This has, however, not been brought up as a major issue in Sweden, since no eID issuers claim (or feel the need to claim) that their certificates are "qualified" certificates or can be used to create "qualified" electronic signatures.

The brand of supported cards, middleware, signature mechanisms etc differ to some extent among the issuers. Below we will present the main technical features of the different eIDs.

Nordea[38]

Nordea eIDs can be issued either on smart cards or as files (in PKCS#12 format) to be stored on the hard disk. The eID cards used are Setec TAG AB (PKCS#15 profile), with the operating system SetC0S version 4.4.1. Nordea's bank cards (XponCard with operating system Proton Prisma EMV) can also be used as the carrier of the eID. All PC/SC readers can be used to access the cards, but Nordea only supports Todos Argos Mini II.

For key and certificate access Nordea provides the middleware Nexus Personal to Nordea customer. Nexus Personal supports both CSP and PKCS#11. The supported hash algorithms are SHA-1 and MD5 and the signing algorithm is RSA. The RSA key-length is 1024 bits for e-IDs and 2048 bits for the CA key.

For the validation of electronic signatures created by means of the eID the Online Certificate Status Protocol (OCSP) is used. However, there is also a possibility to use the Certificate Revocation Lists (CRLs).

Nordea does not have a CA hierarchy but works with a flat solution with self-signed CAs, which includes separate CAs for eIDs issued on cards and on files.

---

38 Information provided by Roger Landin, roger.landin@nordea.com, +46 8 534 91297, and Rolf Larsson, rolf.a.larsson@nordea.com, +46 8 614 8156

The certificates follow the X509v3 standard. The user receives two certificates: one certificate for authentication and one for signing. These certificates constitute a pair; they have the same name (subject DN) and are issued and revoked together (and are from a user perspective "one eID"). The personal identity number is used as the subject serial number.

Nordea's Certificate Policy and Certification Practice Statement are available online.[39] More details on the certificates and the CA can be found on Nordea's website.[40]

Steria[41]

Steria's eIDs can be issued either on smart cards or as files (in PKCS#12 format) to be stored on the hard disk. The cards used are operating system Setec SetCOS (various versions) and Cryptoflex from Axalto. All PC/SC readers can be used to access the cards. For key and certificate access Steria provides both CSP and PKCS#11 drivers. The reader needs to follow the PC/SC card reader standard and the ISO7816 physical and electrical standards for a smart card reader.

As for the e-signature mechanisms, the hash algorithm used is SHA-1, the signing algorithm is RSA, and the key-length is 1024 bits.

Steria provides different PKI client middleware based on customer needs.

For the validation of electronic signatures created with Steria eIDs Certificate Revocation Lists (CRLs) are used. The Online Certificate Status Protocol (OCSP) is planned to be supported in the future.

Steria's CA hierarchy has a self-signed root CA, under which four CAs follow (for certificates on files and cards respectively, for organizational certificates, and finally one CA for testing purposes).

The certificates contain the following information: public key, serial number for the certificate, validity period for certificate, all first names, last name, personal identity number, name of CA (Certificate Authority).

The certificates follow the X509v3 standard and the Swedish standard SS 614331 for SIS-approved ID-cards with crypto chip. The user receives two certificates: one for authentication and one for signing. These certificates constitute a pair; they have the same name (subject DN) and are issued and revoked together (and are from a user perspective "one eID"). The personal identity number is used as the subject serial number.

---

39 See (in Swedish) http://www.nordea.se/sitemod/upload/root/se_org/e-legitimation/resurs/medcert.pdf

40 http://www.nordea.se

41 Information provided by Staffan Bergholm, staffan.bergholm@steria.se, +46 709 21 42 87.

Steria's Certificate Policy and Certification Practice Statement can be found online.[42] More details on the certificates and the CA can be found on Steria's website.[43]

BankID[44]

BankID eIDs can be issued either on smart cards or as files (in PKCS#12 format) to be stored on the hard disk. The cards are delivered by Setec, with operating system SetCOS v4.4.1 32K with a PKCS#15 profile. The chip used is Infineon SLE 66CX320P chip (32K). Any standard card reader can be used to access the cards, e.g. Todos card readers. The reader needs to follow the PC/SC card reader standard and the ISO7816 physical and electrical standards for a smart card reader.

