Nordic digital identification (eID)

Survey and recommendations for cross border cooperation


norden

Nordic digital identification (eID)

Survey and recommendations
for cross border cooperation

Kjell Hansteen, Jon Ølnes and Tor Alvik

TemaNord 2016:508

Nordic digital identification (eID)
Survey and recommendations for cross border cooperation
Kjell Hansteen, Jon Ølnes and Tor Alvik

ISBN 978-92-893-4469-2 (PRINT)
ISBN 978-92-893-4470-8 (PDF)
ISBN 978-92-893-4496-8 (EPUB)
http://dx.doi.org/10.6027/TN2016-508

TemaNord 2016:508
ISSN 0908-6692

Layout: Hanne Lebech
Cover photo: ImageSelect

Print: Rosendahls-Schultz Grafisk
Copies: 150
Printed in Denmark

This publication has been published with financial support by the Nordic Council of Ministers. However, the contents of this publication do not necessarily reflect the views, policies or recommendations of the Nordic Council of Ministers.

www.norden.org/nordpub

Nordic co-operation
Nordic co-operation is one of the world's most extensive forms of regional collaboration, involving Denmark, Finland, Iceland, Norway, Sweden, and the Faroe Islands, Greenland, and Åland.

Nordic co-operation has firm traditions in politics, the economy, and culture. It plays an important role in European and international collaboration, and aims at creating a strong Nordic community in a strong Europe.

Nordic co-operation seeks to safeguard Nordic and regional interests and principles in the global community. Common Nordic values help the region solidify its position as one of the world's most innovative and competitive.

Nordic Council of Ministers
Ved Stranden 18
DK-1061 Copenhagen K
Phone (+45) 3396 0200

www.norden.org

Contents

Executive summary

Background

Considerable effort has been invested in Europe over the last couple of years on eID and e-signature interoperability across borders. With the eIDAS regulation coming into force 1st July 2016, there will be a legal obligation to accept eIDs from other countries. One of the measures taken by the European Commission is to make cross-border building blocks available from the CEF Digital Programme to establish digital service infrastructures at European level.

The study

This study has been initiated by the Nordic Council of Ministers with the aim to facilitate a Nordic discussion on eID similarities and differences.

A project was set up to investigate and map the eID systems of the Nordic countries; Denmark, Finland, Iceland, Norway and Sweden. The project was asked to investigate and uncover eID related issues of importance for cross-border access to electronic services among the Nordic countries:

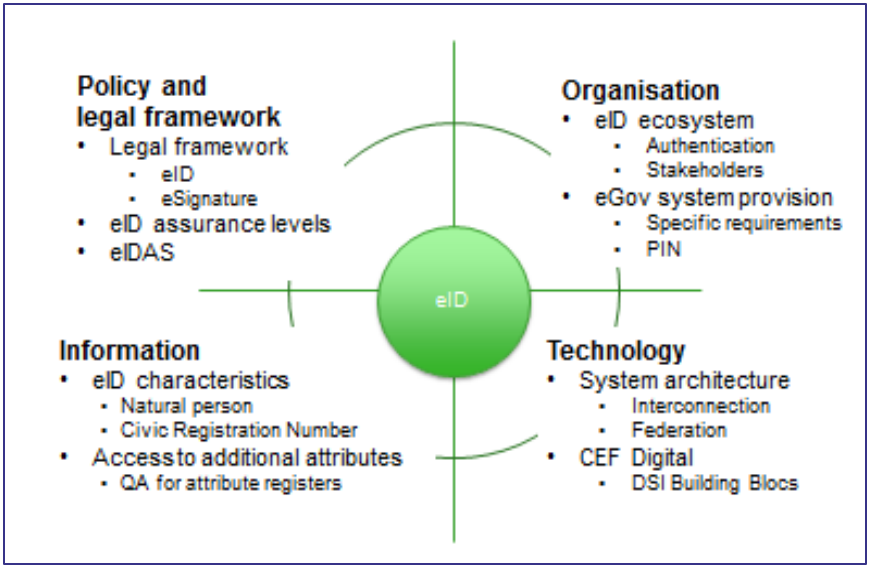
- The Nordic Council of Ministers is the project's sponsor and the formal recipient of the project deliverables.
- The project was carried out by a team set up by Difi, the Norwegian Agency for Public Management and eGovernment.
- The Nordic Council of Ministers established a reference/resource group with participants from the Nordic countries.

The reference group was to actively participate in the study. The group has had three meetings, of which two have been workshop oriented. In addition, two experts have been invited to highlight issues of special interest.

The reference group has been the main source of information for the survey data, which covers:

- Policy and legal framework.
- Organisation.
- Technology.
- Information.

Figure 1: The analytic template



Issues and considerations

Cross border eGov services score low on national policy agendas

Issues	Considerations
The survey question, "Does the eGovernment policy express ambitions for cross border operation, e.g. making eGov services available to foreigners?" revealed a lack of explicitly expressed intentions for such. (4.2).	Nordic cross border eGov service provision would benefit from more support

National eID infrastructures are well organised, but there is a lack of Nordic interconnections

Issues	Considerations
The survey reveals a Nordic system where individual countries have well organised systems for identification and authentication of own resident users. However, these national systems are not interconnected. There are, in 2015, no operational cross border connections between any of the countries with a level of service comparable to that offered to residents within a country. Several Nordic countries have participated in interconnection pilot projects; however, the effort has been technically oriented and limited to proof of concepts.	The EU is promoting the creation of digital connections between European countries through the CEF Digital Programme. Over time, all Nordic countries will connect to this infrastructure. Will these connections fit Nordic needs? A coordination on Nordic level would probably be advantageous for the countries as such, as well as for Nordic interoperability

National eID assurance policies differ greatly. eIDAS will not (in itself) lead to Nordic harmonisation

Issues	Considerations
An eID assurance level is a measure of the trust assigned to a specific eID credential. National policies about how eID assurance levels are defined and how these are applied to specific eGov services vary greatly (3.1). All Nordic countries need to initiate local implementations of the eIDAS regulation. The regulation is "EU-law" and defines a common European norm (low, substantial, high). However, it makes no reference to technical specifications, standards or procedures. This leaves much work to be done at national levels (3.2).	A harmonisation would facilitate cross-border service provision. Will there be harmonisation? Not by itself. The topic is complex and loaded with different national traditions

All Nordic countries have a "Waiting Room" issue

Issues	Considerations 
The provision of eGov services is commonly dependant on a specific PID – a national person identifier with a country specific format. This identifier is a carrier of embedded information about the citizen; e.g. gender and birth date (5.1). Existing procedures to provide a PID to a foreigner are often lengthy and paper based. It is technically possible to create dummy PIDs on the fly that would fit national format requirements and not collide with an existing person identity. However, the use of such solutions is hampered by legal and institutional barriers. When a person has eID tokens from several countries, it is a challenge to assure that they all refer to the same physical person. There is a risk that the person is already registered in the population register, but with reference to some other foreign eID. This calls for sharing of PID information across Nordic borders.	Solutions for real time provision of PIDs for eGov usage could be tested out in pilots and Nordic proof of concept workshops Nordic countries have a tradition for the sharing of civic information, e.g. when people are moving. Online sharing of national civic registration numbers across borders would be useful in order to solve the "waiting room" issue. However, this may imply unexpected risks in the Internet age. A case for a Nordic study?

Differences in the way information access is organised and national information policies make the retrieval of information from other countries difficult

Issues	Considerations 
Many public services depend on access to additional personal information in order to provide the service. This can include information about a person's family situation, skills or education. In the cross border context, this implies retrieval of information from registers in another country. Nordic countries have very different system architectures and practice for accessing and handling person related information. The retrieval of citizen specific information from governmental information sources in other countries faces a number of challenges.	The Nordic countries have a tradition for trusting each other. Can they do so also in the Internet age? Cross-border access to authoritative information registers in other countries will be very challenging. A Nordic survey could be a useful first step.

Nordic eID interoperability is made difficult by a lack of standards

Issues	Considerations
The information content of national eIDs used in the various Nordic countries varies from country to country. This complicates the conversion of a person's eID from one Nordic country's format to another (6.4). The eIDAS regulation defines a minimum European eID dataset for natural persons. The dataset specifies four mandatory attributes and four optional attributes. For operational use this specification needs enlargement and further specification. Some of this work could advantageously be coordinated on Nordic level.	A Nordic eID profile referring to international standards would be very useful. A study could be combined with "proof of concept workshops" to develop best practice solutions.

The Nordic eSignature situation is unique

Issues	Considerations
Electronic signatures have developed to become a complex topic in many circumstances. Considerable confusion results from the fact that "signature" is both a legal and a technical term (8.1). The survey has revealed that most e-government services (and other services) in the Nordic countries arebased on the authentication of the user's identity only, as a basis for "simple" electronic signatures. This is different from European countries with a tradition for Notary and Registrar confirmed documents. Sweden is the only Nordic country where government agencies frequently choose to require advanced electronic signatures to be used. To fulfil this and still offer the user friendliness of a "click to consent" signature, a central signing service has been developed.	How can we make sure that the Nordic countries do not make new and unnecessary demands for the use of qualified or advanced e-signatures? The "Swedish solution" should be investigated further as a combination of a pilot project and related workshops

1. Nordic authentication systems

Identification
Providing answers to the question “who are you?” Typical answers canbe:

- My name is John Clark.
- My user identity is Joclarc200.

Authentication
Providing answers to the request “Please, prove your identity”:

- The most common response to this demand is to present a password.

Figure 2: On the Internet, nobody knows you're a dog

Source: The New Yorker, 1993.

1.1 Governmental eID stakeholders

Survey question 2.1.2

- Please give a short overview of key (eID) governmental stakeholders Roles and responsibilities.

1.1.1 Denmark

The Danish eID framework is based on the open OCES standard. OCES is the Danish designation for Public Certificates for Electronic Services "Offentlige Certifikater til Elektronisk Service".

The legal framework of the OCES concept demands agreements to be set up between Certification Authorities (CA) and the Agency of Digitisation in order to issue OCES certificates. In this agreement, the CA undertakes to comply with the terms of the certificate policies drawn up by the Agency.

At the moment an agreement exists with Nets/DanID as a CA issuing OCES signatures.

1.1.2 Finland

The Ministry of transport and communication (MINTC) is responsible for the laws regulating the Finish eID framework.

The only public authority issuing qualified certificates and strong eID means is the Population Register Centre.

Ministry of Finance (MoF) has a significant role in promoting the digitalization of government services and the Population Register Centre is an organisation under the Ministry of Finance.

FICORA (government agency under MINTC) is responsible of supervision according to the law.

