isa
Interoperability Solutions
for European Public Administrations

European Commission

Information Society and Media
Directorate-General

Towards a Trusted and Sustainable European Federated eID system

Final Report

JOINING UP GOVERNMENTS

15.09.2011

Request for Services (Request Form ID: INFSO-H2 (2010) ARES)

European Commission

Information Society and Media Directorate-General

STORK sustainability study

Final report, September 15, 2011

Authors: Cristof Fleurus, Sebastiaan van der Peijl, Erik Van Zuuren, Patrick Wauters, Diane Whitehouse.

DISCLAIMER
Neither the European Commission nor any person acting on its behalf is responsible for the use which might be made of the information contained in the present publication. The European Commission is not responsible for the external web sites referred to in the present publication.

The views expressed in this publication are those of the authors and do not necessarily reflect the official European Commission‘s view on the subject.

TABLE OF CONTENTS

1. INTRODUCTION

Deloitte was commissioned a strategic study on possible future models for the European eID management context and the role of the STORK Large Scale Pilot project under the CIP ICT PSP programme within this context.

As use of the Internet expands, a European Union (EU)-wide means of ensuring users'1 cross border online identity is becoming necessary. A large-scale pilot has already begun to test the possibilities of such a system. Its strengths, weaknesses, opportunities and strengths have been enumerated, and the potential for future progress in this field explored.

Key Action 16 of the Digital Agenda announces by 2012 a Council and Parliament Decision to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States (which may use the most appropriate official citizen documents – issued by the public or the private sector).

1.1 CONTEXT AND ASSOCIATED CHALLENGES

In today's digital environment businesses and citizens interact increasingly both with each other and with government through online services. Whether they are used for example for eBanking, eCommerce, eGovernment, reading email or social networking, these online services generally need some form of online credentialing to identify and authenticate users.

Many different organisations have set up solutions to provide online services that use an electronic identity (eID) to identify their end-users. Member States have adopted national eID schemes that provide end-users of eGovernment services (such as citizens and businesses) with the means to identify themselves securely. In the private sector, many different types of eID solutions have been implemented (for example, by banks or by companies selling online products or services). eIDs have been developed for specific domains such as eHealth, social security or the legal system.

Trust, data protection, privacy; interoperability and the existence of a legal framework providing legal certainty to cross-border authentication/mutual recognition of (national) eIDs, are all essential when it comes to online services that use eIDs, and it is crucial to provide trusted and secure credentials to authenticate users when setting up targeted online services. Delivering an eID solution at European level, which allows for the mutual recognition of eIDs across different Member States and different organisations (such that a citizen from country A can use his/her eID in country B) requires going beyond these key elements by establishing an environment that enables this interoperability across borders. Here a number of challenges, such as the technical, semantic, organisational as well as policy/legal implications come in to play.

The focus of this study is to look into the existing efforts at European level in establishing this enabling environment and looking beyond these achievements at what key elements should be put in place in

[1] By users we mean both physical persons representing themselves and physical persons representing companies.

order to move towards a trusted and sustainable cross-border eID solution at the European level. The aim is to take a pragmatic approach and provide insights into the elements that should be taken into account when setting up a running solution for cross-border interoperability for eIDs at the European level.

