

ICA 37th Conference: Fourth Session

PROVIDING DENMARK WITH DIGITAL SIGNATURES

Yih-Jeou Wang

Ministry of Science, Technology and Innovation

DENMARK

Yih-Jeou Wang is Head of Division in the Danish Ministry of Science Technology and Innovation and is the ICA National Representative for Denmark. He has responsibility for IT security policy matters and the Danish National Digital Signature project.

For the past two years he has participated in the implementation of a new IT and telecom policy in the Danish Confederation of Industries where he was responsible for significant re-orientation of the Confederation's industry policy.

For several years different Danish Governments have pushed forward reforms of the public sector looking at IT usage as a means for making public sector more effective and user oriented.

The key barrier has in all these years been the lack of digital signature making electronic communication both reliable and safe. Therefore the Danish Government has made digitalisation of public sectors administration a significant area for reform including a total revision of the governmental structure at local level. It is in this context that the Danish Government has emphasised the importance of getting a common public sector digital signature in order to ensure a fast development of a more effective and digitised public sector for the benefit of citizens and businesses and of course the public sector itself.

I'm going to give you a first hand insight into one of the most significant projects in Danish administrative history, a project which in four years should provide all Danish citizens and businesses with digital signatures. Statistics; Denmark's recent survey on the Danish public sector IT use in 2002 shows that the public authorities and institutions are expecting to make use of digital signatures in administration this year. The differences between the state, the counties and the municipalities should be understood in the context that the local Governments have most of the direct contact with citizens. The counties have, there is two of them, major responsibilities, the hospitals and right to protection issues. The municipalities are primarily responsible for issues like child care, schools and social security involving a very heavy and intense communication with the citizens therefore local Government's expectations are generally high and positive regarding uses of digital signatures. If you take a look at the situation in a Danish private sector there is a lot of potential for better IS security culture using basic security methods to protect communication between businesses themselves as well as between businesses and the customers. Only 24% of the businesses on the internet use a secure server connection. 14% of the businesses have made it possible to receive digital signatures. 12% use other identification methods such as pin codes and only 9% use encryption to protect the content of the communication. The Danish Digital Signature project is based on several years of

experiences concerning technical considerations, user and market observations and judicial considerations. Several technical and use experiences were gained through a number of pilot projects in municipalities in a period 1999 – 2000. Denmark was among the first EU member states to implement the Electronic Signature Directive in national legislation back in 2000 and based on the electronic signature public tender and security solutions were carried through in 2001 giving the public institutions the possibility of using a framework agreement to buy qualified digital signatures and other security products supporting the implementation of digital signatures. It was in fact expected that given the legal basis and a commercial attractive framework agreement the market would have sufficient incentives to secure the development of security solutions, a basic industry standardisation and market-based interoperability. On the other side it was also expected that public institutions would commence to demand products and services from the market players but all that just didn't happen and could see that it was the same picture all over Europe.

We identified different areas. There was a lack of standardisation of a digital signature. In order to get a digital signature according to the act you have to be identified in person by a third trusted party. It was just too expensive for citizens to get a digital signature and if he or she wanted to use it at home many technical problems occurred and the most important thing at that time it was very difficult finding an electronic service, public or private where it was possible to use a digital signature and lastly, it was extremely difficult for marketers to find a feasible business case to build a sound business on. It takes several millions of Euros to establish certificate authority and who should pay for the services. The aim of the Danish Government was to establish a general scaleable and transparent security infrastructure based on public key infrastructure. By establishing this it would be possible to use advanced security methods like digital signatures and encryption.

