IDIS (2010) 3:155–174
DOI 10.1007/s12394-010-0056-9

The Danish eID case: twenty years of delay

Jens Villiam Hoff · Frederik Villiam Hoff

Received: 22 October 2009 / Accepted: 24 March 2010 / Published online: 27 April 2010

Abstract The focus of this article is to explain why there is still no qualified digital signature in Denmark as defined by the EU eSignatures Directive nor any other nationwide eID even though Denmark had an early start in eGovernment, and a high level of "e-readiness" compared to other nations. Laying out the technological, organizational and legal dimensions of eID in Denmark, and comparing these with a number of other European countries made it possible to explain this paradox. Thus, the three main reasons for the special route development has taken in Denmark seems to be concerns over privacy, lack of intergovernmental coordination and lack of cooperation between public and private sector. However, with the recent tender on digital signatures won by the PBS and the roll-out of the NemID it seems that Denmark will finally—after twenty years of delay—have an eID which can be widely used in the public as well as the private sector.

Keywords Electronic identification · eID · Digital signature · e-Government · OCES · Digital Taskforce · NemID

Introduction

Denmark had an early start concerning eGovernment solutions compared to most other nations, and there has consistently been a rather high political attention on eGovernment since the first coherent eGovernment strategy "Effective IT in State Administration" which had been launched by the Ministry of Finance in 1992. Also, the Danish development has been marked by a relatively high degree of political

The research reported here is based on the analysis of documents and personal experience of the authors. It has been conducted under contract with the Institute for Information Management Bremen (ifrib), Germany, funded by Volkswagen Foundation, Germany.

J. V. Hoff (✉) · F. V. Hoff
Department of Political Science, University of Copenhagen, Øster Farimagsgade 5,
1353 Copenhagen K, Denmark
e-mail: jh@ifs.ku.dk

consensus around ICT-policies. Furthermore, diffusion of computers, Internet penetration and level of ICT competences are high among the Danish population consistently placing Denmark on the top in international comparisons on "e-readiness"[1]. It is therefore a paradox that as of today (January 2010) no citizen card for unique identification of citizens exists, and no qualified electronic signature is being offered by certification service providers (CAs) in Denmark. This article will, by laying out the history of eID's in Denmark, and by looking at the technological as well as organizational and legal choices made, try to explain this paradox.

The history of personal identification and public registries in Denmark

There is no national ID card in Denmark, neither mandatory nor optional. Regular identity documents are passports and drivers licences. Danish citizens above the age of 18 have passports with a validity of 10 years. Children must have their own passports regardless of age,

Since 1985 the Danish passport has had the same format as passports issued in other EU-countries, apart from the Danish code of arms on the cover. On March 1st 1997, the passports became machine readable. EU regulations stipulated in December 2004 that biometric passports be made mandatory in all EU-countries, and after August 1st 2006, all passports issued in Denmark contains biometric data according to the standards of the International Civil Aviation Organization (ICAO). From January 1st 2007, the new larger municipalities have taken over the issuing of biometric passports, and delegated the individual responsibility to the citizen service centers ("Borgerservice") that handle individual passport applications[2].

Besides the passport the drivers licence is the second identity token. The identity-relevant information of the drivers license follow the older EU standard (not the one agreed upon in 2006[3]) and include: Photo, names, date and place of birth, issue date and expiration date of the card (period of validity usually being 50 years), issuing authority, personal identity (CPR) number and a card identity-code.

The identity data in the passport and the driver's license originate from the Central Population Register, which was established in 1924 and kept locally by the municipalities. Since 1968 there is an IT-based central personal register (CPR) for the registration of information on every citizen in Denmark. At the same time each citizen became identifiable by a unique personal number[4] that would track the citizens' personal information through the CPR. The preparations with planning and establishing the CPR-system was undertaken by the personal registration secretariat ("Sekretariatet for Personregistrering"), which was established February 1st 1965,

[1] See for example World Economic Forum 2009, The Economists's Intelligence Unit 2009 (http://graphics.eiu.com/pdf/E-readiness%20rankings.pdf) or the report from the EU Commission (http://ec.europe.eu/information_society/eeurope)

[2] http://www.politi.dk/da/borgerservice/pas/pasudstedelse/. Accessed on 20/8-09.

[3] http://www.transportnyhederne.dk/?Id=23104. Accessed on 25/8-09.

[4] The personal number contains 10 digits. The first 6 digits are the birth date, month and year of the person. This is followed by three random digits and a final control digit, which is even for women and uneven for men.

and thereby became the earliest version of the national CPR-office which today oversees the task of managing personal registrations and the CPR-system itself.[5]

The CPR registry is publically accessible with a digital signature, and here (www.cpr.dk/cpr/) the citizen is able to review the complete list of personal information stored by the governmental authorities. The data is personal and not accessible by any private entities. Data contained by the CPR includes: Names, CPR number, fathers/mothers CPR number, current/previous addresses, citizenship, date of birth, membership of national church, place of birth, public and private subscribers to changes in CPR registrations (this includes the police, e.g. universities (for college students), the citizens' bank and insurance company, etc.) as well as private subscribers who are only able to see address changes (e.g. postal services).

In general, the CPR-number can be said to be a central component in most public and private systems of identification of persons in Denmark. Thus, all public IT-systems, which handle information on citizens will inevitable draw on information from this register. The same is true for all digital signatures used for access to public databases. Concerning the protection of the citizen the Law on Personal Data ("Persondataloven") encompasses the regulations that govern private, public as well as associations' treatment of personal information online. Apart from dividing information into different sensitivity-ranges, the law grants a number of basic rights to the citizen which includes right to insight as to what information is processed as well as the right to know that information might be collected about the citizen.