1.1.3 Island

The central identification and authentication system is operated by Registers Iceland. Registers Iceland also issues Icekey (national ID-number and a strong password) and a multi-factor Icekey (Icekey plus a text message sent to the user's mobile phone). Registers Iceland belongs to the Ministry of the Interior.

Ministry of Finance and economic affairs is the owner of the Icelandic root on which the electronic certificates are based.

Auðkenni (a private company) – issuer of qualified electronic certificates on smartcards and electronic certificates on SIM-cards under the Icelandic root.

1.1.4 Norway

Responsibility for the eID area is split as follows:

- Ministry of Local Government and Modernisation: Responsible for regulation and implementation (via Difi) of eID usage for e-government services.
- Ministry of Finance: Responsible (via Norwegian Tax Administration) for the Norwegian Population Register, which is the main attribute provider for identity information.
- Ministry of Trade, Industry and Fisheries: Owns the law on e-signature and is responsible for implementation of the eIDAS regulation into Norwegian law.
- Ministry of Transport and Communications: Responsible for Norwegian Communications Authority (Nkom) and thereby for supervision.

At directorate level Difi (Agency for Public Management and e-Government) is responsible for co-ordination of use of eID towards the public sector through the services of ID-porten. Difi also runs the contact and reservation register holding email and mobile phone numbers used to alert users, and users' reservations against use of electronic communication.

1.1.5 Sweden

The Swedish Ministry of Enterprise and Innovation holds the main responsibility for policy and legal matters.

The Swedish E-identification Board is main responsible for the Swedish eID System and for the STORK 1 PEPS node.

1.2 Authentication for public services

Survey questions 4.1.1 and 4.2.3

- How is the authentication for public services done in your country?
- Is there a common gateway or a portal used by eGovernment services?
- If so, is the use of this portal mandatory or voluntary?

1.2.1 Denmark

In Denmark the use of NemID as token and NemLog-in as authentication portal is mandatory for public-sector service providers. "NemLog-in" provides authentication and single sign-on for public eGovernment services. The national eID infrastructure is controlled by the state ad operated by private Certificate authorities (CA). NemLog-in also provides a power of attorney solution.

NemID is a two-factor eID with username, password and a one time password (OTP). The OTP is a credit card sized paper card with passwords consisting of six numeric digits.

1.2.2 Island

There is a common gateway, the Icelandic identification and authentication portal, run by Registers Iceland. The gateway is used by most public agencies and many private companies. Usage is not mandatory.

There is a choice between using IceKey, Multi factor Icekey (+ SMS) and electronic certificates in phones or on smartcards. The user is sent temporarily to the authentication gateway and returned to the service provider with a digitally signed proof of authentication.

1.2.3 Norway

In Norway the eID gateway "ID-porten" is mandatory and used for authentication by most public services on governmental level. It is also used by many service providers on regional and local level. ID-porten currently serve more than 660 public services.

Norwegian citizens have a choice between four eID alternatives:

- *MinID*: Developed and run by Difi. Only for public sector services. Security level 3.
- *BankID:* Developed and run by banks. Security level 4.
- *Buypass:* Private eID supplier offering eIDs on security level 3 and 4. The level 4 eID can be used in ID-porten.
- *Commfides*: Private eID supplier offering eIDs on security level 3 and 4. The level 4 eID can be used in ID-porten.

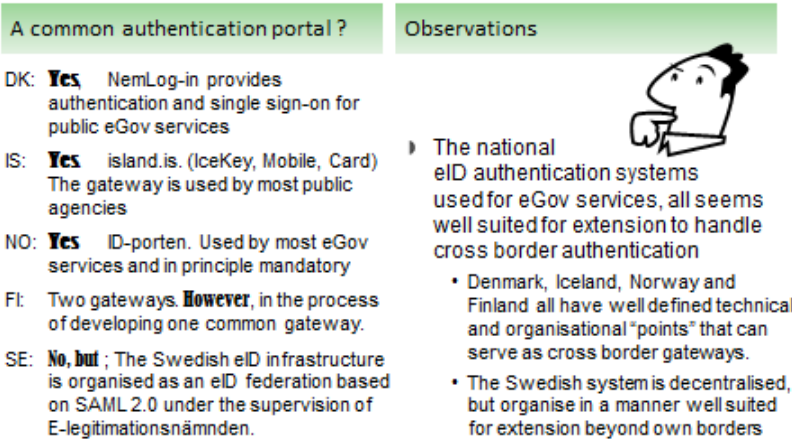
1.2.4 Finland

In Finland there are at the moment there two separate gateways used by eGoverment services (tunnistus.fi and Vetuma). "Vetuma" is the public administration's joint service for citizen electronic authentication and payment. Depending on the online service, a citizen can identify him/herself with bank identifiers and a certificate card or a mobile certificate provided by the telephone operators. Tunnistus.fi is similar to Vetuma but providing service only to its owners which are the Tax Administration, the Ministry of Employment and The Economy.

Finland is currently developing a 2nd generation centralised, common eID portal. The new government operated eID-portal will do a background query for each authentication request, and retrieve up-to-date information from the population register. This data set will be sent to the service provider that requested the authentication (a municipality or a government agency).

Usage of common eID portal is at least for now voluntary.

Figure 3: National solutions for eID Authentication



1.2.5 Sweden

E-identification for citizens is issued by private sector – mainly through banks and a large telecommunication provider. The public sector purchases authentication from the identity providers on a commercial basis.

The current Swedish eID infrastructure is based on PKI and a framework agreement from 2008 with four suppliers (three banks selling BankID and Telia). Each individual contracting agency is responsible for making call offs from the framework agreement and ensuring necessary technical integration of the eID-services into the respective e-service. Authentication and SSO between certain e-services is coordinated on a voluntary basis.

The new Swedish eID infrastructure (Svensk e-legitimation) is organised as an eID federation based on SAML 2.0 under the supervision of the Swedish E-Identification Board, E-legitimationsnämnden. Issuers of eID and service providers are trusted members of this identity federation provided.

SAML 2.0 is a version of the SAML standard that allows for exchange of authentication and authorization data between partners within a trusted security domain. The trusted partners of the federation has access to a SAML metadata system. This system holds updated information on partner, roles and technicalities like URL addresses.

2. eID Assurance policies

2.1 National assurance levels for eID

Identity assurance is a measure for the strength of assurance of an eID credential, it indicates to what degree an eID can be trusted as a digital proxy for a person online.

Survey questions 2.4.1 and 3.3

- What are the eID assurance levels in use nationally today?
- Which assurance levels are typically required for (different) eGov services?
- Are there guidelines for risk evaluation for selection of eID assurance level for a service?

2.1.1 Denmark

The NemID solution has one assurance level and it would probably be mapped to level Substantial in the eIDAS LoA framework. The credentials are OTP (two-factor tokens) and online enrollment is allowed (no physical presence required during enrollment). UniLog-in and WAYF would probably be mapped to level Low.

DK is working on a revised trust framework in order to align the national eID solution with the eIDAS levels of Assurance.

Guidelines for risk evaluation and selection of appropriate eID assurance level is found at http://www.skat.dk/skat.aspx?oId=1779998&vId=0

2.1.2 Finland

Only one level “Strong electronic identification" is defined in the Act on Strong Electronic Identification and Electronic Signatures (617/2009). The definition is as follows:

- Strong electronic identification means the identification of a person and the verification of the authenticity and validity of the identification by an electronic method based on at least two of the following three alternatives:
  1. Password or something similar that the identification device holder knows.
  2. Chip card or something similar that the identification device holder has in his possession.
  3. Fingerprint or some other characteristic identifying the device holder.
- Finland has guidelines for risk evaluation and selection of appropriate eID assurance level. It dates from 2001 and is currently under revision.

2.1.3 Iceland

The Icelandic identification and authentication portal offers a choice of assurance levels. Iceland has adopted ISO/IEC 29115:2013. Iceland’s assurance levels are:

- IceKey=Moderate.
- Multi-factor IceKey=High.
- Electronic certificates=Very high.

Service providers find guidance for risk assessment of their services and suggested assurance levels at Instructions at the national portal island.is. Very few service providers require more than IceKey to access their services.

The Ministry of Finance and Economic Affairs has issued a recommendation to public service providers to always require qualified electronic certificates.

2.1.4 Norway

"Framework for authentication and non-repudiation in electronic communication with and in the public sector" defines four risk levels and corresponding requirements for authentication and non-repudiation mechanisms.

The "framework for authentication and non-repudiation for electronic communication with and within the public sector" provides guidelines for risk evaluation related to authentication. Each service provider is solely responsible for assessing risks and setting the required assurance level. Most government services are at assurance level 2 or 3. A few services require authentication at assurance level 4, notably in the health care sector.

2.1.5 Sweden

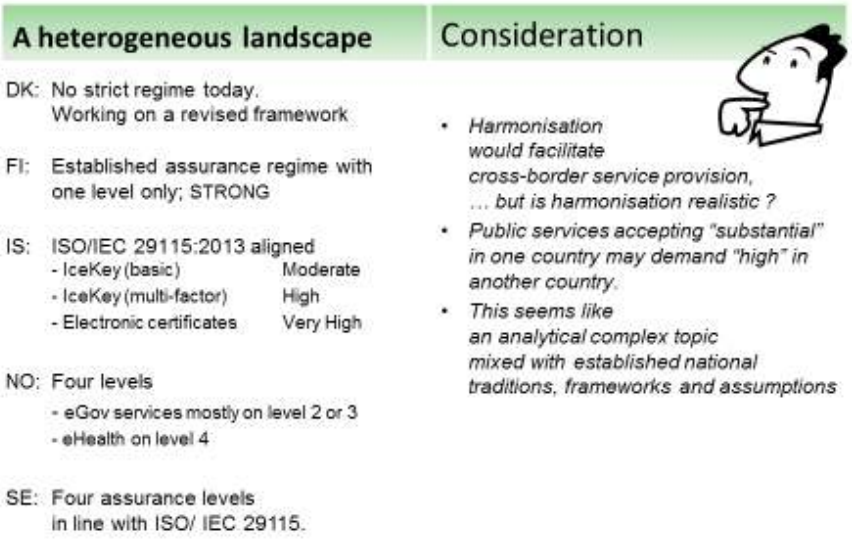
The document "Tillitsramverk för Svensk e-legitimation" defines three assurance levels (LoA 2, 3 and 4) in line with the standard ISO/ IEC 29115 and the eIDAS trust framework. The currently issued eIDs are estimated to be corresponding to LoA 3, or "substantial" according to eIDAS.