Having these experiences in mind the next obvious step to take was to overcome the lack of a common standard for digital signatures making it possible for marketers to concentrate on delivering services rather than speculating on which de-facto standard would win on the market. The Ministry of Science Technology and Innovation took up the task of defining common standards for common public sector digital signature. It was important for us to make the digital signature easy to distribute and for receiver of a digital signature easy to install and at the same time securing a sufficient security level of the signature sufficiently enough for public authorities to recognise it and to use it for authentication of citizens and businesses. It was very important to overcome the demand for personal presence for identification when a person wanted to get a digital signature. It was therefore decided to define the digital signature at the lower security level using a softer based digital signature issued after a controlled check of a person's identity in a Danish central person register but activated through a pin code letter sent through by ordinary mail. The Certificate of Authority has an extended and unlimited responsibility towards citizens concerning the burden of proof if the signature should be mis-used by others. This extended responsibility is just the same as the citizens would have had according to the National Act on Electronic Signatures. Businesses can though rely on several agreements with a Certificate of Authority.

A digital signature can be used for admittance control, lock on, encryption of e-mails and for digital signing of e-mails and at web sites. The digital signature can be issued as a personal certificate for citizens, as employee certificates for employees in a

business or public institution and as a business certificate to identify business or public institution. The Danish Data Protection Authority approved the common public sector digital signature as sufficiently secure for most kind of communications including sensitive communications. The aim of the Danish National Digital Signature project or the OCES project was to find one or more suppliers of digital signatures based on those as standard. The Government set aside a budget of €6.7 million Euros for a project. It was important for the Danish Government that it would be possible to find one or more models for public private partnerships. It was extremely important to have the private sector as a partner and as an active user of the digital signature as this would give each citizen more services to access using the signature.

The public tender was gone through in two steps. Step One was to go through a project competition focusing on having marketers to creatively suggest feasible business models. How they can support a fast dissemination of digital signatures and how existing services could be activated to boost the usage of digital signatures. The project competition ended with three winners, one didn't want to continue in their negotiations, the two remaining bidders for the contract were a consortium of Danish banks and TDC the former national telecom company. After 1.5 months of tough negotiations with both bidders the winner of the contract was TDC.

The contract was signed in February this year, but what was the outcome of the tender and how did the contract implement the goal for providing Denmark with digital signatures? We got a contract, which is for four years with an option of one more year. The contract contains a corporate agreement and a framework agreement. The corporate agreement covers all public authorities, all institutions, central Government, all the counties and all the municipalities. The framework agreement contains a product catalogue and a model delivery contract for the public sector to use. The contract also contains a list of recommended prices and a business model for the private sector to use. The corporate agreement makes it possible to issue digital signatures free of charge to all citizens in Denmark. It makes it possible for all citizens to get installation support free of charge. It makes it possible for all citizens to make use of digital signatures between each other and between the citizens and the public sector free of charge. It makes it possible for all business to communicate with the public sector using digital signatures free of charge.

In a traditional business model the principle was that the sender of a digital signature had to pay for getting a digital signature. The business model agreed upon in Denmark has turned this around so the receiver of the digital signature has to pay. The background for having this business model is that there is a significant barrier identified from our pilot projects which was that practically no-one would pay for getting a business signature mainly because there was nowhere to use it. To make the receiver of the digital signature digital signature compliant, the burden of payment has been laid at organisations which may benefit from the efficiency gains of digitalisation. That is, the Danish government has paid for all citizens' usage of digital signatures where we have the nature of the usage through the public tender. The Danish government also paid for all Danish businesses' usage of digital signatures in their interface with the public sector, while the usage with regard to business to business, or business to customer has to be paid by the private sector themselves.

Furthermore, TDC has, according to contract, the legal obligation of distributing certificates through at least five major public or private hosts and they also have the obligation to actively promote the digital signature and usage of it. Their essential obligation is that TDC will only receive full payment, according to the contract, if TDC fulfils the contractual stated goals for the number of certificates issued each year in the full year period of the contract. That is, after one year they have to reach 350,000 issued and activated certificates, increasing to 1.3 million issued certificates in the fourth year. The framework agreement contains a number of products and services, together with the negotiated model delivery contract. All this is to ease the public institution's purchase of digital signature solutions. It contains the issue and usage of employee and business certificates, all kinds of certificates and add-on components for the reception and handling of web signatures. Local registration functions for management and employee certificates, support for the employees, support for citizens, education on installation and usage and other useful services like time stamping and archival functions.