Plans for introducing an eID in Denmark

Plans for establishing an eID in Denmark had been presented already in the eGovernment strategy of 1992. The development since then can be divided into four phases each with a specific constellation of actors (see Table 1):

(1) 1992–1995. In the first eGovernment strategy, laid down in the "Effective IT in State Administration" report in 1992, the idea of a multi-purpose ID card was presented by the Ministry of Finance in an alliance with the Ministry of Interior and Local Government Denmark (KL). The so-called "citizens card", based on smart card technology, should serve as an electronic key to the CPR-register, a means to visual identification, as a tool for the authorities to access specific personal information in citizen-government interactions, and would eventually substitute social security cards, student- and library cards as well as drivers licences and other means of exchanging personal information. However, they were countered by the Board of Technology and a majority in Parliament, who raised concerns over privacy issues. This led to an "indefinite postponing" of a citizen card and a reduction of the ambition to a system with digital signatures only.

(2) 1995–2001. In 1995 eGovernment matters were allocated to the newly established Ministry of Science, Technology and Innovation. The Ministry launched the Dybkjær-Christensen report, which among other things presented the idea of a "Public Service Net" (Hoff and Rosenkrands 2000), essentially a

[5] http://www.cpr.dk/cpr/site.aspx?p=16. Accessed on 1/8-09

Table 1 Phases in the development of eIDMS in Denmark till 2002

Phases in the development of the citizen card and the inception of the eID									
PHASE 0 "discovery" phase	PHASE 1 digitalization phase	PHASE 2 eCard-phase		PHASE 3 eSignature phase					
"Smart card" technology considered modernizing citizen-government interaction tool	The Ministry of Finance presents "Effektiv edb i Staten" the first government strategy on ICT	The Ministry of Science Technology and Development presents the Info 2000 plan and specifies the properties of a "client card"	the Danish parliaments first annual debate on information technology-> a conditional acceptance of a client card based on optional use	Compromise between Parliament and government institutions = a digital signature to be developed	The Committee on the Legal Effects of Digital signatures is formed (Nov. 3rd)	EU directive on digital signatures (1999/93/EF) is created (Dec. 13th). This establishes a common EU frame for electronic signatures	Danish law on electronic signatures (law nr. 417 of May 31st)	The Digital Taskforce (est. Aug.) formulates the ID3 strategy (digitalization of the public sector between 2007 and 2010)	The Board of IT- and Telecommunications establishes the OCES standard in December - focus is turned from client card to digital signature with the public tender at the end of 2002
				Proposal from Ministry of Science Technology and Development on optionality of a client card					
1991	1992	1994	1995	1996	1998	1999	2000	2001	2002

"paperless" form of administration ,where a chipcard, now called the "client card" would be a means of identification in self-service systems. The card would also support future solutions of digital signatures, needed for legally binding transactions.

Public concerns that being forced to have such card would lead to an increase of monitoring and governmental control, were picked up in a debate in the Danish Parliament, which showed that a majority would only agree to such a card if it was made optional. In 1996 the Ministry of Science, Technology and Innovation submitted a proposal for such an optional card for online authentication for self-service systems. But it was not possible to settle on a technical standard. Instead the introduction of digital signatures as a separate solution was defined as a strategic goal in the process towards workable public self-service systems[6]. The Dybkjær-Christensen report released a lot of "utopian energy" (Johansson 2004:155), and managed to give ICT-policies a much more central position in the political arena than it had had before. However, it did not have many practical implications, as did several follow-up reports.

(3) 2001–2002 : New impetus came from the opening speech to Parliament of former Prime Minister Poul Nyrup Rasmussen on October 3rd 2000, in which he stressed the need for a "digitalization of public administration". The policy field of eGovernment was removed from the Ministry of Science, Technology and Innovation and again placed under the Ministry of Finance, and was now to be managed by a cross-sectorial unit; the so-called *Digital Taskforce*, including representatives from Local Government Denmark and the Danish regions, The Project was lead by a steering committee established under the National eGovernment initiative[7].

The guiding idea behind the eGovernment initiative is that the responsibility for the implementation of eGovernment lies at the decentral level, but that in several cases, there can be a need for common guidelines and solutions to general problems of legal, technical and organizational nature in order to support the transition process. One of the areas deemed to be of central importance to eGovernment at all governmental levels is the question of eID, and therefore one of the projects became the establishment of a national digital signature solution, the so-called OCES ("Offentlige certificater til elektronisk service" meaning "public certificates for electronic services". The practical implementation of OCES was given to the Ministry of Science, Technology and Innovation; more specifically the Board of IT and Telecommunications and its Center for Digital Signature. It was decided that the OCES digital signature was to be implemented through an independent Certification Authority, and in order to realise this solution a first public tender was announced in

[6] Hoff & Rosenkrands (op.cit.:106) have identified two strategies behind the citizens and the client card: *An efficiency-oriented strategy* pursued by the Ministry of Interior and Local Government Denmark, which supported a *multi-purpose ID card,* and a *citizen oriented strategy*, supported by the Danish Board of Technology (an advisory board to parliament) and ICT experts centered on the client card, but especially on a third type of card, which would function as a personal security key for communication purposes.

[7] For further information about the eGovernment initiative; see www.e-gov.dk

late 2002. The tender was won by TDC, the largest Danish telecom provider and operator.

(4) 2002–present: Merging of eGovernment and electronic banking signatures: Even though banks had been providing digital access and netbanking to their customers since around 2000 in parallel to the solutions being developed in the public sector, the second public tender marked a new and more important role for the private sector in developing eID and an important step towards a common national solution. The second public tender in 2009 was won by PBS, an institution owned by the banks. Through its organization for eSignatures, danID, PBS will roll out a new, more secure eID solution under a contract, which lasts until 2017. However, this has again caused concern over privacy issues, and in order to counter criticism the Board of IT and Telecommunications at an early stage tried to integrate civil society concerns by allowing the IT-Political Association and the Danish Consumer Council, both representing public interests, a role in the choice of software and standards.

As a result of this "cooptation strategy" public criticism of this new eID solution has dried out, even though the IT-Political Association left the working group established to create the new standards due to dissatisfaction with the results obtained.

Sector specific eID systems at present

As the citizen card did not materialize, and no common standard for the citizens to electronically identify themselves vis-à-vis public administration was developed, the period from 1995 to 2005 saw the development of a number of different sector specific eID solutions in particular in the health sector, in the tax system and in other public services, besides electronic banking in the private sector.