Guide for risk assessment is available at https://www.informationssakerhet.se/Global/Metodstöd%20för%20LIS/Riskanalys.pdf. Specific guidelines on choosing the right level of assurance are in development.

The eID assurance discussion comprises two topics:

- What is the assurance level of the eID credential?
- What assurance level will a service provider require in order to provide user access?

Figure 4: National eID assurance levels



The eIDAS regulation defines a European measurement scale with three levels (Low, Substantial, and High). However, the level of assurance demanded for access to specific services varies from sector to sector and from country to country. Public services ranked as having a "substantial" level in one country may be ranked as "high" in another.

3. eID Assurance policies

3.1 National assurance levels for eID

Identity assurance is a measure for the strength of assurance of an eID credential, it indicates to what degree an eID can be trusted as a digital proxy for a person online.

Survey questions 2.4.1 and 3.3

- What are the eID assurance levels in use nationally today?
- Which assurance levels are typically required for (different) eGov services?
- Are there guidelines for risk evaluation for selection of eID assurance level for a service?

3.1.1 Denmark

The NemID solution has one assurance level and it would probably be mapped to level Substantial in the eIDAS LoA framework. The credentials are OTP (two-factor tokens) and online enrollment is allowed (no physical presence required during enrollment). UniLog-in and WAYF would probably be mapped to level Low.

DK is working on a revised trust framework in order to align the national eID solution with the eIDAS levels of Assurance.

Guidelines for risk evaluation and selection of appropriate eID assurance level is found at http://www.skat.dk/skat.aspx?oId=1779998&vId=0

3.1.2 Finland

Only one level “Strong electronic identification" is defined in the Act on Strong Electronic Identification and Electronic Signatures (617/2009). The definition is as follows:

Strong electronic identification means the identification of a person and the verification of the authenticity and validity of the identification by an electronic method based on at least two of the following three alternatives:

1. Password or something similar that the identification device holder knows.
2. Chip card or something similar that the identification device holder has in his possession.
3. Fingerprint or some other characteristic identifying the device holder.

Finland has guidelines for risk evaluation and selection of appropriate eID assurance level. It dates from 2001 and is currently under revision.

3.1.3 Iceland

The Icelandic identification and authentication portal offers a choice of assurance levels. Iceland has adopted ISO/IEC 29115:2013. Iceland’s assurance levels are:

- IceKey=Moderate.
- Multi-factor IceKey=High.
- Electronic certificates=Very high.

Service providers find guidance for risk assessment of their services and suggested assurance levels at Instructions at the national portal island.is. Very few service providers require more than IceKey to access their services.

The Ministry of Finance and Economic Affairs has issued a recommendation to public service providers to always require qualified electronic certificates.

3.1.4 Norway

"Framework for authentication and non-repudiation in electronic communication with and in the public sector" defines four risk levels and corresponding requirements for authentication and non-repudiation mechanisms.

The "framework for authentication and non-repudiation for electronic communication with and within the public sector" provides guidelines for risk evaluation related to authentication. Each service provider is solely responsible for assessing risks and setting the required assurance.

3.2 The eIDAS regulation

The eIDAS regulation is the European Union's new regulation on electronic identification and trust services. Being a regulation, it is an "EU-law" directly applicable in all member states.[1] The regulation enters into force on July 1st 2016, with a deadline for implementation in September 2018. eIDAS aims to solve a range of electronic identity related issues. In addition, a range of trust services are defined, and eIDAS requires these to be legally recognized cross-border (electronic signatures, registered e-delivery services, website authentication and more).

Obligation to "recognise" eID from other countries

The primary target of eIDAS is to facilitate cross-border access to public services. When it enters into force, users can be authenticated for public services using any EU-notified "electronic identification means" equivalent to, or better than, the eID issued nationally.

[1] For EEA countries Iceland and Norway, the regulation will not become a national law directly, but as eIDAS is "EEA relevant", the EEA countries have an obligation to implement eIDAS into national law.

Survey question 2.5.1

- Please indicate timeline and milestones related to the adoption of the eIDAS regime.

3.2.1 Denmark

Denmark plans to have a CEF eID node in production, i.e. up and running in an operational environment by 1st January 2017. Denmark is also running an eID pilot in e-SENS in order to get technical experience necessary for setting up the production eID node to be compliant with the eIDAS regulation.

DK expects to integrate Danish e-services in an iterative process after the national eID node has been set up in an operational environment. We expect the eID node to be able to handle all foreign, notified eIDs via uniform interface and that the biggest burden therefore will not be on the Danish e-Service side.

3.2.2 Finland

Updated national legislation and regulations on the basis of eIDAS planned to be in force 1/7/2016.

3.2.3 Iceland

Registers Iceland has received a 3 year funding from CEF and plans to adopt the identification and authentication portal to the eIDAS regulation within this period.

3.2.4 Norway

Work on incorporation of eIDAS in Norwegian legislation is ongoing.

Norway (Difi, ID-porten) will connect to the STORK (CEF Digital) infrastructure second half 2015. The technical measures for authenticating persons from other European countries will then be in place.

3.2.5 Sweden

A timeline will be established later this year. The new law complementing the eIDAS regulation will enter into force on 1st July, 2016.

Sweden will build an infrastructure through eIDAS nodes and a national proxy service integrated in to the national identity federation that enables Swedish service providers to authenticate users from other countries.

3.3 eIDAS requires national implementation efforts

eIDAS defines a regime with three assurance levels in relation to cross border use of notified eIDs; Low, Substantial, and High. However, the eIDAS regulation is a legal text without references to technical specifications, standards or procedures. This work remains to be done. Nordic alignment is not a requirement, but will facilitate cross-border operations.

The cross border eID acceptance regime of eIDAS, is based on a system where countries apply for "EU notification" of selected national eID schemes. The process comprises three main steps

- Submission; Notifying countries submits the notification support material to the "Cooperation Network".[2]
- Peer review: a review of eID scheme under the monitoring of the other countries. The applying country may at this stage be asked to provide additional information on specific issues.
- Notification: Publication in the Official Journal.

The above procedure will be resource demanding and a Nordic sharing of expertise and knowhow will be beneficial. Notification is not mandatory and it remains to see which Nordic countries will notify. Anyhow, it will probably be of interest to provide experts to the "Cooperation Network" as well as the review team.

[2] Commission Implementing Decision (EU) 2015/296.

4. Cross border connections

4.1 Future trend – Service infrastructures at European level

In 2011 the European Commission adopted a proposal for a Multi-Annual Financial Framework for the period 2014–2020, "The Connecting Europe Facility" (CEF). The section CEF Digital has a total budget of euros 1.14 billion, out of which 970 million euros are dedicated to Digital Service Infrastructures (DSIs). A main objective for this section is to facilitate the cross-border and cross-sector interaction between European public administrations.

4.1.1 CEF eID Building Block

CEF Digital comprises a number of re-usable components known as DSI Building Blocks. Building blocks for eID and eSignature are among the first to be available together with eInvoicing, eDelivery and automated translation.[3]

The eID building block supports cross-border authentication by the interconnection of existing national eID authentication systems. The system architecture for the European DSIs is based on dedicated core service platforms for the individual DSIs and connection gateways at national levels. The core platforms will be implemented and operated by the EU while connection gateways at national level will be implemented and managed locally

[3] https://joinup.ec.europa.eu/community/cef/description

A new agency created in 2014, INEA,[4] is responsible for the financial implementation of CEF Digital and for the technical management of the core service platforms of the DSIs.

The final technical specifications as well as some operational aspects of the DSIs brought forward by CEF Digital are still to be finalised. CEF Digital is implemented via annual Work Programmes prepared in cooperation with the Member States and participating EEA countries. It is a "system under construction". However, it seems clear that the European Commission is determined to roll out a number of digital service infrastructures for cross border eGovernment services in the years to come.

4.1.2 ISA²

ISA² will cover the period 2016–2020 will replace the ISA programme which comes to an end in December 2015. The ISA programme supports the development of tools, services and frameworks in the area of e-Government through more than 40 actions some of which is listed below:

- CPSV-AP – A data model for public services.
- EFIR – The European Federated Interoperability Repository.
- AMDS – The Asset Description Metadata Schema.
- Joinup – A internet platform facilitating the sharing and reuse of IT solutions developed for Public Administrations.

Solutions are with a few exceptions available free of charge to European Public Administrations.

[4] http://ec.europa.eu/inea/en

4.2 The Nordic situation – An ocean of islands?

Survey questions 3.1.5 and 3.3.4

- Does your national eID policy address issues related to acceptance of eIDs from other countries?
- Does the eGovernment policy express ambitions for cross border operation, e.g. making eGov services available to foreigners?

4.2.1 Denmark

The existing eID policy only addresses issues relating to foreign citizens who have a residence permit and hence a Danish central registration number (cpr.nr.). Foreign citizens can based on this get NemID on the same conditions as Danish citizens.

No explicit policy expressed for making eGov services available for foreigners, but Denmark is piloting cross border eGov services through the e-SENS project.

4.2.2 Finland

No explicit policy expressed for making eGov services available for foreigners.

4.2.3 Iceland

No explicit policy expressed for making eGov services available for foreigners, but Iceland has participated in both STORK projects. A PEPS gateway has been established and run under both projects.

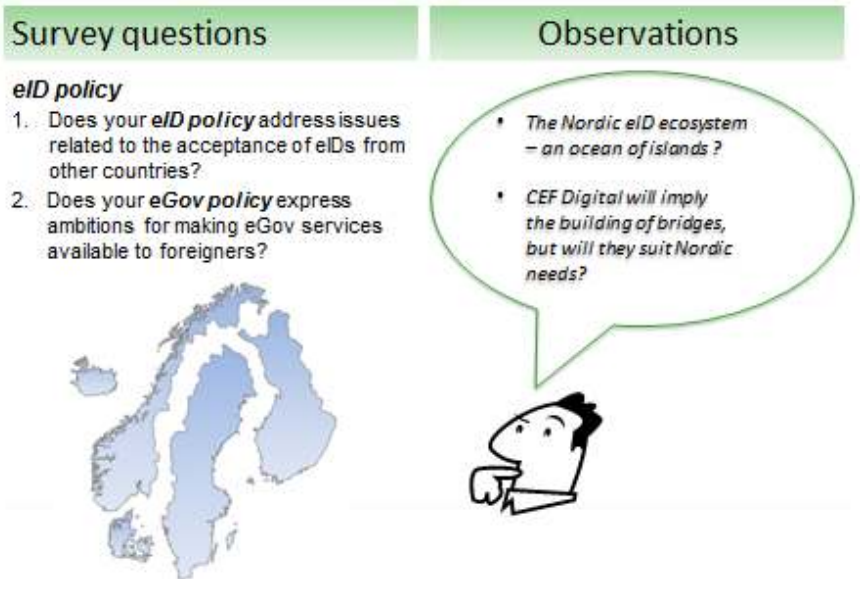
4.2.4 Norway

Work has been carried out in Difi on acceptance of foreign eIDs and a connection to the STORK infrastructure will be in place in the autumn.

