Supporting Decision Making and Policy Through Large Scale Pilots

Herbert Leitold

A-SIT, Secure Information Technology Center
Graz, Austria

ABSTRACT

Under the European Commission's ICT Policy Support Programme (ICT-PSP) so-called Large Scale Pilots (LSPs) have been launched to advance cross-border interoperability in key policy areas like eID, eHealth, eProcurement, eJustice or the Services Directive. Member States (MS) collaborated to make their existing services interoperable. The first LSPs started in 2008 and impressive results have meanwhile been achieved. Although being technical projects, key hurdles that had to be overcome wasn't technology, but legal and operational issues, understanding the legacy and administrative cultures in the participating states, or governance of results. This paper will focus on those aspects. Taking the LSP STORK as an example, the experience made on decision making in such complex initiatives is discussed. The paper will discuss what activities preceded the piloting, like the ministerial declaration that expressed the political will, how the LSP was set up to implement it, and how it led to policy initiative like the upcoming Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

Keywords: Large Scale Pilots, e-government, Electronic Identity, STORK

INTRODUCTION

With the emergence of the Internet to a mass phenomenon, governments started to bring their services online. First as sole information services in the 1990s, soon transactional services appeared. The eGovernment benchmarks carried out by the European Union (EU) showed as online availability trend, that citizens services grew from less than 20% availability in 2001 to about 80% in 2010, business services grew from about 30% to almost 90% (European Commission, 2010). In this 2010 benchmark report, the top six countries assembled at 100% online-availability of benchmarked services and at a 99-100% sophistication rating. While such availability figures may sound impressive, it is limited to national use, lists services that may be isolated islands that do not need to collaborate, and an Internal Market asks for more: The 2013 follow-up report emphasized that "*Services must be far more integrated across government entities, and indeed across borders.*" (European Commission, 2013). This has not been recognized just recently, the need for providing services for citizens and businesses across borders has e.g. been stated already in 2002 in the eEurope 2005 Action Plan (European Commission, 2002).

The provision of online public services cross-borders is however complex. It by far cannot be seen solely from a technological viewpoint. Legal and operational aspects are to be considered. National systems inherit legacy and administrative culture that may not easily be transposed to other states. In order to advance to interoperable public services, the European Interoperability Framework (EIF) defines Political Context, Legal Interoperability, Organizational Interoperability, Semantic Interoperability, and Technical Interoperability as the levels to take into account (European Commission, 2010):

- Political Context claims that each European public service is the result of direct or indirect action at political level.

- Legal Interoperability refers to each public administration working within its own national legal framework. Incompatibilities can make collaboration complex or even impossible.

- Organizational Interoperability covers business process alignment, organizational relationships, and change management.

- Semantic Interoperability allows to process information in a meaningful way. This can be easy in highly regulated sectors or where de-facto standards exist. It however can be hard in cross-sectorial communities.

- Technical Interoperability finally covers the linking of services and information systems.

Even if each layer above gets well considered, there is no such thing as a success guarantee. This holds in particular true, if complex policy areas get addressed. Piloting in real-world environments is advisable so that barriers can be identified through lessons learned. The European Commission therefore initiated Large-Scale Pilots (LSPs) that are driven by Member States (MS) to develop cross-border services in key policy areas.

This paper discusses how such LSPs can successfully support policies. It takes electronic identity (eID) and a LSP "STORK" on European eID interoperability as an example. This as eID is a sector-independent service and as approaches taken by European MS on eID vary significantly. Thus, the chosen example is well suited to illustrate how piloting can support policy. For eID this LSP's lessons learned showed that lacking legal basis for mutual recognition is the main barrier. This culminated into input to a European Regulation – the eIDAS Regulation (European Commission, 2012). Thus, the LSP can be argued as an initiative that supported policy making.

The remainder of this paper is structured, as follows: First the LSP family is introduced. This to give the reader some insight on what policy areas have been addressed and supported by LSPs. As eID has been picked as an example to illustrate how the LSP process works, issues related to cross-border use of eID are discussed. This includes discussion on what initiatives existed before an LSP on cross-border eID has been launched. This LSP has been STORK – its objectives and main results are discussed in the subsequent section. The process of how decisions have been made in STORK are described and the lessons learned are given from the author's personal perspective. The author has contributed to the STORK LSP, did lead a pilot, as well as had he honor to serve as co-chair of the Member State Council. The Member State Council was the governance body responsible of STORK's strategic orientation. Finally, conclusions are given.