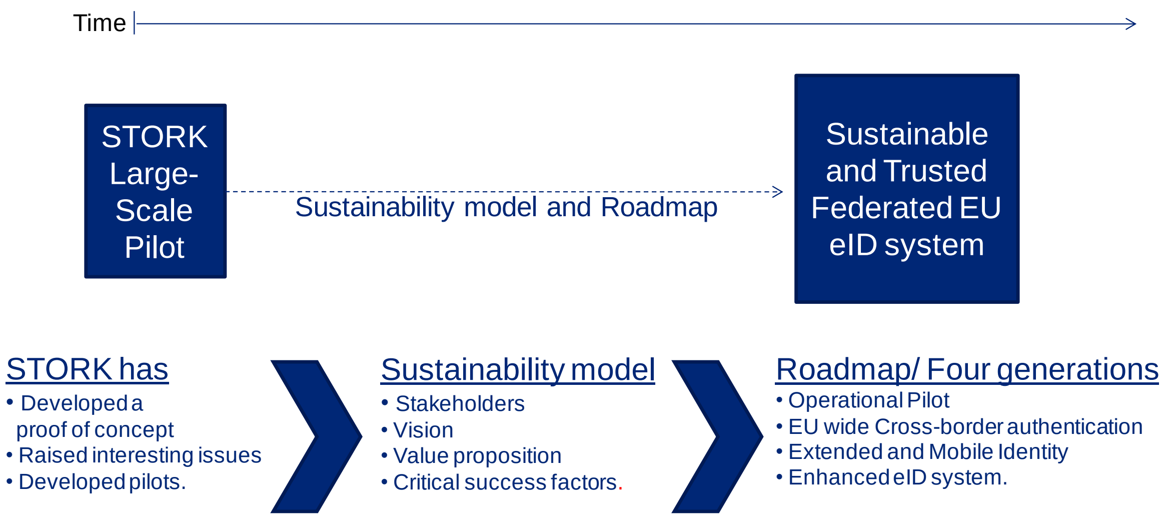
1.2 TOWARDS A SUSTAINABLE AND TRUSTED EU EID

In 2008, the European Commission launched the CIP ICT PSP large-scale pilot for the establishment of a European eID Interoperability Platform called Secure identiTy acrOss boRders linKed (or STORK). STORK's basic underlying principle is that systems that exist in the different Member States can be linked through a European Union (EU)-wide eID management (eIDM) platform which leaves intact the national approach to identification and authentication.

The objective of this study was to analyse the sustainability and the possible wider implementation of electronic identities on a European level, based on the lessons learned so far from the STORK large-scale pilot project co-financed by the Competitiveness and Innovation Programme Information and Communication Technology Policy Support Programme (CIP ICT PSP). The study examined the key aspects of a European Federated eID system2, especially the added-value of the potential services that could be offered by such a platform as well as well as the need for an efficient governance structure and basic financial aspects.

The relationship between the STORK large-scale pilot project and this study is outlined here (see figure 1). The figure highlights the way in which this study looks into a sustainability roadmap for STORK based on the implications of the activities and achievements of the STORK large scale pilot3.

Figure 1. Study logic


Time
STORK Large-Scale Pilot
Sustainability model and Roadmap
Sustainable and Trusted Federated EU eID system
STORK has
• Developed a proof of concept
• Raised interesting issues
• Developed pilots.
Sustainability model
• Stakeholders
• Vision
• Value proposition
• Critical success factors.
Roadmap/ Four generations
• Operational Pilot
• EU wide Cross-border authentication
• Extended and Mobile Identity
• Enhanced eID system.

[2] Taking into account the layers of the European Interoperability Framework for Pan-European eGovernment Services: legal, organisational, semantic, technological.

[3] STORK is, as Large Scale Pilot, delivering a report on sustainability and an action plans with specific recommendations for the sustainability of the STORK.

1.3 RESULTS AND SWOT OF THE STORK LARGE-SCALE PILOT

The STORK large scale pilot delivered a number of key results as an outcome of its pilot eID platform that operated across European borders.4

STORK's four main sets of results regarding a set of common specifications, a model for quality authentication assurance levels, a common code and six pilot applications. These deliverables are described in more detail below:

- **Common specifications**: The minimum requirements on legal, organisational and technical matters needed to establish a cross-border authentication platform between participating Member States have been defined. This resulted in an architecture based on an interoperable Pan European Proxy Service, middleware models and various other materials on non-technical issues. These latter issues are currently not yet all resolved.

- **Quality Authentication Assurance (QAA) levels:** eID and authentication credentials, registration and lifecycle processes have been defined on the level of the Member States' identity providers: they depend on the issuer of the electronic identity. As a result, there is a variety of policies and procedures used to identify and authenticate the establishment of credentials during the lifecycle management. To align this range of policies and procedures, QAA levels were defined. These permit a common interpretation of the different identity and authentication credential policies and procedures. The WP2 deliverables of STORK makes a detailed study by MS (including STORK enlargement MS) of the national QAA models and their mapping to the common Pan-European QAA model defined by STORK.