Regional health cards

One of the predecessors for current eID solutions is the National Health Insurance Card, which is issued to all Danish nationals at age 16. The National Health Insurance Card ("Sygesikringskortet" or "Sygesikringsbevis") is a plastic card with a chip and guarantees the holder the right to free services in healthcare[8]. Originally it was only an ID card for visual authentication, and after the structural reform January 1st 2007 the card changed its name to simply the Health Card ("Sundhedskort") but retained its original properties[9].

The Health Card does not have a photo on it, but it has card holders name, address, and CPR number. It also has a chip on it used for identification whenever a citizen sees a general practioner. The data the card connects to are not PIN protected,

[8] http://www.im.dk/publikationer/fremtid/verdist.htm. Accessed on 25/8-09

[9] There is also a blue version of the Health card issued, which guarantees medical assistance and treatment within the EU and a number of European countries (Iceland, Liechtenstein, Norway and Switzerland), http://www.scandihealth.dk/Losninger/Losninger_infoark_pdf/Sygesikring/Vejledninger/Sygesikring_EU-sygesikringskort.pdf. Accessed on 25/8-09 and http://ec.europa.eu/social/main.jsp?catId=652&langId=da. Accessed on 24/8-09

but the chip in principle enables PIN protected online authentication. The card covers three domestic costs in public healthcare[10]: Basic medical assistance, prescription medicine and prescription of medical equipment and aids. Apart from this, it is used by general practioners to retrieve personal medical history through the CPR (and in this way links to the national healthcare portal: www.sundhed.dk; see below). It can be used as a library loaner card in all public libraries (accompanied by a designated PIN-code) in Denmark, as well as a means of visual identification in post offices and pharmacies (even though it contains no photo).

Since its inception in June 2004–December 2005, Danish citizens have also been able to have a blue version of the Health card (see footnote 13).It contains the same data as the yellow card, but has an expiration data, and can contain a digital signature. In order to get a blue Health card citizens do not have to show up in person at the local “Borgerservice” office, but can order it online with a digital signature, which has to be installed on the terminal used. Alternatively, a userID/password issued from the regional health care system can be used.

As the health care sector in Denmark is managed by the regions each regional IT-department, determines what is required to apply for a card and what services are accessible. This practice is therefore not yet aligned with the national government’s newer digitalization strategies.

Tax system

In the public sector two major digital signature solutions are currently used: “Fælles Pinkode” and “Tast-selv”. These solutions are usable by both citizens (“borger”) and private companies (“erhverv”). “TastSelv” is only used by the tax authorities (SKAT), which deliver an interchangeable One-Time Password (OTP) on the individual tax return. SKAT has itself expressed interest in uniting the two solutions, as each one requires maintenance and supervision because of alternating security-level requirements. The older solution (“Fælles Pinkode”) is purely software based, and requires that a piece of software be installed on the users’ computer, which supports digital signing. This solution has facilities for security-copying that provides the user with an opportunity to export the signature to another PC. The digital keys and certificates are tied to the individual citizens PC, and thereby mimic the current solution used by e-banking services where a key-file and an applet/software-based solution runs through the e-bank domain where the user is able to log in. This is supported by a personal password that de-encrypts the key on the PC.

Online banking

In online banking the so-called “netID” has been the preferred eID solution since netbanking took off around year 2000. The issuer of the netID are the individual banks or other proprietary institutions (e.g. insurance companies). The certification authority of netID is PBS, an institution owned by the National Bank and a number of independent banks. The content of the certificate is the name of the holder’s bank,

[10] For more specific information on coverage, see the Ministry of Interior and Health (2007) “Nyhedsbrev: om international social sikring”, nr. 1.

his/hers name, address, CPR number and e-mail address. The way the holder of the certificate or the nemID is authentificated by the bank is that a letter containing a PIN-code is send to the applicant simultaneously as an installation-link, which is sent electronically. When the two are paired the applicant has access to his/hers accounts and can do Internet banking. The way the nemID is related to the CPR registry is that issuing a nemID to a customer requires that the bank check his/hers personal information with the CPR registry.

The present eID in eGovernment: OCES

As mentioned above, from 2002 till now the only cross-sectional eID in eGovernment has been the software based solution called OCES. OCES is basically an electronic signature used also for online authentication.

Technical and organizational characteristics

The passing of the European Directive on a Community framework for electronic signatures necessitated a Danish law and some executive orders in order to transpose the Directive into Danish legislation[11]. In the law and executive orders the definitions of advanced and qualified electronic signature are very close to the definition of the European Directive[12]. However, so far no qualified electronic signatures are offered by certification service providers in Denmark. One of the main obstacles, detected already in 1999 through some pilot projects, has been the requirement for signature holders to meet and identify themselves in person in order to receive a qualified signature. Realising that few people would do this the Government established the so-called OCES standard. In charge of this was the Center for Digital Signature under the Ministry of Science, Technology and Innovation[13].

The OCES signature is a "light version" of the qualified electronic signature with the important difference that the holder of an OCES signature does not have to perform face-to-face identification. The OCES certification requirements were ready in 2003, and the OCES signature is widely supported by public authorities in their

[11] These were Act no. 417 of 1 October 2000 on Electronic Signatures, Executive Order no. 922 of 16 October 2000 on "Reporting of Information to the National Telecom Agency by CA's and System Auditors" and Executive Order no. 923 of 16 October 2000 on "Security Requirements etc. for Certification Authorities".

[12] According to the European Directive on digital signatures a qualified electronic signature is an advanced electronic signature based on a qualified certificate, and created by a secure-signature-creation device, (see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML). An advanced electronic signature is defined as 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 so that subsequent change in the data is detectable (see "Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications. National Profile Denmark". European eGovernment Services (IDABC). European Commission. Directorate General Enterprise. November 2006.

[13] IT-og Telestyrelsen (Board of IT and Telecommunications) under the Ministry of Science, Technology and Innovation: "Digital Signatur OCES – en fælles offentlig certifikat-standard". December 2002.

eGoverment applications[14]. OCES signatures can be issued as personal certificates, company certificates and employee certificates. Accordingly three certificate policies (CPs) exists.