THE LSP FAMILY

The idea of Large Scale Pilots to support European key policy areas has been introduced with the ICT Policy Support Programme (ICT-PSP) which is part of the European Commission's Competitiveness and Innovation Framework Programme (CIP). CIP has been established as a funding programme in 2006 (European Union, 2006). First calls for grants have been launched in 2007. CIP ICT-PSP addressed the themes "ICT for health, ageing well and inclusion", "Innovative government and public services", "ICT for a low carbon economy and smart mobility", and "Open innovation for internet enabled services".

In the two first themes "ICT for health, ageing well and inclusion" and "Innovative government and public services", this paper gives particular attention to so-called "pilot A" LSPs. A pilot A is "*Building on initiatives in Member States or associated countries to ensure the EU-wide interoperability of ICT-based solutions. The large-scale pilot projects fall into this category and embrace at least six Member States, with potential for further extension to all Member States;*" Six such pilot A LSPs have been launched and are briefly sketched in the following sub-sections.

e-CODEX

The objective of e-Justice Communication via Online Data Exchange (e-CODEX, 2010) is to "*improve the cross-border access of citizens and businesses to legal means in Europe as well as to improve the interoperability between legal authorities within the EU.*". The project started in 2010 and will run until 2015. More than 20 European states collaborate. The pilots aimed are:

- Small Claims
- The European procedure for Payment Order (EPO)
- The European Arrest Warrant
- Secure cross-border exchange of sensitive judicial data
- Mutual Recognition of Financial Penalties

epSOS

The aim of European Patients Smart Open Services (epSOS, 2008) is to "*design, build and evaluate a service infrastructure that demonstrates cross-border interoperability between electronic health record systems in Europe*". epSOS started in 2008 and is still running. It gathers twenty-five European states. To demonstrate meeting the objectiveand to test the results, two pilots have been defined: Patient Summary and ePrescription,

PEPPOL

The LSP Pan-European Public Procurement Online (PEPPOL, 2008) did run from 2008 to 2012. The overall objective was to "*enable businesses to communicate electronically with any European government institution in the procurement process, increasing efficiencies and reducing costs.*" Eleven MS participated and piloted by interconnecting existing eProcurement solutions. PEPPOL developed specifications such as a Virtual Company Dossier (VCD) that allows suppliers to submit company information in a common format. Further results have been eCatalogue, eOrders, and eInvoice specifications and an e-signature validation service.

SPOCS

Simple Procedures Online for Cross-border Services (SPOCS, 2009) was driven by sixteen European states and did run from 2009 to 2012. It did facilitate the creation of businesses and providing services cross-borders under the Services Directive (European Union, 2006b). SPOCS did four pilots on professions typically providing cross-border services. The four pilot professions were Travel Agent, Real Estate Agent, Architect, and Master Builder.

STORK / STORK 2.0

The LSP Secure idenTities acrOss boRders linked (STORK, 2008) was operational from 2008 to 2011. It provided a framework on eID federation for natural persons. This is discussed in detail in the remainder of this paper. A follow-up project STORK 2.0 (STORK, 2012) extended on eID for representation, such as a natural person representing a legal person, and extended from e-government to eID in private sector services like Internet banking. STORK and STORK 2.0 gathered both about 20 European states. STORK 2.0 will run until 2015.

eSENS

Given the results of the LSPs mentioned before, twenty European states gathered to the Electronic Simple European Networked Services (eSENS, 2013) LSP that has been launched in 2013. The objective is to build upon the results of other LSPs and to consolidate their results. Building blocks like eID, eSignature, eDelivery, and eDocuments shall get piloted in a way to demonstrate maturity and sector-independent applicability. The piloting areas are Business Creation, eJustice, eHealth, and eProcurement. By advancing to mature sector-independent building blocks, a sustainable infrastructure shall be demonstrated. This shall be a basis for the Connecting Europe Facilities (CEF) meant to provide such an infrastructure on the longer run. (European Union, 2013).

Each of the six LSPs mentioned above was meant to support policy. Among those, STORK is the LSP that has the most sector-independent characteristic, as eID and authentication is generic and needed by many service. This paper thus uses STORK as an example to illustrate how LSPs can support policies and their decisions making.

ELECTRONIC IDENTIFCATION AND ITS CROSS-BORDER ISSUES

Secure authentication is a starting point for Web applications that process sensitive or personal data. States started to issue eID as credentials to provide such secure authentication in the late 1990s. To give a definition what eID and authentication aim at, the draft eIDAS Regulation states (text taken from the Regulation proposal (European Commission, 2012). For the changes on these definition out of the Council and Parliament legislative process, that hasn't been completed at time of writing this paper, see the final Regulation, once published):

- *'electronic identification' means the process of using person identification data in electronic form unambiguously representing a natural or legal person;*
- *'authentication' means an electronic process that allows the validation of the electronic identification of a natural or legal person; or of the origin and integrity of an electronic data;*

In order to highlight the challenge when aiming at interoperability between eID solutions, the following sub-sections give a few examples where national eID systems differ. These differences are shown to highlight why decision making needs a proper process in order to on the one hand not reinvent the wheel, but on the other hand still consider national differences. To structure where such differences exist, the categories EIF (European Commission, 2010) defines as levels of interoperability are used (cf. Introduction of this paper). A comprehensive comparison of national eIDs is beyond scope of this paper. For such comprehensive comparisons, the reader is directed to studies like the IDABC eID Interoperability Study (European Commission, 2009).

