



Ministeriet for Videnskab
Teknologi og Udvikling

eID/Authentication/Digital signatures in Denmark

8. July 2008

*Nikolas Triantafyllidis / Charlotte Jacoby
Special Advisors
Centre for Digital Signatures
National IT- and Telecom Agency*



Digital Signatur-én kode er nok



Authentication and eID Services

Def.: Authentication (including eID) constitutes the process of verifying a person's identity to be authentic. In e-government authentication is an essential mechanism ensuring that a user is the person he claims to be.

- No national eID in Denmark under the notion of a national identification card
- Instead a national digital signature infrastructure based on PKI
- National digital signature standard called OCES (Public Certificates for Electronic Services)
 - Based on the national central personal register (CPR)
 - Based on the national central company register (CVR)





Background

- History:
 - EU Electronic Signatures Directives December 13, 1999
 - Act on Electronic Signatures October 1, 2000
 - Public tender on security solutions May 2001
- Barriers for the usage of Electronic Signatures
 - Lack of Standardisation
 - Demand for Personal Presence for Identification
 - Expensive and Difficult Accessible Hardware Solutions
 - Lack of Electronic Services using Electronic Signatures
 - Lack of a Feasible Business Case and Business Models





Goal and foundation of the OCES project

- OCES: Public Certificates to Electronic Services
- Goal:
 - Establishing a general **open**, scalable and transparent security infrastructure based on PKI, controlled by the state and operated by private Certificate authorities (CA)
- Foundation:
 - Defining a state-owned Certificate Policies (CP) and an open architecture based on international standards – called OCES CP
 - EU-Tender with a public private partnership in mind
 - Establishing a non-discrimination approval process for potential OCES CA
 - Broad dialogue with relevant partners





OCES I (2003- 2009)

Security Level:

- Software based digital signature (with mandatory password usage)
- Issued without the demand of personal presence for identification
- CA responsibility:
 - Extended responsibility towards citizens
 - Private businesses may rely on separate agreements
- Authorisation and controlling as in the Danish Act on Electronic Signatures

Issued as:

- Personal certificates – PID (a unique number related to civil registration number)
- Employee certificates – RID/CVR (Employee number/Central company number)
- Business certificates – CVR (Central company number)
- Function certificates – CVR/deviceID

Other relevant information:

- EU-tender (Total funding: €6,7 million)
- Contract with TDC February 6, 2003
- The contract between the Ministry and TDC will be in force 2003 –2007 with an option for one more year
- Business model: The receiving partner is paying a flat rate: € 0.5 – 1.0 per certificate per year – free of charge for citizens
- Corporate agreement covering receiving certificates for all public institutions in central government, counties and municipalities





OCES II (2009 – 2014)

- Centrally stored private keys (mobility)
- Real 2-factor security solution (enhanced security)
 - Username + personal password
 - OTP (One-time password) card
- Fully independent of PC (user-friendliness)
- Acquisition of smartcard/eToken/mobile phone possible
- Joint infrastructure with the Danish banks
- Consistent user experience regardless where the signature is used
- The public sectors share in the infrastructure: €27,3 million over 5 years (1/3 state institutions, 1/3 municipalities, 1/3 regions)
- Free of charge for citizens





Number of digital signatures issued (8. July 2008)

■ Personal signatures:	1.004.612
■ Employee signatures:	172.772
■ Business signatures:	5.484
■ Function signatures:	115
■ <u>Total:</u>	<u>1.182.983</u>





Examples of electronic services using digital signatures

- Sundhed.dk – the public sector's health portal
- The National Tax Authority
- The State Education Fund
- The City of Copenhagen
- Borger.dk – A portal for citizen used by all local authorities
- TDC On-line – online telecom resource (potential 700,000 users)
- "danmark" – the private Danish health insurance company (1.7 million customers)
- "Virk.dk" – the common public sector portal for companies (potential 250.000 companies)
- ATP - the Danish supplementary labour market pension fund (1.9 million customers)
- The Ministry of Education: Central Education Admission Portal (60,000 people per year)
- Many more...



Key success factors in the implementation of the project

- Establishing a standard (CP etc.)
- Easy rollout and usability
- Balancing security and cost
- Public/private partnership
- The business model
- The public sector as a driver





Lessons Learned

- It takes time to establish an open infrastructure in large scale for digital signatures and to get people to use it
- The electronic services are the driver for the rollout of digital signatures
 - Marketing complexity
 - And focus on how to get citizens and companies to use them
 - What is the benefit for the users ?
 - PIN-code solutions are still in use – and they work
 - Important to get the private sector involved





Challenges on in international perspective

- Crossborder issues
 - Trust issues
 - Interoperability issues (certificate semantics, national ID's)
 - Different security levels
- Many different EU-projects with different goals and focus areas





References and links

- www.digitalsignatur.dk (only in Danish)
- www.oces.dk (certificate policies – also in English)
- www.itst.dk (official site for National IT and Telecom Agency)





Ministeriet for Videnskab
Teknologi og Udvikling



Charlotte Jacoby (cj@itst.dk)

Nikolas Triantafyllidis (nt@itst.dk)



Digital Signatur-én kode er nok