A citizen obtains an OCES certified digital signature from a Certification Authority's (CA) website (most eGovernment application will have links to such website(s)[15]) by entering CPR-number, postal code and e-mail address. The CA then checks the CPR-number in the CPR-register and extracts the person's registered postal address, at the same time confirming that the postal code matches the entered postal code. A confirmation e-mail containing an activation link is sent to the specified e-mail address. At the same time a PIN-letter containing an activation code, necessary for the activation and installation of the digital signature is sent to the registered postal address. Installation of the digital signature is possible by combining the activation link in the confirmation e-mail with the received activation code from the PIN-letter (as with the netID solution used for Internet banking). Activation of the digital signature must happen within four weeks of the application, otherwise the signature is revoked. It follows from this that the OCES signatures are basically signatures installed on peoples computers. However, they can also be obtained on hardware such as eTokens or smart cards.

A citizen will log into a site needing a digital signature by entering his/her personal code, which has been chosen when he/she activated the signature. The same will be the case when he/she signs a document.

The legal framework of the OCES concept consists of an agreement between the CA and the National Board of IT- and Telecommunications, and the three OCES CP's are part of this agreement. The line-up for such agreements is regulated by the Danish eSignature Act. The Board supervises the CAs that are responsible for issuing digital signatures via defined certificate policies[16] (e.g. OCES) concerning privacy, registration procedures and other infrastructural demands such as contingency plans etc. The CAs have to formulate a Certificate Practice Statement (CPS) and to submit an annual report to the Board. They are also subjects of an external audit.

The first call for tender concerning the establishment of a CA was launched towards the end of 2002 and won by TDC, the former National Telecom Company and largest Danish telecom provider and operator.

Rollout and usage

In the period 2003–2006 about 755,000 certificates have been issued. Of these 625,000 have been personal eSignatures (IDABC report:23). These numbers should be compared to the more than 2 million persons using Internet banking.

The scientific magazine "Ingeniøren" ("the Engineer", 12 October 2007) estimated that during the five years the OCES-signature has existed only around 250,000 citizens have actively used this signature. This can be compared to the

[14] It should be noted here that the OCES signature is not covered by the Danish eSignature Act as the OCES signature is not based on a qualified certificate. Neither is the OCES signature covered by any other general eSignature legislation under Danish law.

[15] Currently the organization danID is the only authority issuing OCES certified signatures.

[16] www.signatursekratariatet.dk. Accessed on 30/8-09.

existence of approximately three million Danish internet users (54.4% of the total population). By comparison, in 2007 there were 2.2 million users (39.9% of total population) of the banks' digital-sign-on solution: netID[17].

There seem to be a number of reasons for the slow uptake of the OCES signature. The first one is the obvious fact that there has been no clear benefits for citizens and businesses in using digital signatures. Thus, even though a number of eGovernment solutions have existed for a long time, and new ones are continually being developed, it is not always clear how citizens or business benefit from using them. Secondly, there have been technical difficulties with TDC`s version of a digital signature where especially Mac-users have had problems in installing the software.

However, during the last 1½ year the figures have changed dramatically. According to Statistics Denmark (the national statistic agency) there were 1,176,260 digital signatures (21.3% of total population) in 2009, composed of 999,263 personal certificates, 171,447 employee certificates in 51,000 corporations/ public authorities, 5,441 corporate certificates and 109 functionary/secondary certificates. Furthermore, 215 public authorities (and 8 private companies) can receive e-mails signed with a digital signature and 121 government authorities (and 33 private companies) offer digital service solutions including digital signature. A PBS overview of the eID diffusion in eCommerce shows that in 2008 there were 2.9 billion transactions conducted via PBS[18]. These numbers indicates that despite a slow start, "critical mass" concerning digital signature has finally been reached during 2008.

At the *state level* the first and still most widely used of all public eGovernment applications is in the area of taxation. The first solution to be implemented was the national tax agency SKAT's possibility of personal management of the personal "estimate of future income" statement, and the yearly tax statement with a PIN-code based digital signature, where the citizen could make changes and file reports.

Today, the above mentioned "TastSelv Borger", a system for personal income taxes declarations, is based on an automated tax process, where 97% of all data of importance for Danish citizens' tax declarations are reported by employers, banks, mortgage institutions, trade unions, social benefit administrations, etc. to SKAT. The citizens can report corrections or approve their tax return via the Internet. The result in the form of an annual settlement can be seen immediately. If tax overpayments are due, they are transferred to the citizens' account. If additional tax is to be paid a trade charge form will be sent to the citizen[19].

The system can be accessed using all standard browsers, and exchange of data is encrypted with 128 bits SSL via a proxy server. An XML interface has been defined for the annual tax settlement. The purpose is that the annual settlement data can be transferred via web services following citizen's approval to a bank or another private credit provider for use when citizens apply for loans in banks. The system uses OCES signatures and/or an One-Time-Password (OTP) solution. In 2005 TastSelv Borger had more than 3 million logins through the password solution and around

[17] http://ing.dk/artikel/83002-hoejt-spil-om-den-digitale-signatur. Accessed on 9/11-07.

[18] http://www.pbs.dk/dk/ompbs/fakta/. Accessed on 28/8-09.

[19] Denmark has a pay-as-you-earn income tax system; meaning that for most wage earners there will be little to regulate.

490,000 logins with OCES signatures. This indicated a rapid increase in use of OCES signatures from 2004 (see Table 2).