- **Common code:** A common code was created by STORK to facilitate the integration of identity providers and service providers i.e., those who are the main parties who deliver services in an online system. It eases the integration of the providers and creates interoperability between connected parties. This common code was provided to STORK participants so as to achieve a level of integration.[5]

- **The STORK Pilots**: Six pilots were put into production by STORK: they demonstrate that this kind of eID environment can work in a user-friendly way. The pilots were: Cross-Border Authentication for Electronic Services, Safer Chat, Student Mobility, Electronic Delivery, Change of Address and the European Commission Authentication System "ECAS" Integration. The pilots will be running as part of the project until December 2011

A strengths, weaknesses, opportunities and threats (SWOT) analysis was undertaken in relation to the delta between the STORK large-scale pilot and the conditions for the establishment of a production federated identity system. The main outcomes of such analysis can be summarised as:

- STORK's main strengths are: a working environment that was used actively in the six pilots, an architecture which is well documented and flexible, an architecture which is based on close to currently leading standards, and a set of comprehensive materials on crucial non-technical concerns.

[4] STORK, however, did not involve the creation or completion of a production environment. It was purely a large-scale pilot.

[5] The code will also be published under EUPL license and conveniently packaged for Member States and service providers to facilitate future integration beyond the lifetime of the project. Likewise, it will also be officially delivered to ISA for the "STORK Sustainability" action envisaged in ISA's 2011 Work Programme (http://ec.europa.eu/isa/workprogramme/doc/detail_description_of_actions.pdf).

- The main weakness to solve, albeit it was not part of the objectives of the large-scale pilot to solve it, is the lack of a legal basis with regard to cross-border identifiers and matching QAA-levels.

- The main opportunities perceived that arise out of STORK are: the considerable opportunities that exist when transforming STORK into a trusted European Federated eID system, the clear ability to support online services and cross-border public services, a high potential for cross-border private sector services and clear eID management opportunities for Public-Private collaborations/partnership/convergence in a number of contexts including Future Internet, Cloud Computing, Internet of Things.

- The main threats perceived that arise out of STORK (and which still need to be resolved) are undecided governance of the environment and its specifications[6], legal uncertainty and potential liabilities as a result of there being no existent legal framework, no relevant membership criteria or required service levels[7].

[6] The STORK specifications were issued by the pilot's consortium, were reviewed by technical teams of eID experts from several MS and have been adapted to serve the needs/take into account the specificities from all MS participating in the technical outcome of the project (14 countries). .

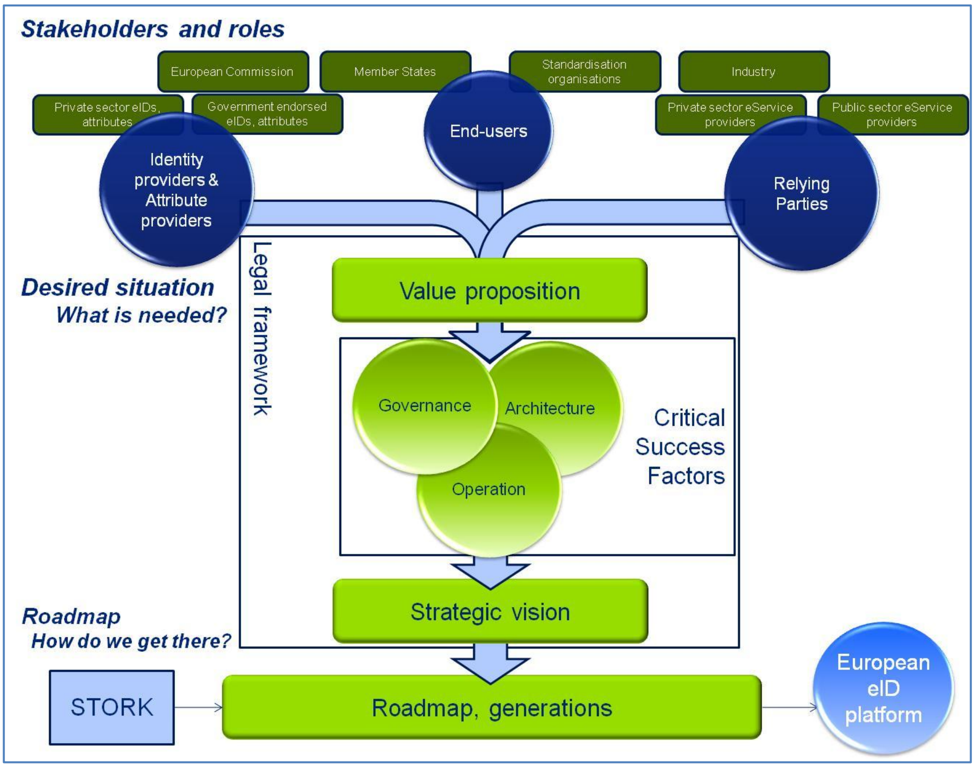
7 These aspects are subject to detailed discussion by the Consortium and clear recommendations will be provided i.e. in WP7 sustainability deliverables.