Political

Defining the political context as "*each European public service being the result of direct or indirect action at political level*", most eID systems in Europe origin from a political decision to facilitate citizen services online. Where the solutions that emerged however differ, is the level on which such eID means are provided:

- Some states went for a national solution by issuing a mandatory eID card to each citizen. This as a homogeneous single authentication means – often amending an existing ID card by a chip. Examples are the BELPIC card in Belgium or the ID-kaart in Estonia (Estonia later complemented by a mobile eID).
- Some states introduced ID cards on the national level, but also on the regional level. An example is Italy where a national identity card CIE is issued, but some regions also issue a citizen service card CNS.
- A technology-neutral approach has been taken by Austria where citizens can choose from card solutions by both the private sector and the public sector (that includes bank cards, health insurance cards, student cards, profession cards, etc.), but also mobile eID got seamlessly integrated.
- The situation in the Netherlands is different with DigiD: no electronic ID card has been issued, but an authentication portal is provided for username-password authentication, username-password-SMS multifactor authentication, respectively.
- Other states piggybacked on existing authentication solutions by the private sector, like Internet banking systems with BankID in Norway and Sweden.

The political intention has been the same in many MS – providing secure means of authentications. The approaches however differ in various dimensions: in making eID mandatory or a voluntary citizen's choice; in issuing eID by the government or relying on the private sector; in allowing multiple means and technologies or relying on a single token; and given the different technologies and issuance processes applied, in the security levels and the assurance provided.

Legal

Where eID has been state issued, it usually is based on an explicit legal basis. This can be a law solely on eID, like the Law on ID cards and electronic identification means in Germany, or a comprehensive law covering various aspects like the e-government Act in Austria.

Differences in the legal basis exist in particular in the use of personal identifiers. In some states it is allowable to use a single personal identifier like a population register number or a tax identifier across sectors. The identifiers are persistent, i.e. do not change during the citizen’s life. This is for instance the case in Estonia, Italy, Spain, or Sweden. Such unique and persistent identifier then often get included in digital certificates. Other states have persistent identifiers, but do not include them in digital certificates for data protection reasons. That was the case in Finland. In other states a persistent identifier used across sectors is even unconstitutional, like in Germany. Identifiers in the German eID are bound to the physical ID token and change whenever this token get replaced. Moreover, the eIdentifier is cryptographically derived differently for each application so that cross-relating sectors or between applications is not possible. Some states continue to maintain sector-specific identifiers in parallel, such as social insurance numbers, tax numbers, student numbers, etc. Austria combines the approaches, as while a unique persistent identifier exists via the Population Register, these however get cryptographically derived to sector-specific or application-specific identifiers in online authentication.

These differences are major, like a unique identifier used cross-sectors being normal in some states, violating the constitution in others. The differences also root deeply in administrative processes. I.e. when cross-relating sectors is legal, application may relate citizen dossiers by matching the identifiers in the backend. If such identifiers do not exist, this may not be possible and only the citizen may establish the link.

In many states identifiers are also defined nationally, usage across borders is disallowed. A reason is that under the Data Protection Directive (European Union, 1995) article 8.7 defined particular attention for identification numbers by stating that “*Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed*”. Such conditions are often defined nationally, inhibiting its cross-border use.

Organizational

Differences in the business process exist in particular in the issuance process. Some states rely on handing credential physically to the person, others have online processes and validation in the backend processes. Both may reach comparable security mechanisms, but often are hard to compare without knowing the details.

In organizational relationships the main differences exist on who is responsible for and who issues eID. While usually (but not necessarily) a link to government responsibility exists, some states keep issuance under their sole responsibility, such as Germany and Estonia (which still may involve private sector organizations in the process), other states rely on the private sector like bank identification in several Nordic countries. A public-private collaboration exists in other states like Austria, where the government is responsible for the identity base (Population Register), but eID tokens can be issued either by private or public organizations and certificate issuance is in the private sector.

Where government responsibility is given, a difference may also be in the government level involved. It may by the federal level in some states, the regional and local in others, or a combination.