Another important eGovernment application at the state level is NemKonto. Thus, as of Dec. 27th, 2003 it is mandatory for all citizens and companies in Denmark to have a NemKonto ("Easy Account"). A NemKonto is a normal bank account which the citizen/company already has, and which they have designated as their NemKonto. All payments from public institutions (including salaries) are being transferred directly to this account via the NemKonto System (NKS). The NKS is a database with account numbers and CPR-numbers or company numbers. When a public institution makes a payment to a citizen or a company, the payment is made to a CPR- or company number. The payment then goes from the institution's payment system to the NKS, which attaches an account number, and then to the institutions bank and further to the citizens'/company's bank account. *In this way all public payments are made electronically to bank accounts; there are no longer any checks or cash payments*. For citizens and public institutions it is possible, at www.nemkonto.dk to designate, change or delete an Easy Account. Staff in public institutions with the rights of access can log on to the website and stop payments or search for payments their institution has made. Access is attained by logging on to the website using an OCES signature.

At the *regional level* an important application is the national healthcare portal (www.sundhed.dk) run by the regional organization *Danish Regions*. Sundhed.dk brings together the entire Danish health services on the Internet, making it the electronic way for patients, their families, and health care professionals to obtain information, communicate and maintain an overview. The application processes XML-based datastructures for national CAs, Lab-systems in hospitals, national medicine and patient databases. At the moment there is no certificate signature exchange between systems. The security between systems is handled by a point-to-point private secure network. Users use OCES software certificates to access the application. Some users copy the certificate to a "token/memory stick" and use it like a smart card. However, this is not application driven. In 2006/2007 there were approximately 110,000 users with their own eSignature.

The Danish municipalities offer a range of eGovernment applications in areas such as child care, schools, building permissions, welfare benefits, etc[20]. Many of these applications are used by a large number of municipalities and provided through the website www.netborger.dk. This site is owned by Local Government Denmark (KL). The applications of the website is developed and operated by KMD (now KOMBIT A/S), a Danish software house, which until recently was 100% owned by the municipalities through KL. KMD/KOMBIT A/S is operating on market terms but has a very strong position in the Danish market for municipal ICT-services and applications. As www.netborger.dk is an umbrella application with a range of individual applications no general rule covers the use of eSignatures in the application. However, the application uses OCES signatures, and in week 43, 2006 it had approximately 800,000 log-ins of which 25% were using OCES certified eSignatures.

[20] For a full list of applications; see IDABC report: "Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications. National Profile Denmark". European Commission, Directorate General Enterprise. November 2006.

Table 2 Rollout of eIDs in Denmark compared to Belgium, Spain and Austria

	BE	ES	AT	DK (OCES)	
State of rollout early in 2009	9.3 million, 90 % of the Belgians entitled to an ID card	3 million, 10% of the Spaniards entitled to ID card	8.4 million e-Cards, 100% of all citizens	1.2 million digital signatures, 21% of all citizens	
eID function activated	7.5 million (80%)	not necessary	approx. 74000, 0,9% thereof approx. 20000 office ID cards	not necessary	
Use rate of electronic personal income tax (% of tax payers)	2008: 24% 2009: 56%	21%	25.7%	2007: 59% 2008: 71% 2009: 87%	
eID use rate for income tax (% of the electronic applications)	2008: 3.6% 2009: 14,2% (half of them with the help of civil servants in the tax office)	2008: 0.1% 2009: 0,2%	2008 0,7% 2009 1,0%	OTP TastSelv / OCES	
				2007 0,3 Mio (18 %)	1,9 Mio
				2008 0,4 Mio. (15,3 %)	2,2 Mio
				2009 0,6 Mio (18,8 %)	2,6 Mio

As of January 1st 2007 a central entrance to public eGovernment services has been established: www.borger.dk, and most eGovernment services mentioned in this article is available through this portal. From January 2008 a "my page" has been accessible to all citizens with a digital signature based on the OCES standard.

The newest development in this area is the development of the EasyLog-in (NemLog-in) solution, which was an initiative taken to incorporate the vision of the Government's Digitalization Strategy 2007–2010. The EasyLog-in claims to be the world's first cross-governmental Single Sign-On solution. It makes it possible for a user to log-in and gain access to all public systems without being prompted to log-in again at each of them (see: www.epractice.eu/en/cases/easylogin). The development of the EasyLog-in is related to the development of the www.borger.dk portal, because when the portal was launched it was crucial to have a log-in solution that accommodated single sign-on. However, EasyLog-in is not restricted to www.borger.dk but is adapted across multiple public digital services. The vision is that the EasyLog-on will provide citizens with a single sign-on to all public digital national services by 2010.

As of 2009 the EasyLog-in was implemented in 22 cross-governmental digital services, which the citizen can then access through a single-sign-on. When the citizen access the "my page" the citizen can access his/hers own individual data collected through multiple public authorities, including tax services and local authorities, thereby creating a seamless public sector and easing work flows for the citizen. As a part of the 2007–2010 Government Digitalization Strategy it is recommended that EasyLog-in is made mandatory as the only authentication for all nationwide citizen-oriented services that require secure identification by 2010. At the moment the EasyLog-in requires that the user use an OCES-based digital signature to log-on to the system. However, in order to achieve the same or even better functionality with a heightened level of security a new version of the digital signature is currently being developed: The NemID, dealt with below.

The near future: the creation of a common public/private standard?

The contract between TDC and the National Board of IT- and Telecommunications (NBIT) expired in 2008. The new tender for implementation during 2009 was won by a joint venture between TDC and PBS. Soon afterwards TDC retired from this business and PBS, via danID, its organization for eSignatures taken on the contract with NBIT alone. Thus, danID (PBS) is now responsible for the "old" OCES certified digital signature as well as for the development of the new generation of eSignatures and their rollout. This will be the case till 2017, when a new round of tendering will take place.

The new digital signature will still be software-based, but will be a true two-factor identification solution, which contains something you know (username/password) and something you get (OTP), independent of the PC the citizen employs. When the cardboard OTP card runs out, danID will send a new one by mail, and the user will then be centrally certified meaning that any computer—domestic or foreign—can be used as a point of access[21]. In addition to what is required to get an OCES certified eSignature (see above) a passport- or driving licence-number (which is checked against the police registry) will also be required when applying for the new digital signature. This is in order to achieve an elevated level of security; the so-called "White-washing level" equivalent to that used by eCommerce banking etc., which will function as a comprehensive private and public solution. This development has meant that Danish banks are now en route to implement the new digital signature and migrate their existing customers as starting from February 2010. Users will be able to order this new so-called *"nemID"* from public authorities, and choose whether they will also attach their already existing e-banking log-on or not. Table 3 gives an overview over differences between the different OCES-based eSignatures, the old netID and the NemID, which will unite the two other ones.