Today, a number of electronic services, digital signature enabled down service, among those are electronic services at the National Tax Authority with more than 300,000 potential users at the moment. The Ministry of Foreign Affairs is one of the first Danish Ministries to take up digital signatures, primarily in their communication with presentations and the European Union. Fifteen municipalities are today digital signature enabled, primarily making it possible for citizens to send digital signed emails and for citizens to digitally sign forms in electronic self-service solutions. TDC has enabled two on-line services until now and it is contractually obliged to enable all their electronic customer services. The potential is more than six million customer relations, bearing in mind that the Danish population is 5.1 million inhabitants. The largest private health insurance company in Denmark has, within the last three weeks, enabled their e-services with the potential of 1.7 million customers using their e-services. Virk.dk is an official public sector portal for companies making it easy for companies to deal with the public sector channelled through this portal. All public authorities having administrative dealing with companies are available through this portal. It is expected that more than 250,000 companies will use the portal that makes it mandatory to use digital signatures.

As you can see on this slide, significant number of our electronic services will double in the next half to one year, expanding a number of attractive public and private electronic services, where it will be possible to use digital signatures. Well, what have we achieved until now? You have to remember that the contract was signed in February this year. TDC, our supplier of signatures, were registered to produce and deliver signature-related product services from March this year. TDC opened for employee and business certificates in July and Virk.dk, the official public sector portal for companies only opened six days ago. It has been a very difficult co-ordinating task, getting the entire public sector to work together on this significant and, at the same time, technical and organisational challenging task of introducing on a large scale, the usage of a public key infrastructure and digital signatures. By September 1st, Denmark employed e-day: on this day all communication between public authorities and institutions, in central and local governments, have to be electronic but only with up to non-sensitive communications. This covers about 80% of different types of non-sensitive communications between public authorities and

institutions. The Danish Government announced earlier this month, a supplementary policy statement, committing themselves to the effect that all Danish citizens and businesses may send communication digital-signed, with a digital signature to a public authority or institution. The public authority or institution should then be obliged to receive emails with digital signatures. An 'eDateII' will probably be announced later this year, committing the whole public sector to make another significant leap towards digitalisation next year.

The Danish Government has promised to deliver digital signatures to all citizens also encompasses different groups of citizens with special needs, as more than 5,000 are additional handicapped. A strong focus of projects is also the task of converging existing electronic services using pin codes to digital signatures. In order to secure a growing open source community, the possibility of making use of digital signatures within an open source solution has been developed in a giant project between TDC and the Open Source Community. A solution is under development concerning Danish citizens registered with secret addresses or citizens living abroad. A solution concept for mobility of digital signatures has been developed by TDC giving the possibility of storing your digital signature on an encryption chip or on a smart card.

What kind of experiences have been gained so far? Well, it does take a long time to establish an open security infrastructure in large scale for digital signatures. Even though we have chosen to use a software based digital signature, it is still our long term goal to meet higher security levels by using qualified certificates according to the new Director and National Act. We hope that by introducing the software based digital signature and using it as a common public sector solution today, it will have a quicker penetration in Denmark, and thus making people more aware of using security products, and efforts in protecting one's own electronic communication on the internet. With experiences so far, it is obvious that the main driver for fast penetration of signatures is the number of relevant and interesting electronic services available whether they are private or public.

We are still at the beginning of our project, and we anticipate a fast increase in the use of digital signatures in the coming years. Our supplier, TDC is still very optimistic and expect to meet their goals on the number of certificates issued each year in the contract period. Their motivation is imminent. They don't get full pay if they don't meet the goals. The public sector's motivation is imminent too. If you don't make your administration still more effective, you don't cash the efficiency gains; thus you won't get the budgetary fees to meet the challenge of a constant pressure on public budgets in coming years.

Thank you for your attention.