The organizational integration on eID can also differ in the sense that some solutions have the service provider delegate authentication to a third party, like to an Identity Provider (IdP). Other approaches rely on each service provider having the eID tokens integrated into their applications. The difference is technical, but has also legal consequences, as delegating responsibilities gives a shift of liability and data protection responsibilities.

Semantic

The semantic differences are in the personal identifiers and the personal attributes associated with it.

The identifier usually is some alphanumeric value, that easily can be used across applications and cross-borders. As however indicated in the section on legal differences, the identifier may be persistent in some countries, or bound to a physical token or application in others. An application assuming the former, like a citizen always having the same identifier when authenticating, may need processes to cover cases where hat does not hold true.

On attributes the differences can be in the meaning, but also sector specific. To give an example, some sectors or legislations may assume two genders “male/female” as the only value set, other legislations or the health sector may distinguish further like ASTM E1633 having nine and DICOM eleven values (Male, Female, Hermaphrodite, …).

Technical

Technical differences exist in the token types and how these get integrated in service providers.

Token types range from smartcards, mobile ID, software certificates, one-time password (OTP) generators, or username and password. Some states have just one token, others use various types.

Integration into services provider applications usually follows one of two options: The first is that authentication can be delegated by the application to an authentication portal. The portal can be central or it can be a federation with several portals. Such delegations are also referred to as a “proxy model”. An example Netherlands with DigiD authentication. The second option is that the authentication token gets integrated by the service provider. Usually some integration software or middleware is provided. The model is also referred to as a “middleware model”.

EFFORTS ON EID INTEROPERABILITY

The political will to advance to an eID ecosystem that can be used across Europe was expressed in the Manchester Ministerial Declaration (European Union, 2005) as “*By 2010 European citizens and businesses shall be able to benefit from secure means of electronic identification that maximise user convenience while respecting data protection regulations. Such means shall be made available under the responsibility of the Member States but recognised across the EU*”. This was an enabler that started a number of initiatives, but also settled the scene in a sense that no harmonization or EU-wide eID token is aimed, but the responsibility remains with the states; interoperability and recognition of national solutions is the goal.

The Ministerial Declaration was preceded by work in eEurope 2005 subgroups. One of the subgroups was on eID that settled the scene and provided a timeline. It defined a number of actions like defining terminology or a common framework, as illustrated in figure 1.

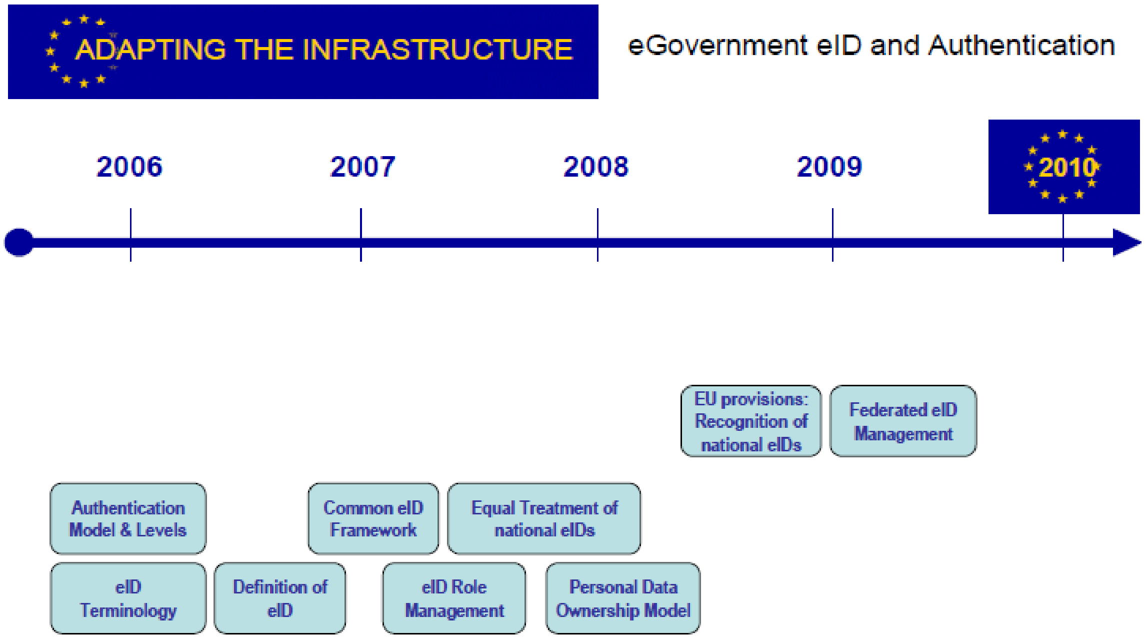
ADAPTING THE INFRASTRUCTURE
eGovernment eID and Authentication
2006
2007
2008
2009
2010
EU provisions: Recognition of national eIDs
Federated eID Management
Authentication Model & Levels
Common eID Framework
Equal Treatment of national eIDs
eID Terminology
Definition of eID
eID Role Management
Personal Data Ownership Model