With NemID the citizen with a single signature—and later card—will be able to carry out any transaction or use any public service without being restricted

[21] Digital Signatur, danID "Ny digital signatur – DanID: fakta om den tekniske løsning" on http://www.pbs.dk/wwcm/resources/file/ebea790bf0593d0/danID-Faktaark.pdf. Accessed on 27/8-09.

Table 3 Differences between the OCES-based eIDs, the netID and the NemID

	OCES	netID (banks – old)	NemID (new eID)
Issuer	Regional Certification Centres (answering to the Center for Digital Signature)	Individual banks and other proprietary institutions (e.g. insurance companies)	danID (OCES certified eID's)
Authentication components	SW cert.	Based on existing financial institutions' identification solutions	SW cert.
Certification authority	The Ministry of Science Technology and Innovation	PBS develops and issues netID software commissioned by individual banks	Ministries and financial institutions (all complying to the OCES standard)
Reg. auth.	Certification Centres	Branch bank/financial institution	Certification Centres
Content of certificate:	-Name (optional) -Address (optional)	-Bank used -Name	-CPR number -Zip code
-Name		-Address	-Email address
-CPR No.	PID	-CPR number	
		-Email address	
Authentication of applicants	Address is checked against CPR registry, but CPR number is not included in the certificate itself	A pairing of an issued PIN-code letter and an installation-link. Signed written agreement by mail	A pairing of an issued PIN-code letter and an installation-link as well as a passport- or driver's license number.
Relation to CPR	Does not contain CPR number, but PID which can be converted to CPR No.	Requires personal information checking with the CPR registry	Requires address checking with the CPR registry

geographically, and at the same time be able to use the signature for Internet-banking and many other commercial services.

Assisted by the IT-Political Association, the Ministry of Science, Technology and Development has developed requirement-specifications for danID, who has had to live up to the Danish Industry Union's (DI) recommendations on privacy and security. However, especially the debate concerning central vs. local storage of keys and OTP's has exacerbated the debate on Internet forums where programmers and interested associations have seriously questioned the possible maintenance of private information integrity when storing these. Still, this debate concerning whether it was in fact possible to compartmentalize information across both public authorities and the public/private divide, so that only those who were authorized and needed the information would have access to it, was most intense before real demands on technologies and standards used were decided. Since then, with the inclusion of concerned parties in monitoring groups that are in continual dialogue with danID, the debate has somewhat cooled. That the specific technologies and standards were not completely decided upon was a huge factor in fueling this debate and despite later clarification continues to foster some concern. The Danish Consumer Council ("Forbrugerrådet") were summoned at the beginning of the new tender, and expressed similar concerns regarding the level of security and problems related to the sharing of information on such a large scale. According to the Center for Digital Signature, the choice of standards and software has however somewhat appeased this consumer rights group.

Other features inherent in the new solution have also helped in putting concerns about security to rest. The flexibility of the new solution means that add-on solutions where the signature can be stored on e.g. a smartcard can be purchased, and gives a further sense of security if you are concerned about unauthorized access or need a signature for very specific application purposes. At the same time, despite keys being held centrally, the password that can de-encrypt these will still only be known by the citizen.

The new "nemID" digital signature being the de-facto solution in Denmark, the tendency in eSignatures is now that other solutions are being phased out. The government's ID3 digitalization strategy's 2012 objective is that all adult Danish citizens should have a digital sign-on solution, and includes standardization demands for this signature. The B 103[22] connects seven open standards to be used within public administration on a national level, where any new solution should support the 2012 objective concerning digital signatures. If on a ministerial or municipal level, an actor wishes not to conform to the technical standard, the burden of proof falls on the issuing party.

At the time of writing the current focus is on the employment of OTP-cards with a limited number of passwords, as they will be printed on cardboard or the like, and these will in effect provide the two-factor solution referred to above. In the long term, electronic credit-card size cards that will generate an OTP will be the goal. Furthermore it is imagined that mobile phone technology will assist in this endeavor, especially text-message (SMS) based OTP's that can be sent via cellphones (the Wireless Public Key Infrastructure solution WPKI). To be able to follow the development and adapt/adjust this development if a technological breakthrough should occur is also a built-in requirement of the contract. As the Subscriber Identity Module-card (SIM card) existing in mobile phones in Denmark today are not able to store digital signatures, one could imagine following the Norwegian example where government authorities are already issuing SIM-cards prepared for this solution. At an estimated 1.5 € more than regular SIM-cards this would not be a cost-heavy nor technically demanding possibility.

The Minister of Science, Technology and Development—Mr. Helge Sander—has in addition to this expressed a long-term vision containing a citizen card, which among other things would contain the new digital signature. At the same time, cross-sectoral use of a single identification mechanism, and the possibility of adding information from the Health Card and passport will over time create such true eID/eIDC solution.

[22] The decision of June 2nd 2006 to include mandatory open standards (ODF and OOXML) in digitalization strategies on http://www.itst.dk/filer/Publikationer/aabnestandarder/Rapport_om_implementeringen_af_ODF_og_OOXML/html/chapter04.htm. Accessed on 30/8-09.

Similarities and differences in relation to other EU Member States

Actors constellation and influence

There is little doubt that the state and public administration was the main driver in trying to establish eID in Denmark from the beginning when this was set as a priority in the first government IT-strategy in 1992 and until the first public tender on digital signature in 2002. After 2002 the private sector; i.e. the telecom industry and the banks have come to play a more significant role realising that there might be advantages in developing an eID that is uniform and can be used across sectors.

Within Government the dominant policy field was Public Administration, in particular modernization via eGovernment. Issues of visual authentication, important in Belgium, Germany and Spain did not play any role as there is no national ID card in Denmark which could have been used as a token for the eID. Due to the outsourcing strategy of government the Telecom Industry and later on the banking sector have played a major role (see Table 4).