4.2.5 Sweden

In the budget bills for 2015 and 2016, the Swedish government states that the routines for electronic identification and signature should be as easy as possible to use, no matter if the user is located in Sweden or in another country. The routines must also ascertain a high level of security. The government also states that the implementation of the eIDAS-regulation is prioritised.

Figure 5: eID interconnection



- During the latest years, SE has established several pilots to test cross-border authentication and electronic signing, mainly under the eSENS project.

4.3 Nordic interconnection via EU?

Survey questions 4.4.1 and 4.4.2

- Please provide information on plans for connecting up to CEF eID Building Block.
- Please inform on engagement in Nordic cross border pilots.

4.3.1 Denmark

Denmark plans to have an CEF eID node in production, i.e. up and running in an operational environment by 31st May 2016. At present DK is running an eID pilot in e-SENS to get technical experience necessary for setting up a production eID node compliant with the eIDAS regulation.

DK participates in the e-SENS pilot with eID in the domains business lifecycle and citizen lifecycle. Adjacent to the e-SENS pilot project, the Nordic Ministers Council has financed a Nordic e-SENS project with focus on:

- Identify and execute Cross Border Pilots.
- Coordinate resources for better efficiency in the e-SENS project.
- Perform workshops in order to identify pilots as well as getting a better.

4.3.2 Finland

No input.

4.3.3 Iceland

Iceland participated in the STORK projects.A PEPS is already operational and Registers Iceland has applied for and received positive response for funding from CEF Telecom for the continued operation of the service.

4.3.4 Norway

The Norwegian eID gateway (ID-porten) will be connected to the CEF eID Core Service Platform in autumn 2015. Difi is a central actor in the e-SENS project, and the Brønnøysund register centre is also involved. The work includes piloting in the public procurement area and for registration of a company in Norway from Sweden and Denmark (and the opposite direction).

4.3.5 Sweden

Sweden takes part in eSENS – Cross Border Company Registration.

5. Providing eGov services for foreigners

5.1 Welcome to the Waiting Room

Figure 6: You are welcome to hang around in our waiting room until you receive your national person identifier

We have identified you as Sture Jansson from Sweden.

To access our eGovernment services you must have a national person identifier (PID):

- *Click here* to apply for a national person identifier (PID).

Please note that the waiting time for a new PID is typically 2–4 weeks.

Survey question 4.3.1

- Access to public services routinely requires a unique national identifier e.g. the civic registration number. If this is the case in your country, please provide information on this topic.

Figure 7: Access to eGov services

5.1.1 Denmark

All Danish services for citizens are based on a unique national identifier, the central person registration number (CPR).

5.1.2 Finland

The civic registration number is most commonly used.

5.1.3 Iceland

The unique national identifier, "kennitala", is fundamental in providing eServices.

5.1.4 Norway

A Norwegian person identifier ("fødselsnummer – birth number") is required for most government services and many services in the private sector; persons that are not citizens or permanent residents of Norway can obtain a "D-nummer" that is compatible in use.

5.1.5 Sweden

The Swedish civic registration number "personnummer" is required for most government services.

6. Enabling foreigners to proceed beyond the "Waiting Room"

6.1 All Nordic citizens have a national personal identifier, but…

All Nordic countries use a system where natural persons are associated with a unique national person identifier – a PID. This identifier is commonly used as access key to eGov services, however, the syntax of this identifier varies much from country to country.

6.1.1 Denmark

Personnummer (DK) – also called CPR – consists of 10 digits. The format of the first six digits is: DDMMYY. Information of the birth century information is embedded in the seventh digit and the last digit carries information about gender.

6.1.2 Finland

Henkilötunnus (FI) consists of 10 characters separated in two groups DDMMYY-XXXX. The first group indicates birthdate using numbers. Then comes the separation character which can be "-" (born in 1900–99) or "A" (born in 2000-). The last 4-characters contain serial number (3 chars)and a checksum. Checksum is a single character that is being calculated using public algorithm and it verifies the integrity of personal identification number. Serial number not only quaranties the uniqueness of personal

identification number but it also contains the gender information. Odd number is for male and even number is for female citizen.

6.1.3 Iceland

Kennitala (IS). The kennitala consists of 10 digits and includes information about birthday and birth century; DDMMYYxxxC.

6.1.4 Norway

Fødselsnummer/D-nummer (NO) comprises 11 digits DDMMYY-XXX-XX. D-numbers are used for non-resident persons and has the same structure as "fødselsnummer", but the date of birth is adjusted to be out of range (DD+40) MMYY-XXX-XX. There is an added rule that the ninth digit also indicates gender (odd = male, even = female).

6.1.5 Sweden

Personnummer/Samordningsnummer (SE). The Swedish number has10 digits separated in two groups (6 + 4 digits). The first group indicates a person's date of birth using the format YYMMDD. The two groups are normally separated by a hyphen (-). However, if the person is more than 100 years old, this is indicated using a plus sign (+) as a separator.

6.2 A dummy PID for foreigners?

The waiting room issue is closely related to the use of national PIDs as access key to public services. An apparent straight forward solution is to assign a national PID to the foreign person. However, national procedures are often lengthy and paper based. This is understandable as the use of a national PID is closely related to legal rights and responsibilities.

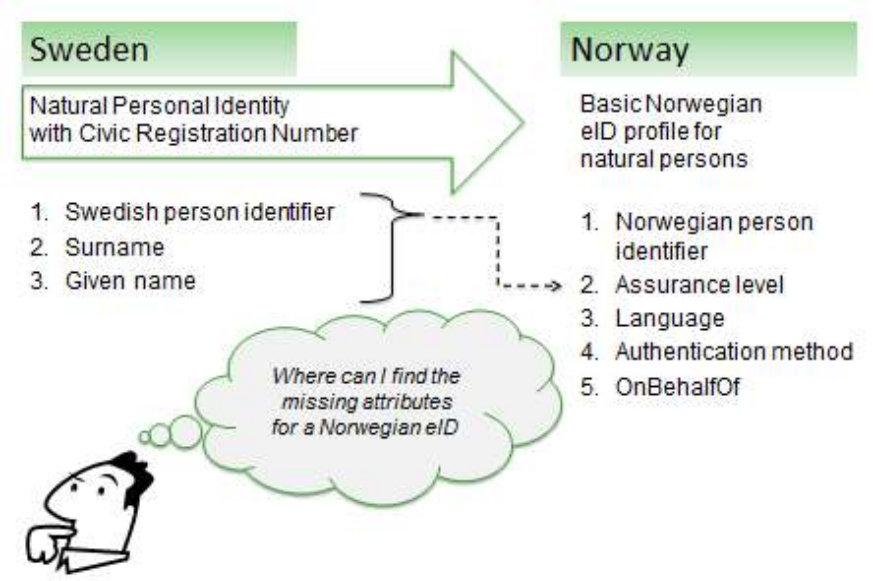
An alternative solution is to assign a dummy PID that fulfils format requirements, but where certain information elements are left undefined. This PID could typically be of temporary nature and have built-in limitations with regard to access rights.

It is technically feasible to create dummy PIDs on the fly. However, a solution needs to take into account certain legal, institutional and information issues:

- The dummy PID must not collide with any existing person identity.
- There are inherent limits to the number of dummies that can be fit into a national PID system.
- The need for a life cycle management of the dummy PIDs is e.g. when the person gets a permanent PID.
- The life cycle management of national PIDs in the situation where persons possesses eID tokens and eIDs from several countries. It will be a challenge to assure that they all refer to the same physical person.

6.3 Nordic eID datasets

Figure 8: Convension from Swedish to Norwegian eID



The format and content of an eID issued in a foreign country will typically be different to that used in the country providing the public service. The picture illustrates the conversion from a Swedish eID to a Norwegian eID. The Swedish eID comprises three attributes; a Swedish person identifier, surname and Given name.

The Norwegian eID comprises five attributes; Norwegian PID, Assurance level, Language, Authentication method and "OnBehalfOf". None of the Norwegian attributes correspond to the attributes of the Swedish eID.

Survey questions 5.1.1 and 5.1.2

- Please provide a description of the core eID dataset for natural persons.
- Is the dataset formally defined or merely a commonly used set of data (a profile)?
- Is the core dataset available as a credential issued by some Authoritative Source?

National laws and regulations determine who may requisition a civic registration number. Use is commonly restricted to government agencies, health care bodies and organisations with specific documented needs. The survey does not have a comprehensive overview of this, but a first mapping indicates that an exchange of this type of information across Nordic borders will meet obstacles.

6.3.1 Denmark

The Danish eID is bound to the Danish natural person certificate (POCES). It contains a country code, PID number,[5] given name, surname, common name/pseudonym, postal address, and e-mail address.

Person certificates are issued by specific certification authorities (CAs) under the supervision of The Danish Agency for Digitalisation.

[5] Personspecifik Identifikationsnummer.

6.3.2 Finland

The Finish eID is based on a core dataset formally described in the document "Finnish formal core dataset.pdf". The document lists more than 30 attributes.

The core dataset is maintained by the Finish Population Register Centre. It is possible to use subsets of the core dataset. Datasets are implemented as SAML2 profile and signed by the Population Register Centre.

6.3.3 Iceland

The core dataset consists of the unique national identifier (kennitala) and the name of the person. The dataset is retrieved from the national registry, operated by Registers Iceland.

Icelandic authentication service (electronic certificate, IceKey), issues this information in a digitally signed SAML 2 profile. The same information is available in passport and drivers licence.

6.3.4 Norway

The mandatory eID authentication portal, ID-porten, issues a SAML assertion as response to authentication requests. Profiles are defined by the Agency for Public Management and eGovernment (Difi). Currently three profiles are in use.

The basic profile comprises five information elements (SAML statements) civic registration number, authentication assurance level, language, authentication method and an "OnBehalfOf" statement.

6.3.5 Sweden

The Attribute Specification for the new Swedish eID Framework issued by E-legitimationsnämnden defines four eID profiles. The profile "Natural Personal Identity with Civic Registration Number" comprises three mandatory information elements; Surname, given name and National civic registration number.

Other profiles are "Natural Personal Identity without Civic Registration Number" and "Pseudonym Identity".