Figure 1. eID initial timeline (from European Commission, 2005)

While its overall timeline hasn’t been met, the Manchester Declaration lead to several initiatives. To take stocks, studies of the eID landscape have been launched, like (MODINIS-IDM, 2005) or (European Commission, 2009) that initially got published in 2007 and got amended in 2009. The eID subgroup (European Commission, 2005) already indicated the importance of piloting, given the complex area eID is. This suggestion of pilots was one of the initiatives that finally lead to the STORK LSP.

THE STORK LSP

The STORK project started in May 2008 with an original duration of three years. As a “pilot A” it had been driven by MS. The project started with 14 EU and EEA states (Austria, Belgium, Estonia, France, Germany, Iceland, Italy, Luxemburg, Portugal, Slovenia, Spain, Sweden, The Netherlands, and United Kingdom). It had an original budget of € 20 million. In 2010 an extension by four further MS (Finland, Greece, Lithuania, and Slovak Republic) and to a budget of € 26 million took place. Under the CIP ICT-PSP co-funding regime, 50% of the project costs have been co-funded by the European Commission, 50% is borne by the project partners.

The overall idea was to define a framework that does not change the existing national eID infrastructure, but does define an eID interoperability layer on top of the national systems. The technical model was eID federation based on the Security Assertion Markup Language version 2.0 (SAML 2.0). It is described in (Leitold, Zwattendorfer, 2010).

In a nutshell, the project has been structured in three phases:

- In the first project year, common specifications for the eID interoperability framework have been developed.
- In the second year, the common specifications have been implemented and deployed into the national pilot systems.
- The third year was devoted to piloting the framework.

The target was to deploy and pilot in production systems. This to maximize lessons learned, as less compromise or weakening requirements under pilot assumptions is expected, once service providers have to deploy in their production environment. The assumption was that service providers rather will ask for close-to production quality, which increases confidence in the general applicability of pilot results.

The STORK cornerstones are thus the six pilots, each having specific requirements:

- The first pilot *Cross-Border Authentication Platform for Electronic Services* aimed at integrating the STORK framework to e-government portals, thus allowing citizens to authenticate using their eID. The portals did range from sector-specific portals such as the Belgian “Limosa” application for migrant workers to regional portals serving various sectors such as the Baden-Württemberg “service-bw” portal or national portals as the Austrian “myhelp.gv” for personalized e-government services.
- In the *Safer Chat* pilot juveniles could communicate with peers within their age range safely. The pilot has been carried out between several schools. The specific requirement was that in the authentication process the age group delivered by the eID is evaluated to grant access. Unique identification that is the basis of the other pilots is less important, this pilot was on pseudonymous access bases on age ranges.
- *Student Mobility* supported exchange of university students, e.g. under the Erasmus exchange program. As many universities nowadays have electronic campus management systems giving services to their students, STORK could be used to allow foreign students to enroll from abroad using their eID and to access the campus management system’s services during their stay. The prime requirement is authentication, as in the first pilot on cross-border authentication.
- The fourth pilot’s *Electronic Delivery* objective was cross-border qualified delivery, replacing registered letters. On the one hand, delivering cross-border requires protocol conversions between the national delivery standards. On the other hand, qualified delivery usually asks for signed proof of receipts. The latter – signed proof of receipts – is the specific requirement in this pilot. This enabled cross-border tests of signature-functions that most national eIDs have.
- To facilitate moving house across borders, the pilot *Change of Address* has been defined. In addition to authentication, the pilot had transfer of attributes, i.e. the address, as a requirement. An interesting aspect was that – in addition to the population registers – further authorities could be connected and automatically be informed of an address change. Examples are employment centers or billing addresses for the electrical supply companies.

- The European Commission Authentication Service (ECAS) is an authentication platform that serves an ecosystem of applications that are operated by the European Commission. Member States use these services to communicate among themselves and with European institutions. Piloting administration-to-administration (A2A) services with national eIDs was an STORK objective. The pilot *A2A Services and ECAS integration* serves this objective by linking up STORK to ECAS.

DECISION MAKING AND LESSONS LEARNED

In this section the internal operation of the LSP STORK is discussed. The decision processes are described and lessons learned are given. The lessons are solely described from the author’s perspective. Thus, the author is the only to be blamed on his opinions on the project outcome.