Path dependency

The path dependencies of the Danish eIDMS according to the conceptual framework introduced by Kubicek in the introduction to this Special Issue, concern the definition of the eID and the organizational arrangements, the technical components as well as the institutional paths. We will focus on the OCES certificates and the new nemID only.

The definition of the eID, i.e. the data on attributes supported by the OCES certificates and well as the new nemID refer to the data from the CPR including the CPR number, although converted into the BID. The BID is a kind of path creation developed to meet requirements, which did not allow to include the CPR number directly.

In terms of organizational arrangements we can say that in the Danish case there was a path creation as well as a new organization as the certification authority has been created through a tendering process every 4th year.

The technological path refers to the adherence to international trends and standards. In this respect the Danish case differs from most of the other European countries in so far as it did not deploy smart card technology but built on a software

Table 4 Estimate of the importance of different actors in establishing eIDs

Actors and their weighting in the process (1 = low, 3 = high)					
Actors / policy fields	GE	AT	ES	BE	DK
Interior/Police	3	1	3	1	1
Public Admistration	2	3	2	3	3
Industry/Commmerce	1	1	2	1	2
Finance	1	1	1	1	1
Social/Health	1	2	1	2	1
Chancellery/Cabinet	1	3	2	1	2

solution. This is in particular remarkable as it meant that the requirements for qualified digital signatures could not be met. Another difference is that in the other countries included in this special issue there are two certificates, one for authentication and one for signatures while in Denmark the same certificate is used for both functions. The Health Card, which is a chip card, has not received sufficient support to become an eID token beyond the health sector, which is the case in for example Austria. NemID, the new common public/private digital signature solution can be seen as a kind of path merger as it combines OCES with the previous bankID.

Concerning the institutional path or regulatory pattern new institutions have been created to govern the development (the Digital Task Force in particular) . The legal framework, the law on electronic signatures passed in 2000, basically transposed the EU Directive on Digital Signatures into Danish law. However, the outsourcing of the CA and the periodic contracting was a case of path creation, while assigning the governance function to the National Board of IT- and Telecommunications continued an existing path.

Intragovernmental coordination

In the Danish case it is quite clear that even though there were several plans for eID cards already in the mid-1990s, the development of eIDs/digital signatures did not take off till the establishment of the Digital Taskforce, a cross-ministerial and cross-sectoral unit under the leadership of the Ministry of Finance. The taskforce, which can be considered as a clan of civil servants dedicated to make eGovernment work, was given the power to formulate the "eGovernment Initiative" in which the establishment of a common public sector digital signature was a key priority.

However, in order to establish such common signature the Taskforce was dependent on a good working relationship with the Center for Digital Signature under the Ministry of Science, Technology and Innovation, which eventually developed the OCES standard. Also, in order to roll out the signature, the Ministry's Board of IT and Telecommunications has been essential, as the Board has been in charge of the two public tenders outsourcing the CA, and for the formulations of contracts with the CA's as well as the required audits of them. So while the roles of the different actors (ministries) as well as the "line of command" was unclear before 2001, later on this became much clearer: roles have stabilized, and while the supremacy of the Ministry of Finance is quite clear, considerable leeway is given to other ministries as well as the private sector.

Privacy issues

Privacy concerns played a role at several points in time during the twenty year span covered here. The first juncture was in 1992–94, when the idea of a multi-purpose ID card (the "citizen card") was launched. Public administration (Ministry of Interior, Ministry of Finance, Local Government Denmark) tried to push the card, but met resistance from a majority in Parliament and the Board of Technology, the Parliament's advisory board on technological matters. Concerns were first of all over the possible (mis)use of the card by government authorities and over the mandatory nature of the card. The conflict eventually led to the infinite postponing of an eID card in Denmark, and to the search for software based digital signatures as a solution to the question of electronic identification; a type of path dependency which has been visible in Danish eGovernment strategies ever since.

The second juncture started 2009 after the second public tender on digital signatures with regard to the development of the NemID signature. Here critical IT-experts, some of them organized in the IT-Political Association, as well as consumer representatives have raised concerns over the maintenance of private information integrity in connection with the proposed central storage of keys. However, this time government and public administration seemed to have learned the lesson, and have co-opted the critical voices by giving them a place in groups deciding on the standards and software to be used. This seems to somehow have appeased these voices, even though the IT-Political Association has decided to quit the group in which they were represented. This development has meant that the rollout of OCES certified eIDs has been able to continue, and that it now seems to be reaching critical mass.

"Staatsverständnis"

As we have seen above the provision of electronic signatures in Denmark developed in two parallel tracks in the private and public sector respectively. This was very much in accordance with the "mixed economy" or "liberal social democratic" tradition of the Danish welfare state. The validity of this position was not questioned till the establishment of the Digital Taskforce and the "eGovernment Initiative", which pointed at how the "parallel track development" slowed down both e-commerce as well as the use of public eGovernment applications. As a results of this, and maybe also of the shift of government in 2001 from ten years of Socialdemocratic lead governments to a liberal-conservative government, the private sector was given a more prominent role in the provision of electronic signatures through the outsourcing of this provision (establishment of CA's) following the public tenders in 2002 and 2009. With regard to electronic signatures the situation in Denmark since 2002 can therefore be said to be quite similar to the German situation in that there is now a private certification authority under state control. There might be a difference in that the Danish government has from the beginning provided the CAs with quite considerable funds. These funds can be seen as a way of subsidizing the introduction of electronic signatures in Denmark. However, when it comes to the eID function there are big differences to countries like Germany, Austria, Belgium and Spain, which do not leave this to the private sector, while we find developments similar to the Danish case in Sweden and Estonia.

Conclusion

In the beginning of this article the Danish development of eIDs was presented as a paradox as there still is no qualified digital signature as defined by the EU eSignatures Directive nor any other nationwide eID, which can be us to access eGoverment applications on all governmental levels, although Denmark had an early start, and much political attention concerning eGovernment compared to most other nations, and even though the "e-readiness" of the Danish population is considered to be one of the highest in the world.