6.4 The eIDAS dataset

The eIDAS regulation specifies a minimum dataset for natural persons that consists of four mandatory and four optional data elements.[6]

Mandatory

- Current family name(s).
- Current first name(s).
- Date of birth.
- A unique identifier constructed in accordance with the technical specifications for the purpose of cross-border identification and which is as persistent as possible over time.

Optional

- First name(s) and family name(s) at birth.
- Place of birth.
- Current address.
- Gender.

[6] Regulation (EU) 2015/1501.

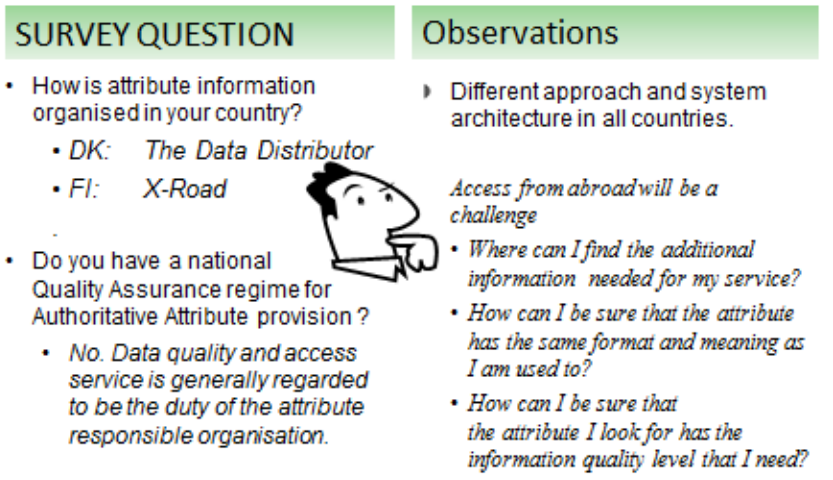
Considerations

- It would be useful to have a Nordic interoperability profile, i.e. a common Nordic understanding of how the above mentioned information elements are interpreted. This would facilitate the exchange of basic information about natural persons.
- When a resident of a Nordic country demands access to an e-government service in another Nordic country, there is a risk that the person is already registered in the country's civic register. This is highly possible if the person is logging into a social benefit service or a health care service. The study has revealed a need to keep trace of the national identities of people across country borders.

7. Providing services for foreigners

The provision of eGovernment services for a person resident in another country will in many cases require access to additional information beyond what is held in a standard eID credential. This brings up the issue of access to authoritative information registers in other countries.

Figure 9: Retrieval of authoritative information



7.1 Organisation of access to authoritative information

Survey question 5.2.1

- Please provide an overview description of national Authoritative Attribute Sources
- Is provision of attributes organised with some sort of common gateway?
- Is there a defined QAA regime for attributes and attribute providers?

7.1.1 Denmark

Central Person Register (CPR) is of national Authoritative Attribute Sources for natural persons and Central Business Register (CVR) for businesses.

In addition, the authorisation register for health professionals at the National Board of Health (Sundhedsstyrelsens autorisationsregister) contains attributes about Danish health professionals amongst others their authorisation to work as health professionals.

Also, the authority service and authorisation administration of NemLog-in can be seen as attribute services (NemLog-in's fuldmagts-tjeneste og brugerrettighedsstyring).

7.1.2 Finland

Dataset for Natural persons is based on Population information system maintained by Population register centre and local register offices.

Core dataset for natural persons is available as SAML2 profile via Finnish Public Sector eIdentification portal and via Soap/xml gateway directly from population information system.

7.1.3 Iceland

National population register and the National property register, run by Registers Iceland. The Company register run by the Directorate of Internal Revenue. The vehicle register run by the Icelandic Transport Authority. A limited health register is run by the Directorate of Health (i.e. vaccinations and prescriptions).

Each person has the right to access information about himself/herself and their properties. Access to the National population register, the National properties register, The Vehicle register and the Vaccination register is provided at "My Pages" at the National Portal "Island.is". Access to certain health information, i.e. prescriptions is available from the health portal "heilsuvera.is".

7.1.4 Norway

Registers are considered as authoritative attribute sources. Norway has a well-developed register infrastructure, although each register must commonly be accessed directly. Some common interfaces exist, notably for different registers provided by the Brønnøysund register centre. Registers typically provide a GUI interface for humans and a web service interface for system integration.

Some registers are available, following open data principles. These can be reached also from abroad. The Norwegian Population Register is subject to access control, and access authorisation may be difficult to obtain from outside of Norway.

7.1.5 Sweden

The population register is where the population of, Sweden is registered. The Swedish Tax Agency is responsible for the population register. You remain registered in Sweden until the day you move abroad or die.

Information regarding the population is distributed to authorities through *Navet* (the Swedish Tax Agency system for distribution of information about the registered population) and *SPAR* (the Swedish

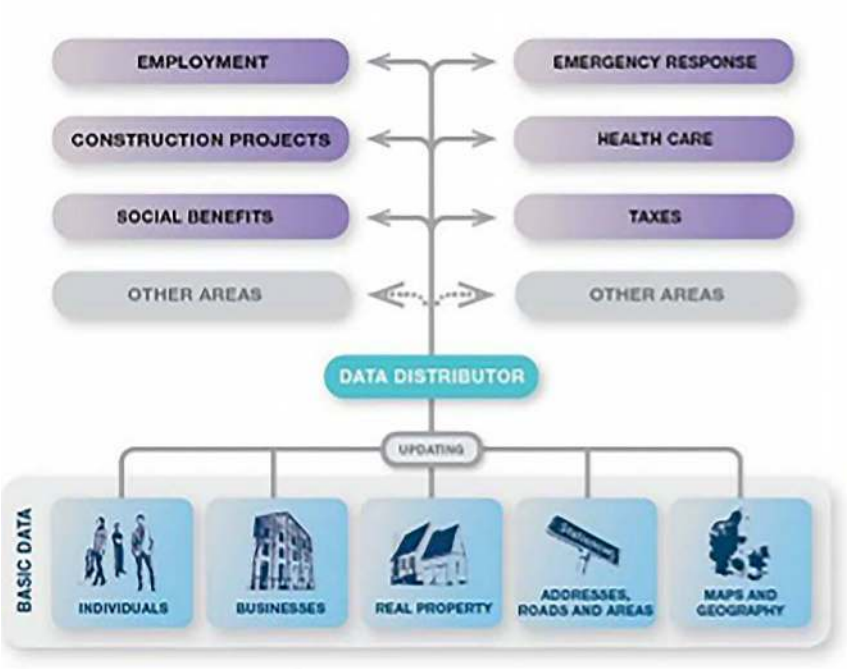
population and address register). Registers are considered as authoritative attribute sources (although that term is not used).

The new Swedish eID identity federation is built to handle distribution of attributes to e-services through the use of different attribute profiles under SAML 2.0, and specific attribute federations have already been established within specific sectors (for instance SAMBI for the eHealth sector).

7.2 Case presentation (DK) – The Data Distributor

Public authorities register various information about individuals, businesses, real estate, buildings and more. In Denmark this is labelled "basic data" and as a general rule, basic data is to be made freely available to all public authorities, private businesses and individuals.

Figure 10: The Data Distributor (DK)



Basic data is regarded to be a common digital resource, which can be exploited freely for commercial as well as non-commercial purposes. To serve this purpose a Common Public-Sector Data Distributor has been established.

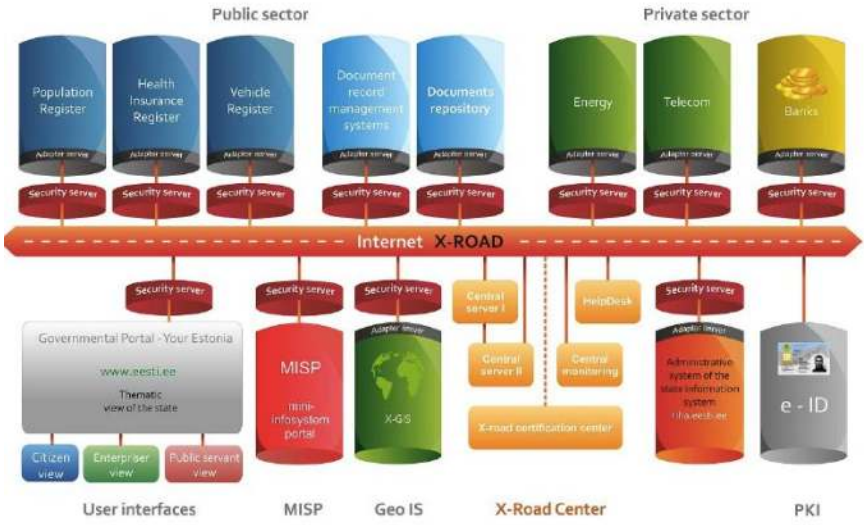
Text taken from GOOD BASIC DATA FOR EVERYONE. (2012) The Danish Government.

7.3 Case presentation (FI) – X-Road

Finland is creating a data exchange layer based on the Estonian X-Road system.

The Government of Finland has decided to create a data exchange layer of e-services and cooperate with Estonia as much as possible.

Figure 11: X-Road (FI)



The X-Road was launched in 2001. The data exchange layer X-Road is a technical and organisational environment, which enables secure Internet-based data exchange between the state's information systems.

The X-Road allows institutions/people to securely exchange data as well as to ensure people's access to the data maintained and processed in state databases.

Public and private sector enterprises and institutions can connect their information systems with the X-Road. This enables them to use X-Road services in their own electronic environment or offer their e-services via the X-Road. Joining the X-Road enables institutions to save resources, since the data exchange layer already exists. This makes data exchange more effective both inside the state institutions as well as for communication between a citizen and the state.

8. eSignature

8.1 Types of signatures – legal definitions and technology

The area of electronic signatures has been a primary focus for legislation and standards development in the EU; in fact the eSignature directive from 1999, and the resulting standardisation mandates given to CEN and ETSI, focus solely on signatures. Only with the introduction of the eIDAS regulation is this expanded to eID (and other trust services). Considerable confusion results from the fact that "signature" is both a legal and a technical term.

In this report, we seek to clarify this by using terms in the following way:

- An "electronic signature" is the legal term for the act of signing, i.e. giving consent to, something. An electronic signature is a replacement for a handwritten signature.
- A "digital signature" is a technical term for a signature created by public key cryptography supported by PKI certificates issued by a recognised certification authority. This technology is currently needed to support "advanced" and "qualified" signatures (see below).