Structure to allow both project management and strategic orientation

A Large Scale Pilot is a complex undertaking. STORK started off in 2008 with 29 partners representing 14 states. The project volume was more than 1.000 person-months. After a year STORK got extended to 18 MS, more than 40 partners and 1.800 person-months.

The project can thus be seen as a big IT project that aims to deliver a result, which is cross-border federation of eID as technical systems, and to set this in production. This requires proper project management. With many partners this may need strict management and its enforcement in order to meet deadlines and to achieve the quality needed.

The project however can also be seen as collection of MS that operate towards a higher policy objective. Each MS has undergone own eID deployment and made own experience. More importantly, national eID infrastructure often represent huge investments that need to be protected. This requires consensus to make sure each MS gets embraced and to avoid a risk of the project falling apart, if MS see their interest not well represented. A strict project management structure putting focus on deadlines and getting the job done may contradict such a requirement of getting MS interest considered. Some diplomacy and sensitivity is needed on where substantial objection exists.

STORK has considered that already in the management structure that is illustrated in the following figure 2. In the bottom part, a management structure consisting of Work Packages (WPs) represented by its respective WP leaders is shown. WPs are defined content-wise, like developing common specifications and developing the software implementing it. To do management and to coordinate between the WPs a Programme Director and an Executive Board consisting of WP leaders does the day to day management. A similar structure is seen in many IT projects.

To avoid unbiased management, the Project Coordinator / Project Director has not been selected amongst the MS involved, but a company being independent from those has been chosen that has no own stakes in the main project content, e.g. that is no IdP issuing eID itself. (Project Coordinator of STORK and STORK 2.0 is ATOS Spain).

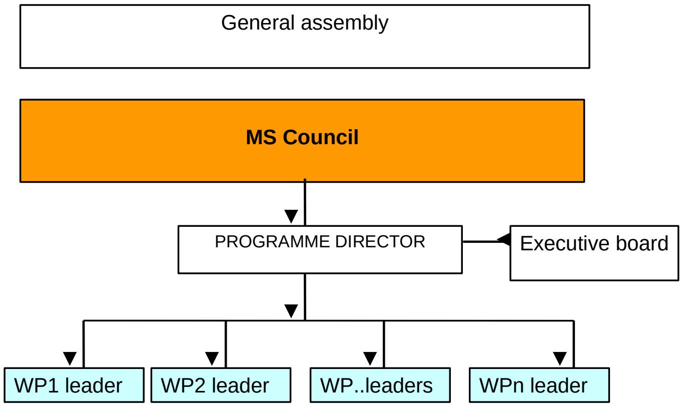

Figure 2. STORK Management Structure (from the LSP STORK contract)

The WP leaders, Project Director, and the Executive Board give a conventional management structure. The control functions are taken by two boards: The General Assembly comprises all project partners and is responsible for contractual aspects. Key on the strategic orientation of the project and for finding a consensus between MS is the Member State Council. It gathers one representative of each MS participating in STORK. It has been defined as the ultimate decision making body on all aspects that touch MS interests. If a substantial issue arises in the day-to-day management of the project, it got escalated to the MS Council. Just if consensus was found and a decision was made, the issue could proceed. The MS Council can be compared to an advisory board in a company, the MS Council however has less of an advisory role, but clear decision responsibilities that also relate to operations.

The lessons learned (again being an author's opinion) is that this separation of duties between traditional project management and the strategic decisions worked out well. There is some potential for friction between the timely provision of results and issues that can get blocking on the Member State Council level. However, the fact that most members of the Member State Council also have been involved in the WPs and had responsibility in the operations, e.g. as WP leaders, resulted in direct communication to the Member State Council and in early escalation.

The relatively lean management structure of a Programme Director and an Executive Board needed some tightening in the coarse of the project: Each of the (originally five, later extended to six) pilots has been defined as a separate WP and each applied its own management and quality control means. While this sounded fine in the beginning with experienced project managers in charge that applied their preferred management measures, the pilots also serve a common goal to test the common infrastructure. The risk of drifting apart existed. In an external project review this e.g. has been expressed for quality management as "*Each participant is declared free to use their own QM method: this makes overall project quality heterogeneous and inconsistent.*" To tighten that up the Member State Council requested to install a new role – a Pilot Coordinator. Its main duty was to make sure that pilots get aligned and to act as a "whip" if pilots drift apart and to enforce alignment.