Laying out the technological, organizational and legal dimensions of the history of eID in Denmark, and comparing these with other European countries, has made it it possible to explain this paradox. Thus, there seems to be three main reasons for why the development in Denmark has taken the special path it has. These are: 1) privacy concerns, 2) lack of intergovernmental coordination, 3) lack of cooperation between public and private sector.

Thus, when the idea of a multi-purpose eID card—the citizen card—was first launched (1992) the idea met popular resistance represented by The Board of Technology and a majority of members of Parliament, who were concerned about the possible misuse of the card by government authorities and the mandatory nature of the card. The "governmental coalition" (Ministry of Interior, Ministry of Finance, Local Government Denmark) pushing for the implementation of the citizen card did not tackle this challenge very well, which lead to the postponing of a general eID in Denmark, and to the search for less ambitious digital signature solutions.

Following this event the responsibility for eGovernment initiatives in Denmark was taken over by the Ministry of Science, Technology and Innovation. However, this newly established (1993) and financially weak Ministry lacked the necessary muscle to coordinate eGovernment initiatives, and in the period 1995–2000 a range of different digital signature solutions were developed in different policy sectors and at different governmental levels. This meant a slow take up of the digital signature and a suboptimal use of eGovernment applications. However, a sharper government focus on eGovernment after 2000 led to the creation of the Digital Taskforce, a cross-ministerial and cross-sectoral unit in 2001, and transferred the overall responsibility for eGovernment policies back to the Ministry of Finance.

Establishing a common public sector digital signature was a key priority for the Digital Taskforce, and it initiated the work with a common public certificate standard for digital signatures—the so-called OCES standard, which was launched in 2003. The OCES-based digital signature(s) is widely supported by public institutions in their eGovernment applications, and it is now mandatory that digital signature(s) to be used in the public sector are based on this certification. This coordination effort and greater pressure on policy sectors and institutions to comply with the common standard seems to have carried fruit as use of digital signature has now dramatically increased; especially within the last 1 1/2 year.

While take up was slow in the public sector the use of digital signatures/eID solutions has exploded in the private sector; especially in the banking sector since 2000. At the outset these solutions were developed in isolation from solutions in the public sector, and the banks saw little benefit in cooperating with the public sector in this area. However, with the public tenders on digital signatures in 2002 and 2009, which has given the private sector a bigger role in this development, the situation has changed. This has become particularly clear after the tender in 2009, which was (in the end) won by PBS, which is a payment service and credit card organization owned jointly by the National Bank and a number of private banks. The banks, which have been much concerned about their security-level, have now been convinced that it is possible to use a new, secure digital signature solution—the so-called "Nem ID"—across the public/private sector divide. The idea with this signature—and later card—is that the citizen will be able to carry out any transaction or use any public service, and at the same time be able to use the signature for

Internet banking and other commercial services. Thus, the commercial banks have now started to migrate their customers to this solution.

The roll-out of the NemID will continue in the next couple of years, so it seems that Denmark will finally—after around twenty years of delay—have an eID card to be widely used in the public as well as the private sector.

References

Digital Signatur (danID). *"Ny digital signatur – DanID: fakta om den tekniske løsning"* on http://www.pbs.dk/wwcm/resources/file/ebea790bf0593d0/danID-Faktaark.pdf. Accessed on 27/8-09.

European eGovernment Services (IDABC). *Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications. National Profile Denmark.* European Commission. Directorate General Enterprise; 2006.

Hoff J, Rosenkrands J. When democratic strategies clash: the citizen card debate in Denmark. In: Hoff J, Horrocks I, Tops P, editors. *Democratic Governance and New Technology.* London: Routledge; 2000. p. 110–24.

Ingeniøren ("the Engineer"). Issue from 12 October 2007. Copenhagen.

Johansson S. Lokaldemokrati i informationsalderen. In: Hoff J, editor. *Danmark som informationsamfund. Muligheder og barrierer for politik og demokrati.* Aarhus: Aarhus Universitetsforlag; 2004. p. 226–50.

Ministry of Finance. *Effektiv EDB i staten* ("Effective It in State Administration"). Copenhagen; 1992.

Ministry of Interior and Health. "Nyhedsbrev: om international social sikring", nr. 1. Copenhagen; 2007.

Ministry of Science, Technology and Innovation. *Digital Signatur OCES – en fælles offentlig certifikat-standard*. Copenhagen; 2002.

The Economist's Intelligence Unit; 2009.

World Economic Forum. *The Global Information Technology Report 2008–2009*; 2009.

Internet references:

http://www.e-gov.dk

http://www.cpr.dk/cpr/

http://www.nemkonto.dk

http://www.sundhed.dk

http://www.netborger.dk

http://www.borger.dk

http://ec.europe.eu/information_society/eeurope

http://www.epractice.eu/en/cases/easylogin. Accessed on 12/2-2010.

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

http://www.politi.dk/da/borgerservice/pas/pasudstedelse/. Accessed on 20/8-09.

http://www.transportnyhederne.dk/?Id=23104. Accessed on 25/8-09.

http://www.cpr.dk/cpr/site.aspx?p=16. Accessed on 1/8-09

http://www.im.dk/publikationer/fremtid/verdist.htm. Accessed on 25/8-09

http://www.scandihealth.dk/Losninger/Losninger_infoark_pdf/Sygesikring/Vejledninger/Sygesikring_EU-sygesikringskort.pdf on 25/8-09.

http://ec.europa.eu/social/main.jsp?catId=652&langId=da. Accessed on 24/8-09

www.signatursekratariatet.dk. Accessed on 30/8-09.

http://ing.dk/artikel/83002-hoejt-spil-om-den-digitale-signatur. Accessed on 9/11-07.

http://www.pbs.dk/dk/ompbs/fakta/. Accessed on 28/8-09.

http://www.itst.dk/filer/Publikationer/aabnestandarder/Rapport_om_implementeringen_af_ODF_og_OOXML/html/chapter04.htm. Accessed on 30/8-09.