The eIDAS regulation defines several types of signatures, all of them legal terms. Since eIDAS is a legal document, the definitions should be technology neutral as far as possible. Taking technology into consideration, the eIDAS definitions are to be understood as follows:

- An "electronic signature" can be created by any technical mechanism that creates a link between the data/information/document that is signed, and the act of the user. Notably, a "click to consent" user interface where an authenticated

user explicitly confirms his/her intention by clicking a button on a web page can be used, preferably in combination with creation of a sufficiently strong audit log record of the event. Some say that even a plaintext "signature" at the bottom of an email constitutes an electronic signature.

- An "advanced electronic signature" (AdES) is in reality not a technology neutral term but requires a "digital signature" and use of PKI technology. A "basic" AdES has no quality requirements, e.g. no requirement on the quality of the PKI certificate used.
- An "advanced electronic signature with qualified certificate" ($AdES_{QC}$) adds the requirement for use of a qualified certificate, i.e. a certificate issued by a certification authority that is nationally supervised and present in the Trusted List system of the EU.
- A "qualified electronic signature" (QES) additionally requires use of a "qualified signature creation device" (QSCD) holding the signer's private signing key. A QSCD can be based on various technologies; although a smart card was initially foreseen, server-based solutions are increasingly being used.

Replacing handwritten signatures, concepts and misconceptions

Since the eSignature directive in 1999, an established principle in the EU is that whenever an electronic process is used, a QES shall be accepted as the equivalent of a handwritten signature. This ensures that there always exists a valid signature option that can be used in the transition from paper based to digital processes.

Unfortunately, many EU Member States have stated that QES is the only mechanism that can replace a handwritten signature. This has blocked the development of alternative more user friendly approaches that would be sufficiently secure. While a handwritten signature is the only mechanism for proving consent on paper, there are several alternatives when it comes to digital consent. The choice should be guided by a convenience and risk analysis.

This "QES only" approach is contrary to the intention of eIDAS and the eSignature directive, which explicitly state that QES is a maximum level. There is no hindrance in eIDAS to accept other forms of electronic

signatures, as long as the mechanism(s) used fulfil the purpose of a signature in the process. One may argue that AdES/AdES$_{QC}$/QES should only be used when:

- There is a legal justification for the use of a specific mechanism.
- A risk analysis has documented its need.

8.2 The Nordic eSignature situation

Survey questions 2.2.2 and 3.2.1

- To what extent do laws and regulations specify the use of advanced and/or qualified e-signatures?
- Is there a preference for government issued certificates for signatures towards e-government services?

8.2.1 Denmark

OCES[7] digital signatures are advanced electronic signatures under the notion of the eSignature directive. There are currently no requirements to use qualified signatures in Danish regulation.

Only OCES certificates that are issued by the government can be used towards e-government services.

8.2.2 Finland

Specification for qualified e-signatures is similar to in the text of the eSignature directive 1999/93/EC (Article 5.)

No legal preference for government issued certificates, but in practise only the government is at the moment issuing qualified certificates.

[7] Offentlige Certifikater til Elektroniske Services (Public Certificates for Electronic Services).

8.2.3 Iceland

The laws state that a qualified e-signature is equal to a handwritten signature.

There is no preference for government issues certificates. Auðkenni is in practice the only issuer of electronic certificates in Iceland. However, both public and private companies/agencies can apply for an intermediate certificate and start issuing eID cards under the Icelandic Root. Almost all e-government transactions rely on "simple" electronic signatures: Authenticate, fill in form or upload document and "sign" by clicking "a submit button.

8.2.4 Norway

In most cases, the interpretation in Norway is that an "electronic signature" in its simplest form is sufficient. Almost all e-government transactions rely on "simple" electronic signatures to authenticate, fill out forms or upload documents and sign by clicking a submit button.

There are no legal requirements for AdES, although, some requirements are posed by guideline type documents extending to $AdES_{QC}$. However, there is no requirement for a "qualified signature".

In Norway, the policy has been to avoid the use of advanced signatures. Signing has been so far supported by market actors: BankID, Buypass and Commfides. The functionality of ID-porten has in 2015 been extended with a common component for signing and validation.

8.2.5 Sweden

The general legal system does not specify the use of qualified e-signatures, but to some extent government specific laws specify requirement on advanced e-signatures or e- signatures in general, and a few old government specific laws still specifies signatures on paper.

Swedish eSignatures created by the new signature service, can be supported by qualified certificates and qualified signature creation devices (The central signing service will be classified as a QSCD).

Certificates for both the current and the new system are typically issued by the private market.

Figure 12: Signature usage in the Nordic countries

	eID based signing	AdES	AdES$_{qc}$	QES
Denmark	Yes	Some use	No	No
Finland	Yes	No	Some use in health etc.	No?
Iceland	Yes	No	No	Some use
Norway	Yes	Some use for eSeal	Required in a few cases	No
Sweden	Yes (at least allowed)	Yes (via signing serv.)	No?	Yes (via signing serv.)

The survey has revealed that most e-government services (and other services) in the Nordic countries are based on the authentication of the user's identity only, as a basis for "simple" electronic signatures. This is different from European countries with a tradition for Notary and Registrar confirmed documents.

Sweden is the only Nordic country where government agencies frequently choose to require advanced electronic signatures to be used. To fulfil this and still offer the user friendliness of a "click to consent" signature, a central signing service has been developed.

8.3 Case study (NO): Altinn electronic signatures

Altinn is a core component of the Norwegian e-government infrastructure. Originally a portal serving as a single access point for businesses to government reporting, Altinn has evolved into a platform

that public agencies can use to offer services to both businesses and citizens. Reports normally need to be "signed", to confirm the consent and commitment of the actor (business or citizen) filing the report.

Forms requiring only one signature

If a form requires only one signature, it is signed and submitted in one operation when you click on the Sign and submit button. The form will be saved under Archived in My message box and submitted to the appropriate public agency.

Forms requiring more than one signature

Some forms must be signed by two persons. For example, some forms will also need to be signed by the auditor. If you have the right required to sign for the first step, the form will be transferred through Altinn to the person who has the right to sign for the second step. The form will be submitted automatically when it has been duly signed.

Although Altinn has a solution for $AdES_{QC}$, signing is almost exclusively done by a click to consent mechanism – see the text box for Altinn's explanation. In this respect, Altinn serves as a common electronic signature solution for the Norwegian government for "simple" electronic signatures.

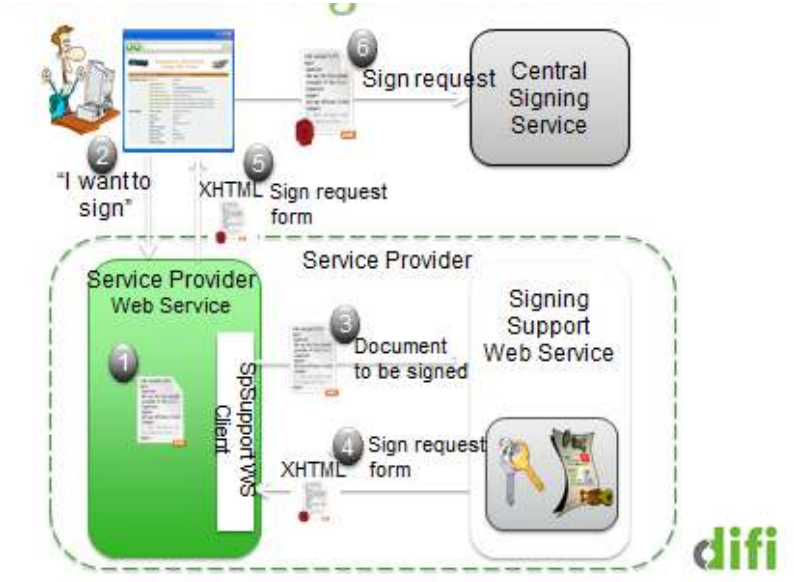
Altinn operates a "third party archive" comprising hash values of the "signed" documents,information about the authentication and authorisations of the person(s) signing, and a time stamp. This information, together with the document content stored in the Altinn archives belonging respectively to the user and the public agency, can be used as proof that the electronic signing took place and that the contents of the actors' archives are unaltered.

8.4 Case Study (SE): The Swedish eSignature solution

Sweden is the only Nordic country where government agencies frequently choose to require AdESs. To fulfil this requirement and still offer the user friendliness of a "click to consent" signature, Sweden implements a central signing service that is integrated into the infrastructure as a service requiring authentication only; the user does not need a separate signing certificate.

As shown in the figure, when the user decides to sign, a signing request containing a hash value (and not the entire document) is created, and the authenticated user is redirected to the signing service with the signing request. The signing service creates a one-time key pair and certificate and upon a "click to consent" by the user signs the request to form a sign response. The response is returned to the service provider, where the signing support service combines the response with the document to form an AdES-signature.

Figure 13: The Swedish eSignature solution



The content of the one-time signing certificate is based on the user's authenticated identity, and the quality of the certificate matches the assurance level of the authentication mechanism. If the user's original authentication is too weak, the user must re-authenticate using a stronger mechanism. When the CA (Certification Authority) for the signing service fulfils requirements for qualified certificates and is supervised, and the user authentication is sufficiently strong, and the crypto hardware of the signing service has the proper product certifications, then even a QES can be produced.

The authenticated user may be a foreigner that is authenticated through the STORK (CEF Digital) infrastructure. Thus, the foreigner will need an authentication eID only, and the signature produced will be "Swedish" in that the Certification Authority is Swedish. The need for cross-border AdES signatures disappears.

9. Recommendations

A primary objective for this project has been to encourage Nordic discussions on eID related similarities and difference. A foundation was created collecting information organised around specific eID related themes. This information constitutes the main body of the chapters 1–8. Input data is displayed on a per country basis and completed with analytic observations and considerations. This has been further compiled into the "Issues and considerations" in the executive summary.

The project was also asked to develop proposals for near term actions and joint Nordic projects, particularly in relation to the eIDAS Regulation and the CEF Digital initiative.[8] The latter is a major EU funding instrument to facilitate cross-border interaction between public administrations, businesses and citizens, by the development of cross border digital service infrastructures at European level.