Core Decisions

The project structure was roughly one year defining common specifications, one year implementing them and one year (later extended to 1 ½ year) testing them in pilots. The critical project phase was to come to agreements in the first year. While many has been discussed and agreed already in project proposal preparation, two aspects needed to be managed that (again from an author's perspective) carried a risk of overall failure, if no agreement is reached:

- The first aspect was on the security and assurance associated with the national systems. The processes and technical security of the systems differ. While each MS is convinced of the own system, in STORK trust in the other MS systems is needed. Trust requires security, but heterogeneous systems cannot easily be compared on its security features.

- The second aspect is that there are substantial differences in national deployment models. With reference to organizational and technical differences discussed in the eID overview section above, some MS favored decoupling MS internal complexity by national gateways in a "proxy model", other wanted to keep and advance their deployed "middleware models". Reasons for that choice rooted in the nationally deployed infrastructure, but also in legal aspects like liability and data protection.

On the former bullet, a quality authentication assurance (QAA) model has been agreed that allows a relatively flexible mapping of national eID issuance and technical security to four levels from "*QAA 1 for no assurance*" to "*QAA 4 for high assurance*". This is comparable to Levels of Assurance (LoA) in (White House, 2003) and (NIST, 2006). In fact, this similarity is intended and origins from basing STORK QAA with (European Commission, 2007) that itself intended to be aligned as good as possible with similar initiatives.

On the second bullet on substantially different national models, a model was found so that both approaches "proxy" and "middleware" can be embraced. It first started as two different approaches "PEPS" (for Pan-European Proxy) and "middleware" using a so-called Virtual Identity Provider (V-IDP) that somehow competed. The consensus finding lead to a result where both can be maintained by the MS, even with using same technical components. Just the deployment differs with "centralized deployment" as national gateway or "decentralized deployment" at the service provider. This mitigated the risk of falling apart in two competing approaches. Each approach has its pro and cons, but enforcing one over the other might have led to major impact on some MS.

The lesson learned by the author was that the project somehow started in partners explaining the merits of the own system and trying to convince others by highlighting its pros, sometimes playing down its cons. This was in partly lively and controversial discussions that at the beginning even delayed the progress. In the author's view this discussion process was however important to get an understanding of the others' systems. This beyond the eID system itself, as it roots deep in the states' administrative culture, processes and infrastructure. Once that got understood and that it was clear that the interoperability system may not interfere with MS situations – a LSP principle anyhow – consensus was found and progress could quickly be made on the common specifications.

Stakeholder Management

STORK covered 18 states which is a critical mass that allows to claim impact. It however does not cover the whole EU of 28 MS and EEA. It is important to inform also those states that are not project partners. Moreover, STORK has been implemented by the partners involved. At the end of the day it needs to get integrated into commercial products. This requires industry involvement. To achieve both, two information streams have been installed:

- A Member State Reference Group consisted of those states that have not been partners of the project
- An Industrial Group that market player could sign up to

Meetings with those groups have been organized about twice a year. The purpose was to inform those stakeholders on the progress and to get feedback. The stakeholder management is illustrated in the following figure 3 where the top shows the main project steps of specifying, developing and testing the interoperability building blocks. At the bottom the feedback loops with the Member State Reference Group and the Industrial Group is shown.

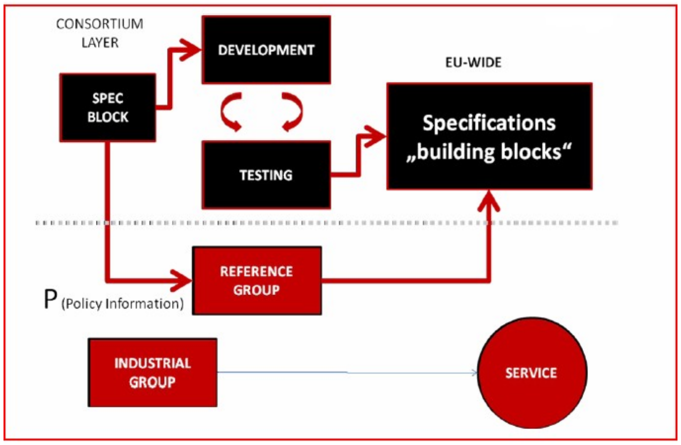

Figure 3. STORK Stakeholder Management (from the LSP STORK contract)

The lesson learned is that stakeholder management is important. The organization of a few workshop-style meetings alone however seems not enough to give sufficiently detailed updates of the progress of a complex project. It needs complemented by regular information via online media, newsletters, or alike. This was done by the project as well.

It is debatable whether industry involvement was sufficient. STORK did this via project presentations in Industry Group meetings. Other LSPs like epSOS had a tighter link with industry by establishing an Industry Team that got involved into the daily project work. Moreover some LSPs were active in standardization like PEPPOL and SPOCS. The approach chosen by STORK allowed MS partners in the critical first phases to establish the overall agreements without influence by industry interests. This may however be seen as a "closed club" that could benefit from more market consultation. No conclusion can be drawn on these aspects, pros and cons can be argued in either approach.