As for the e-signature mechanisms, the hash algorithm used is SHA-1, the signing algorithm is RSA, and the eID key-length is 1024 bits. All CA certificates have 2048 bit keys.

For key, certificate and cryptographic access BankID provides both CSP and PKCS#11 drivers.

As to middleware, on the client side BankID provides an authentication and signing plug-in that all users must use. There are also some applications that are allowed to code directly towards the CSP/CAPI-interfaces to provide third party solutions.

On the server side BankID has certain requirements on the validation software. BankID certifies software that can be used to verify BankID's eID signatures and relying parties are bound to use certified software for validation.

For revocation checks, the Online Certificate Status Protocol (OCSP) is used.

The BankID organizational structure does not depend on or include any Certificate Policy and Certification Practice Statement. Instead, BankID signs contracts with all parties. These contracts are not public. As to the CA hierarchy it starts with the BankID Root CA. Below there are intermediary CAs for the different banks that are part of the BankID consortium. Each bank then has between two and five different CAs, (some of) which issue certificates to the users (bank customers).

The certificates follow the X509v3 standard and the Swedish standard SS 614331 for SIS-approved ID-cards with crypto chip.

The user receives two certificates: one authentication and one for signing. These certificates are very similar; they have the same name (subject DN) and are issued and revoked together (and constitute from a user perspective "one eID"). The personal identity number is used as the subject serial number.

---

42 See http://eid.steria.se/index.php?page=information&sessionID=30de23b7b1385ca9f464fca2503fd70d

43 http://www.steria.se

44 Information provided by Robert Carlsson, robert.carlsson@bankid.com, +46 70 322 1592.

More details on the certificates and the CAs can be found on BankID's website.[45]

TeliaSonera[46]

TeliaSonera's eIDs can be issued either on smart cards or as files (in PKCS#12 format) to be stored on the hard disk. The cards used are from Setec TAG AB (PKCS#15 profile), with Infineon SLE 66CX320P chip (32K) and Infineon SLE 66CX160S (16K); the latter soon to be phased out. The operating system is SetCOS version 4.4.1, Revision A2 and SetCOS version 4.3.1, Revision B3 respectively.

TeliaSonera provides the following readers for the smart card: GemPC USB-SL, GemPC Seriel-SL and GemPC Card, however, all PC/SC compatible readers can be used to access the cards.

For key and certificate access TeliaSonera provides CSP support through the program NetiD from NetMaker.

As for the e-signature mechanisms, the hash algorithm used is SHA-1, the signing algorithm is RSA (MD5 is used in one older CA), and the key-length is 1024 bits for user-keys and 2048 bits for CA-keys (1024 bits for one older CA).

For the validation of electronic signatures the Online Certificate Status Protocol (OCSP) is used for all TeliaSonera eIDs, except for electronic signatures created with certificates issued by one older CA, where Certificate Revocation Lists (CRLs) are still used.

Regarding policies and practices documentation, Telia uses a Certification Practice Statement, but reference in policy issues the ETSI-documents TS 102 042 v1.1.1 and TS 101 456.

CAs used for issuing TeliaSonera's eIDs are currently not part of a common CA hierarchy. A Root CA has, however, been created, under which TeliaSonera potentially will gather these CAs. Today only the CA that is used for issuing eIDs on files to be stored on the hard disk is signed by the Root CA.

The certificates follow the X509v3 standard and are based on the Swedish standard SS 614331 for SIS-approved ID-cards with crypto chip.

More details on the certificates and the CA can be found on TeliaSonera's website.[47]

Commercial CA certificates

---

45 http://www.bankid.com

46 Information provided by Peter Döös, peter.doos@teliasonera.com, +46 8 504 62 174.

47 http://www.teliasonera.com

There are no accreditations, registrations, certifications or other requirements for CAs that want to issue non-qualified certificates to the Swedish public. Furthermore, there is nothing that prevents an individual public authority or municipality to accept other certificates than the eIDs (that have been subject to a public procurement process). Today there are however few CAs on the Swedish market that issue certificates that are used for communication with the public sector.