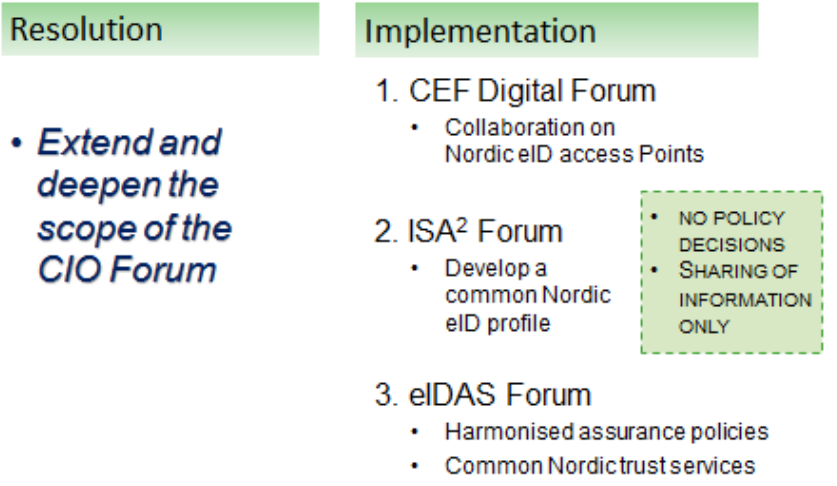
Recommendations and project proposals were discussed at the reference group workshop in Copenhagen in September 2015. The discussions have been summed up in three sections:

- Recommendations for the Nordic CIO Forum (9.1).
- Proposals for projects and studies (9.2).
- Recommendations for support actions at the Nordic Council of Minsters (9.3).

[8] Connecting Europe Facility: http://ec.europa.eu/inea/en/connecting-europe-facility

9.1 Recommendations for the Nordic CIO Forum

Figure 14: Recommendation (1)



The eID issues and challenges highlighted in chapter 1.3 are in general shared by all Nordic countries. This implies that coordinated actions would be beneficial. Not so that the solutions would be the same in all countries, but on a general basis the mutual exchange of information and concerted actions towards the EU would be beneficial.

A main recommendation is therefore to initiate a broadening and deepening of the work of the CIO Forum.

9.1.1 A Nordic collaboration forum for CEF Digital

Proposal: A Nordic CEF Digital Collaboration Forum

- A forum for exchange of information among persons responsible for architectural issues and operational services.
- The group will not take formal policy decisions, but be a forum for mutual exchange of information.

CEF Digital is a possible source of funding from the EU for digital interconnection among Nordic countries. CEF Digital is very broad in its scope and covers a number of digital infrastructure areas, for example eID, eDelivery, Open Public Data and eInvoicing.

CEF Digital supports European cross border infrastructure development with a mix of grants and financial incentives. The "building blocks" developed under CEF Digital have evolved as result of discussions between the European Commission and programme participants. There is much to gain by Nordic collaboration and the alignment of initiatives.

The CEF Digital DSI Building Blocks are technical and operational in nature. The technical system architecture comprises a Core Service Platform and national connection point. The operational responsibility for national access points and related services call for many considerations of a highly specialised nature.

The governance structure for the CEF Digital building blocks is complex and resource demanding. An Architecture Management Board has recently been introduced in addition to the already defined, CEF Expert group and DSI Expert groups.

9.1.2 Nordic ISA² interest forum

Proposal: A Nordic ISA² forum

- A Nordic ISA² study group for the exchange of information on initiatives for, and positions on, the exchange of authoritative information among the Nordic countries. The group would arrange workshops and thematic meetings.
- The ISA² forum should preferably have a kernel that can prepare material for workshops and thematic meetings. The Nordic CIO Forum could serve as reference group.

The survey documented that the data content of the different Nordic eIDs differs much. It would be convenient if there existed a Nordic "standard" that could be used for the exchange of eID data among the Nordic countries. This could be a de facto profile with reference to international standards or metadata at European level.

The cross border provision of public services calls for cooperation not only at a technical and organisational level, but also at a semantic level. The ISA² programme will address these issues at a general and European level. A Nordic "group of likeminded" participants that address issues with a common interest will be beneficial to individual countries as well as to the Nordic community as a whole.

The ISA programme has been EU's instrument for sharing specifications, standards and solutions for cross-border interoperability among European countries. The follow up programme ISA² scheduled for the period 2016–2020, will continue this practice.

ISA² would be a well suited place for Nordic cooperation, the exchange of opinions and possibly Nordic alignment of positions on the aforementioned issues.

9.1.3 eIDAS implementation forum

Proposal: An eIDAS implementation forum

- The thematic group should have a core team to prepare material for workshops and a broader reference group with representatives from all Nordic countries.
- The thematic group should address and document benefits related to Nordic harmonisation where relevant, e.g.
  - Notification of a national eID.
  - Implementation of eIDAS trust services.

The eIDAS regulation implies changes to eID assurance policies in all Nordic countries. The regulation text is deliberately free of references to technical standards or procedures. This leaves much choice – and much work – for the different countries. There is reason to assume that countries can economise their efforts through knowledge sharing and networking with the other countries.

There may not be a consensus among the Nordic countries on all the eIDAS issues. Nevertheless, it will be advantageous for the CIO Forum and countries to establish an arena where eIDAS issues can be addressed as they arise.

There may not be a consensus among the Nordic countries on all the eIDAS issues. Nevertheless, it will be advantageous for the CIO Forum and countries to establish an arena where eIDAS issues can be addressed as they arise.

9.2 Project proposals

One aspect seems particularly important in order to assure high quality projects; projects should be relevant not only on Nordic level, but also for specific countries.

The below proposals are closely related to issues identified during the project and considered to be beneficial to specific countries as well as for the Nordic cooperation more generally. However, the Nordic CIO Forum in invited to take on the role as an active project initiator at Nordic level supplementing the list of proposals and prioritise projects for funding.

The project proposals are presented as a combination of a draft "call for project proposals" (the gray boxes) and supporting explanatory text.

Figure 15: Recommendation (2)

9.2.1 Systems for the provision of a dummy PID

All Nordic countries have a "Waiting Room" issue, i.e. public services are in general dependant on a PID with a specific format. The format varies from country to country, but an inherent problem is that the PID is not only a reference number, but a carrier of information about person attributes, e.g. gender.

A possible solution in order to bring the person "beyond the waiting room", is the creation of dummy PID numbers that fulfils the format requirements and is not already in use by another person. The solution is used by the Norwegian health sector to provide acute health care to unidentified persons. A special online service provides a "FH-nummer" in milliseconds. The PIN is a unique Norwegian reference without information about gender or birthdate. The Norwegian solution allows for generation of some 160 million Norwegian dummy PIDs.

Call for project proposal (DRAFT)

Provision of dummy PID

This expected outcome of this project should be the demonstration and proof of concept of a real time service for national PIDs:

- The start point should be an authenticate eID credential from another Nordic country.
- The project should highlight legal and organisational barriers to its implementation.
- The project should have public agencies from at least two Nordic countries participating as active project partners.

9.2.2 Feasibility study of Swedish eSignature solution

The eIDAS regulation defines several types of electronic signatures – all in principle technology neutral. However, "advanced electronic signature" (AdES) requires the use of PKI technology, "advanced electronic signature with qualified certificate" ($AdES_{QC}$) adds the requirement for use of a qualified certificate and a "qualified electronic signature" (QES) requires the use of a "qualified signature creation device" (QSCD) holding the signer's private signing key.

Our study has shown that Nordic countries makes limited use of advanced electronic signatures (AdES). Sweden seems to be the only country where government agencies frequently require advanced digital electronic signatures (AdES). To fulfil this demand and still offer users the friendliness of a "click to consent" signature, Sweden has developed a central signing service.

This project will investigate whether the Swedish approach can be adopted by other Nordic countries. This will require an investigation of legal framework and possible "red tape" barriers. It will also be necessary to develop and test out technical adaptions required for the solution to work in other countries.

Call for project proposal (DRAFT)

Advanced eSignatures by "click to consent"

The Swedish signing service is a signing service in line with the eIDAS regulation:

- The project should perform an investigation of legal framework and possible "red tape" barriers in countries interested in "the Swedish signing service".
- The project should perform technical proof of concept investigations adapted to the technical infrastructure of the relevant countries.

9.2.3 Survey of Nordic attribute provision systems

Retrieval of information about a person – a physical person or an organisation – from abroad is a challenging task. Survey data from the Nordic countries raise some difficult considerations about the complexity of the issue:

- *Different system architectures and different technological approaches.*
  Denmark has a central core – a common distribution solution.
  Norway has a distributed architecture where service providers have to connect to the relevant information registers
- *Different national policy regimes.*
  In Denmark, basic data is feely available to all public authorities, private business and individuals. In other countries, public institutions charge users for the access to information. In Iceland, citizens own their own personal data. In Norway, personal data registered in the population register is owned by that institution.

Call for project proposal (DRAFT)

Survey of Nordic attribute provision systems

The expected outcome of this study is:

- A survey and comparative mapping of systems currently existing and planned for attribute provision in the Nordic countries.
- The survey should not be limited to technical issues but also investigate and highlight issues related to legal framework, policy and organisational issues.
- The study should line out a possible roadmap for the cross border access to authoritative attributes in the Nordic context.

9.2.4 Analysis of needs and business aspects for Nordic cross-border eGovernment services

There is a long tradition for Nordic cooperation when citizens cross the national physical borders for living or working in another country. Social security agreements and treaties on the cooperation between population registers are well established. Tax authorities of Denmark, Iceland, Norway, Finland and Sweden are operating the portal "Nordisk eTax" in collaboration with the Council of Ministers.

In the internet age, when people cross borders and work in other countries without relocating physically, "cross border public services provision" implies the existence of new issues and a need for new and different approaches. These citizens also expect public services to be available with instant response and without payment for use.

This study should investigate needs and the demand for cross border access to public services in the Nordic countries. It should investigate in depth a limited number of services based on need analysis among a relevant selection of Nordic citizens. It should investigate and highlight issues related to the financing and payment of some designated cross border services.

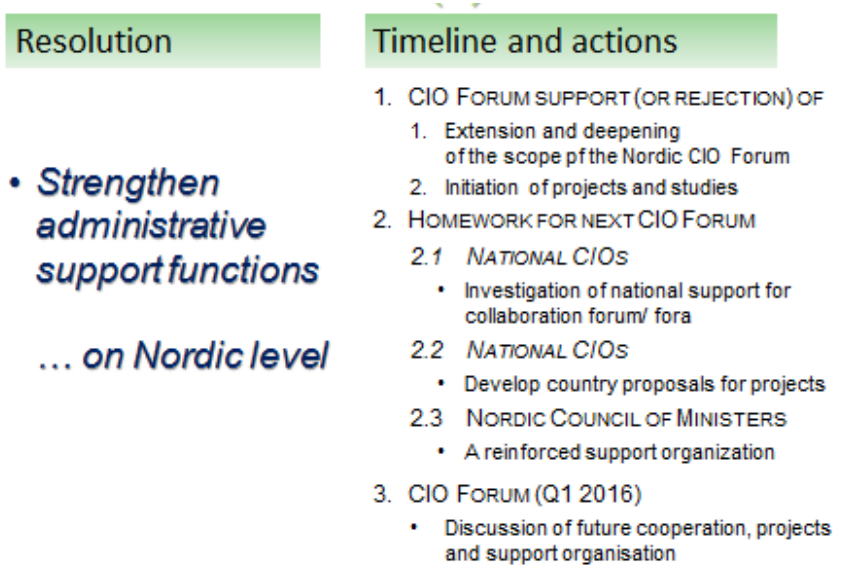
Call for project proposal (DRAFT)

Analysis of needs and business aspects for Nordic cross-border eGovernment services:

- Financial support will take the form of a procurement covering project cost at 100%.
- The project length is limited to one year.