Sustainability

STORK was a project. This inherently means that it also has an end. For a sustainable infrastructure more is needed. It needs governance bodies, software maintenance, standardization or support. After discussion with the European Commission the STORK results have been handed over to Interoperability Solutions for European Public Administrations (ISA) programme that established a dedicated STORK sustainability action with a budget of about € 1,35 million. The sustainability action covers the period 2010-2014 to bridge the gap until the CEF Programme (European Union, 2013) and the eIDAS Regulation form a long-term solution.

CONCLUSIONS

The paper has discussed how Large Scale Pilots support decision making and policy in key areas. The LSP STORK on eID interoperability has been discussed in detail. STORK has started in 2008 and developed a technical model for eID federation between the existing systems of eighteen European states. It tested the results in six production pilots between 2010 and 2011, most pilots remained in production. Decision making that has been used in STORK got discussed. A balance was to be found between tight project management to lead a complex IT project to quality results, and the time it takes to get the consensus needed so that each state gets its interests considered.

The project was a technical success. It demonstrated federation of more than 100 different eID token types in production pilots. The main hurdle encountered was lacking legal basis and lacking mutual cross-border recognition of state's eID systems. This provided valuable input to the European Commission that then proposed a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS) (European Commission, 2012). At time of writing this paper, an informal agreement between the European Commission, the European Parliament, and the Council has been reached on this eIDAS Regulation. With its technical result, the LSP STORK could make some contribution to European policy making.

REFERENCES

e-CODEX (2009), *e-Justice Communication via Online Data Exchange*, The e-CODEX Website: http://www.e-codex.eu

epSOS (2008), *European Patients Smart Open Sevices*, The epSOS Website: http://www.epsos.eu/

eSENS (2013), *Electronic Simple European Networked Services*, The eSENS Website: http://www.esens.eu/

European Commission (2002), "*eEurope 2005: An information society for all. An Action Plan to be presented in view of the Sevilla European Council*", Communication COM(2002) 263 final.

European Commission (2005), "*Signposts towards eGovernment 2010*"

European Commission (2007), "*Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms*", Framework contract ENTR/05/58-SECURITY, Specific contract N°3.

European Commission (2009), "*Study on eID Interoperability for PEGS: Update of Country Profiles; Analysis & assessment report*", Framework contract ENTR/05/58-SECURITY, Specific contract N°12.

European Commission (2010), "*Digitizing Public Services in Europe: Putting ambition into action*", 9th Benchmark Measurement.

European Commission (2010b), "*European Interoperability Framework (EIF) for European public services*", Annex II to Communication COM(2010) 744 final.

European Commission (2012), "*Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*", COM(2012) 238/2.

European Commission (2013), "*Public Services Online 'Digital by Default or by Detour?*" eGovernment Benchmark 2012, DOI: 10.2759/13072 ISBN 978-92-79-29949-0.

European Union (1995), "*Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"*

European Union (2005), *Ministerial Declaration approved unanimously on 24 November 2005, Manchester, United Kingdom Presidency of the EU*.

European Union (2006), "*Decision No 1639/2006/EC of the European Parliament and of the Council of 24 October 2006 establishing a Competitiveness and Innovation Framework Programme (2007 to 2013)*"

European Union (2006b), "*Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market*"

European Union (2013), "*Regulation (EU) No 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility*"

Leitold H., Zwattendorfer B. (2010), "*STORK: Architecture, Implementation and Pilots*", in: Information Security Solutions Europe 2010 (ISSE 2010), Berlin, DOI 10.1007/978-3-8348-9788-6_13, pp. 131-142

MODINIS-IDM (2005), *eID study for the European Commission,* Website: https://www.cosic.esat.kuleuven.be/modinis-idm

NIST (2006), "*Electronic Authentication Guideline*", NIST Special Publication SP800-63, Version 1.0.2.

PEPPOL (2008), *Pan-European Public Procurement Online*, The PEPPOL Website: http://www.peppol.eu/

SPOCS (2009), *Simple Procedures Online for Cross-border Services*, The SPOCS Website: http://www.eu-spocs.eu/

STORK (2008, 2012), *Secure idenTities crOss boRders linKed*, The STORK and STORK 2.0 Websites: http://www.eid-stork.eu/ and https://www.eid-stork2.eu/

White House (2003), "*E-Authentication Guidance for Federal Agencies*", Memorandum M-04-04 to the Heads of All Departments and Agencies, December 16, 2003.