Certificates from **Scandtrust AB** are used in certain public procurement processes. Scandtrust is a private Swedish CA, whose certificates are marketed by ChamberSign, and for which ChamberSign acts as a Registration Authority. Scandtrust maintains a CPS, but the policies referenced in the Scandtrust CSP are "AddTrust policies". The CA hierarchy ends with the AddTrust Public CA Root, under which there are several CAs. For further information see the CA's website.[48]

3.3.4 Organisational aspects

Any physical person with a Swedish personal identity number can obtain an eID. Legal persons can also use an eID, though it must be linked to a user with a Swedish personal identity number. The legal person as such cannot have an eID.

eIDs exist both as smart cards and as files stored on the hard disk. Some issuers provide one or the other, whereas some give the option to choose the form of the eID.

eIDs are issued in two ways; by ordering and downloading it from the user's Internet bank while being logged on (and thus identified by the bank), or by ordering the eID on the Internet. In the latter case the user will receive an activation code by registered mail which has to be collected in person, providing a due physical ID (passport etc). If the eID is issued on a smart card, the user, after having ordered it via the Internet bank, will need to collect the eID at a bank or post office, showing a physical ID.

The type of data stored on the eID (both on file and on smart card) varies between the different providers. In most cases, however, certain personal data, such as last and first name, as well as the personal identity number will be stored. The legal implications when using personal identity numbers were mentioned earlier, in other words the relevant laws have to be adhered to by the providers in this context.

Since the eIDs are issued by different suppliers the authorities providing the e-service, and thus relying on the eIDs, must be able to perform verification checks towards many different parties. Different eID-suppliers may require different client software. The client software may in turn have its own way to authenticate users and trigger e-signature creation. This means that an authority that provides e-services must be able to trigger authentication of users and verification of e-signatures, as well as apply for revocation checks, in different ways towards different eID-suppliers. This problem can be handled by using certified software (*köparprogramvara*) or by using a service (*Infratjänsten*) that is specifically available under another framework agreement (The Infra Service agreement 2003).

48 http://www.scandtrust.se

In the Swedish model, the relying parties (the authorities, municipalities, etc.) pay for the verification service, whereas the cost of producing the eIDs is paid by the market players.

The Verification software (*köparprogramvara*)

To simplify the adjustment between the e-service and the eID-supplier's IT environment (including the user's client software) the framework agreement includes the possibility for the relying party (the authority) to buy specific verification software (*köparprogramvara*). Through this software the e-service can handle authentication, e-signatures and revocation checks, irrespective of which eID supplier's environment is concerned. The idea is thus that the verification software is general, so that the authority only needs to acquire one software module to perform verification for all available eID solutions. Some of the suppliers of certified software are Teleca[49] with the software Teleca Security Server, Nexus[50] with the software Nexus MultiID server, and TietoEnator[51] with the software TECS – TietoEnator Certificate Services.

The Infra Service (*Sw: Infratjänsten*)

As an alternative to the verification software the verification functionality can be accessed via the Infra Service (*Infratjänsten*). This service is accessible under a framework agreement from 2003, and is provided by the suppliers TietoEnator[52] and WM-data[53]. By using the Infra Service the operation of the verification software is a service for the authority.

The aim of the Infra Service is *inter alia* that a customer of this service only needs to contact the service supplier in order to verify eID from all eID suppliers under the framework agreement.

3.4 Interoperability

As mentioned earlier any physical person with a Swedish personal identity number can obtain an eID. Therefore, persons either living in Sweden (including non-nationals) or Swedish nationals can obtain any type of eID. In addition, some solutions require the user to have a bank account from one of the providers of an eID.

Legal persons can also use an eID, though it must be linked to a user with a Swedish personal identity number, the legal person as such cannot have an eID.

Regarding taxes, individuals not in possession of an eID, can use a personal security code via the Internet, phone or SMS; however this option has certain restrictions regarding the possibility to make changes to the tax declaration.

49 http://www.teleca.se

50 http://www.nexussafe.com

51 http://www.tietoenator.com

52 http://www.tietoenator.com

53 http://www.wmdata.com

There are no well-known initiatives dealing with interoperability on an international level, although PTS might be involved in some projects in this respect. On a national level one can claim that interoperability exists as long as e-services allow any type of eID within the framework agreements. Some e-government applications, especially on a local and regional level might limit the possibility to use a specific public e-service to certain types of eIDs, such as the BankID. In these cases interoperability might not be guaranteed as individuals are limited to a certain type of eIDs.

3.5 eIDM Applications

This section will provide a short overview of key applications for the eIDM systems.

3.5.1 eID card applications

Applications for the eID include both the public and the private sector, while the public sector may be responsible for the majority of services at the moment.