9.3 Proposal for support actions

Figure 16: Recommendation (3)



Administrative and financial management of a portfolio of Nordic projects is a task that calls for a secretariat support functions at Nordic level. The task comprises support to the initiation of new projects as well as the selection process.

The initiation and selection of new projects falls logically under the charge of the Nordic CIO Forum. However, the Forum would need secretarial support for the preparation of project candidates as well as the administrative and financial supervision of the funded projects.

Open calls for project proposals with possibly private organisations as project executers, will most probably imply a step up of administrative and financial administration compared to current practice. For this reason it may be advantageous to investigate if project execution should be limited to public institutions with with routines and tradition for project administration. E.g. national ICT laboratories similar to e.g. eGovlab[9] or executive public agencies like Difi.[10]

9.4 A possible timeline?

The recommendations of chapter 9 was presented to the Nordic CIO Forum in November 2015 with a proposed time line as follows:

- November 2015:
  - Presentation and discussion of recommendations.
  - Nordic CIO Forum.
- Q1 2016:
  - Investigation of national support for extension and deepening of the CIO Forum.
  - Investigation of national support for Nordic projects and studies Investigation of possibly for reinforced support organisation at NCM level.
- Next CIO Forum:
  Discussion of future cooperation, projects and support organisation.

[9] eGovlab; an eGov centre within Stockholm University. http://www.egovlab.eu/

[10] Norwegian Agency for Public Management and eGovernment. https://www.difi.no/om-difi/about-difi

Sammendrag (norsk)

EUs forordning om elektronisk identifikasjon (eID) og tjenester til bruk ved elektroniske transaksjoner[11] slår fast at landene skal akseptere eID-er utstedt i andre EU-land på linje med dem man selv utsteder. Forordningen har som siktemål å understøtte fri flyt av tjenester – også offentlige tjenester – over nasjonale landegrenser. Forordninger er EU-lov og gjelder i alle medlemsland på lik linje med deres egne lover. Forordningen som gjerne omtales som eIDAS, er EØS relevant og gjelder for Norge og Island på lik linje med medlemslandene i EU.

I prosjektet "Nordic eID Survey" er det gjort en kartlegging av de eID løsninger som benyttes i Danmark, Island, Finland, Norge og Sverige. Prosjektet har hatt som siktemål å kartlegge eID-relaterte forhold av særlig betydning for digital offentlige tjenesteyting på tvers av landegrensene. Det er samlet inn underlagsdata innenfor fire delområder:

- Lovmessig rammeverk og policy.
- De nasjonale eID-løsningene.
- Informasjonsinnhold og tilgang til personrelatert informasjon.
- Tilgangsbegrensninger i forhold til nettbasert offentlige tjenester.

De nordiske landene har etablert ulike løsninger for digital identifisering av landets innbyggere. To nærliggende spørsmål dukker opp:

- Er de nasjonale løsningene tilgjengelige også fra andre nordiske land?

---

[11] Regulation (EU) No 910/2014 of 23rd July 2014 on electronic identification and trust services for electronic transactions in the internal market. European Union.

- Har de nasjonale løsningene fellestrekk som peker mot synergier og mulig samarbeid?

Basert på data samlet inn våren 2015 legges det fram fakta og betraktninger som i sin tur danner grunnlag for anbefalinger om nordisk samarbeid:

- Nasjonale eID infrastrukturer er godt organisert ut fra nasjonale behov.
- Nordiske sammenkoplinger på eID nivå er fraværende.
- Den nye EU-forordningen (eIDAS) er svært overordnet. Den vil ikke i seg selv tvinge fram nordisk harmonisering.
- En autentisert utenlandsk identitet er bare et første steg mot digital offentlig tjenesteyting over landegrensene. For de fleste offentlige tjenester må brukeren i tillegg tildeles en lokal nasjonal identifikator. De nordiske landene har et "venteromsproblem".
- Nasjonale forskjeller i juridisk rammeverk og valg av teknologi, gjør det vanskelig å hente inn og sette sammen informasjon fra offentlige kilder i flere land til ett helhetsbilde.
- Det mangler fellesnordiske avtaler om bruk av standarder.
- De nordiske landene bruker i (overraskende) liten grad kvalifiserte sertifikater ved eSignatur for offentlige tjenester.

Rapporten munner ut i tre anbefalinger:

- "Nordic CIO Forum" bør videreutvikles og ta ansvar for samarbeidsfora og prosjekter av fellesnordisk interesse.
- Nordisk teknologisamarbeid bør videreutvikles gjennom prosjekter og studier forankret i et flertall av landene. En første liste over prosjektforslag presenteres.
- Støtteapparatet for prosjektsamarbeid på nordisk nivå bør videreutvikles og styrkes. Nordiske fellesprosjekter forutsetter administrativ støtte og de trenger "steder å være", det vil si steder hvor man kan samle prosjektteam og teste ut tekniske løsninger.

Nordisk ministerråd er prosjektets initiativtaker. Arbeidet er utført av et prosjektteam etablert hos Difi, som er det norske direktoratet for forvaltning og IKT. Prosjektet har mottatt faglig støtte og hjelp til datainnsamling fra en referanse-/ressursgruppe med deltakere fra alle de nordiske landene. I tillegg har fageksperter vært invitert inn for å belyse utvalgte problemstillinger.

Appendix

Project participants

The project team

- Kjell Hansteen (Hansteen Consulting AS).
- Jon Ølnes (Unibridge AS).
- Tor Alvik (Difi – Direktoratet for forvaltning og IKT).

The project team was supported by a reference group with members from the participating countries.

Table 1: Reference group

Country	Name		Working place	
DK	Anni	Buhr	Digitaliseringsstyrelsen	
FI	Kimmo	Mäkinen	Ministry of Finance	
FI	Olli-Pekka	Rissanen	Ministry of Finance	
IS	Halla Björg	Baldursdóttir	Registers Iceland	
IS	Bragi-Leifur	Hauksson	Registers Iceland	
NO	Mette	Bredengen	Kommunal- og moderniseringdep.	
NO	Live	Heltberg	Kommunal- og moderniseringdep.	
SE	Per	Granstrand	Bolagsverket	
SE	Anneli	Hagdahl	Näringsdepartementet	
SE	Magnus	Lundsten	Tilväxtverket	
SE	Eva	Sartorius	eLegitimasjonsnämnden	First meeting
SE	Nils	Fjelkegård	Näringsdepartementet; Sverige	Last meeting

Invited speakers

- Stefan Santesson (3xA Security).
- Nathan Ducastel (PBLQ, Dutch Institute for Public Administration).

Terms and definitions

- *Assurance level*
  A measure for the strength of assurance of an eID credential or an attribute.
- *Attribute*
  Information that specifies a characteristic of an entity.
- *Attribute provider*
  An entity that can provide and assert attribute values in line with the policies set by the scheme it is used within.
- *Authentication*
  The act of confirming the truth of a claim, e.g. that the identification of a person by an eID is correct, or that the value assigned to an identity *attribute* is correct.
- *Authentication portal*
  A service provider that carries out *authentication* on behalf of other service providers and issues *credentials* that can be verified by these service providers.
- *Authoritative source*
  A recognised source of information; [in our context] a recognised register or database of attributes.
- *Core dataset*
  A set of identity attributes, providing identification of a *person* and encompassing information designated as essential/mandatory in a given context.
- *Credential*
  An information entity asserting a certain stated facts, e.g. a PKI certificate or a SAML assertion issued by a relevant authority third party.
- *Civic Registration Number*
  Unique identifier assigned to natural persons. See also PID.
- *Claim*
  A statement made by an entity about itself. A claim may be a statement about identity or attributes.

- *eID*
  Electronic Identity; a collection of Identity Attributes in the form of a credential.
- *Electronic signature*
  Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign [eIDAS regulation article 3.10] See also chapter on eSignature.
- *Identification*
  A claim set forth about the unique electronic identity (within a given domain/context) of a natural or legal person. The claim may consist of one identifier or a set of attributes that together provide unique identification.
- *Identity assurance*
  The ability for a party to determine, with some level of certainty, that an *electronic* credential representing an entity (human or a machine) with which it interacts to effect a transaction, can be trusted to actually belong to the entity.
- *Identity Provider (IDP)*
  [in this context] a trusted service provider that creates, maintains and manages identity information.
- *Person*
  - *Natural person:*
    A human being, as opposed to a legal person.
  - *Physical person:*
    See natural person.
  - *Legal Person:*
    An organisation. A private or public entity that can be uniquely identified.
- *PID*
  All Nordic citizens have a national PID – a national identifier that labels the person uniquely within the population of the country.

- *Single Sign-On*
  The property to authenticating a person's eID once for access to several online services within an identity federation.
- *Token*
  Any hardware, software or combination that holds credentials or information attesting and underpinning the integrity of claimed identity or attributes.

TemaNord 2016:508

Nordic Council of Ministers

Ved Stranden 18
DK-1061 Copenhagen K
www.norden.org

Nordic digital identification (eID)

This publication presents the survey results and policy recommendations of a Nordic study of national eID-systems. The countries that have been studied are Denmark, Finland, Iceland, Norway and Sweden. The aim of the study is to facilitate and lay a foundation for discussions about the similarities and differences in legal, organisational, technical and data approaches taken by the different countries.

The survey data has been gathered with the assistance of the members of a project reference group. The data has been analysed and structured into a number of highlighted issues (chapter 1). The highlighted issues have been in turn used as baseline for a set of recommendations (chapter 9).

The Nordic Council of Ministers has provided funding and facilitated the staffing of the reference group. The Norwegian Agency for Public Management and e-Government, Difi, has been the project owner and provided project resources.

TemaNord 2016:508
ISBN 978-92-893-4469-2 (PRINT)
ISBN 978-92-893-4470-8 (PDF)
ISBN 978-92-893-4496-8 (EPUB)
ISSN 0908-6692