Within the public sector the following applications can be mentioned:

- Declaration of personal income tax via the website of the Swedish National Tax Board[54]
- Electronic Tax Return (submission of the PAYE and VAT return electronically via the Swedish National Tax Board website, by using an eID and provided a notification has been made to the National Tax Board beforehand)[55]
- the Swedish Social Insurance Agency (*Försäkringskassan*)56 offers several services including a parental service (*Föräldratjänsten*), application for pension (*Ansökan om ålderspension*) and employers' service (*Arbetsgivartjänsten*)
- Registration of new companies (Companies Registration Office, *Bolagsverket*)57
- Healthcare Guide (*Vårdguiden*) by Stockholm County Council58

In some of these cases, the eID is used both for identification and for signing of documents. In most cases the eID mainly serves identification purposes. A complete list, also including regional and local e-services can be found online.[59]

Private sector applications include:[60]

---

54 http://www.skatteverket.se, see also http://www.skatteverket.se/blanketterbroschyrer/broschyr/info/326b.4.3d21d85f10922490e1080002628.html

55 See http://www.skatteverket.se/international/international/electronictaxreturn

56 http://www.forsakringskassan.se

57 https://www.foretagsregistrering.se

58 http://www.vardguiden.se

59 See (in Swedish) http://www.e-legitimation.se/Elegitimation/Templates/ServiceHitlist.aspx?id=12&search=allservices

- ü Different applications regarding loans and other bank services, e.g. applying for a credit card, login to internet banking.
- ü Change of address.[61]

3.6 Future trends/expectations

The framework agreements will phase out at the end of 2007 with the possibility of prolongation for 6 or 12 months. There have not been any public discussions so far as whether and how to continue the framework.

As eIDs are more and more known[62], including the present solution with involving the banks and private providers in the process of issuing eIDs, no considerable changes are expected when it comes to the providers. One could imagine, however, new players appearing.

To what extent the traditional ID-cards issued by the police will serve as a platform is unknown at this stage.

3.7 Assessment

The Swedish approach offers a number of advantages and disadvantages, which can be summarised as follows.

3.7.1 Advantages:

- The utilisation of the existing bank infrastructure has facilitated access to eIDs as individuals are already familiar with internet banking procedures and therefore may easily take to next step to employ the functions of eIDs as well. In other words the threshold for starting to use eIDs has been rather low.
- In addition, no difficult authentication procedures regarding the issuing of the eID need to take place, as the bank has already identified its customer. This means that in most cases, even

[60] For a more complete list, see (in Swedish) http://www.e-legitimation.se/Elegitimation/Templates/ServiceHitlist.aspx?id=12&search=allservices

[61] http://www.adressandring.se

[62] According to a study by the National Tax Board in May 2006, almost 78 % have heard of the eID (Sw: e-legitimation), compared to 17 % in February 2004. See http://www.e-legitimation.se/Elegitimation/Templates/NormalPage.aspx?id=100

when it comes to smart card solutions, individuals can pick up the eID as well as the card reader from the post office or one of the branch offices of the bank.

- As the main costs for eID solutions are carried by providers of e-services, individuals have low to zero start-up costs regarding eIDs. This facilitates as well the usage of electronic identifications.

- Governmental initiatives, such as the campaign by the National Tax Board regarding the electronic submission of the annual tax declaration, have increased the awareness of citizens and therefore also contributed to an increase in usage, which in turn leads to more eGovernment applications.

- Despite that fact that there are different types of eIDs administered by several private instead of one public entity, a common framework serves as the basis for the different technical solutions. This allows individuals to use the same eID in various state, regional or local government applications as well as private e-services.

3.7.2 Disadvantages:

- As the Swedish eID framework is not based on governmental administration, the actual penetration might be lower than in other countries. On the other hand, traditionally, Swedish physical ID-cards have not been issued by state authorities, but rather private entities, such as banks and post offices.

- The variety of eID solutions might lead to a certain lack of interoperability if local or regional governments decide not to employ all four types of eID, but, due to cost constraints, limit the eGovernment application to one type, such as the BankID. This would lead to the fact that individuals require several different eIDs in order to use all e-services available.

- As the costs are carried by the providers of e-services, especially public authorities might face a shortage of resources and therefore not be able to initiate new online services. Verva is therefore, as previously mentioned, currently running a project to help financing the authorities' verification of eID signatures.