1.4 A SUSTAINABILITY MODEL FOR A EUROPEAN FEDERATED EID SYSTEM

A sustainability model for a European federated eID system was developed as a result of this basic analysis. Such a system could have considerable potential for Europe. Obtaining a sound picture of the critical success factors of a federated eID system and the different requirements and expectations that its stakeholders may have is essential to establish a clear view on the potential of this platform. Capturing the input of the stakeholders involved is key.

The sustainability model therefore starts with an overview of the different stakeholders and their specific roles in relation to a European eID platform. Next a clear value proposition for each of the stakeholders' groups is described. The relevant critical success factors are then examined. The analysis results in a targeted Euro-ID vision and a roadmap. The way in which this sustainability model has been developed is laid out in figure 2.

Figure 2: Sustainability model



2. VISION, SUSTAINABILITY AND BUSINESS CASE

Having a vision of what a European eID system would look like at policy level is crucial. Developing its business case is equally vital, and needs to be persuasive for both the public sector and private sector players involved in the approach. The European eID business case depends on a number of critical success factors. Building an understanding of these factors will facilitate the planning of a potential roadmap and will enable the players concerned to move towards a platform in the short- and medium-term time-horizon.

2.1 A GENERAL VISION OF A EUROPEAN EID SYSTEM

One of the key enablers for establishing cross-border interoperability of services in a European Digital Single Market is the establishment of reliable and trustworthy electronic identities. Being able to rely on the certainty or authenticity of a user's identity with a sufficient level of assurance is crucial for the development of more value-added cross border services. The lack of cross-border interoperability of national electronic identification solutions prevent European users from accessing online services in other Member States and, hence, hinder them to fully benefit from the digital single market.

Citizens of Europe should be able to study, work, reside, receive healthcare and retire anywhere in the European Union (EU). Entrepreneurs should be able to set up and run smoothly a business anywhere in any Member State.

Today most public online services either do not function across borders or they involve cumbersome procedures. People cannot easily apply for public services in an EU country other than the one in which they are resident or where they are established as a business. This reduces seriously the mobility and trade of European businesses and citizens.

There is currently no standardised or trusted eID system available on a European level[8]. As a result, online service providers have either implemented themselves various systems for the authentication and identification of the users accessing their services or rely on other systems. The domains involved include banking, eCommerce, eGovernment, education and telecommunications. In Annex 3 examples of applications in the banking and the telecom sector are provided.

Presently there is a patchwork of authentication and identification solutions in Europe. End-users maintain many different user accounts based on a low level of quality authentication assurance, i.e. username/password and run risks concerning privacy and identity theft on many fronts. It is often unclear how reliable and trustworthy the authenticity of the identity system used in these various systems is and how well a user’s identity and privacy is protected. This creates lack of confidence in citizens to engage in online operations over the Internet which is a barrier for the growth of European economy in the Knowledge Society.

Establishing a trusted, interoperable and federated European eID system could provide a solution to the challenges that service providers are facing. It would facilitate an environment within which they can establish the identity of a user in a sufficiently reliable and trustworthy way. The development of services both in the public and the private sector and the growth of a truly European online market could be the result.

A federated European eID system would provide end-users with a trusted online access to electronic services and service providers with the possibility to use a readymade system to identify their customers and to concentrate on their value-adding services.

[8] The STORK model represents a starting point as it answers several challenges especially at technical and semantic levels

As stated in the Digital Agenda for Europe and the eGovernment Action Plan 2011-2015, cross-border services are a key supporting feature of an integrated European single market and for Europe's competitiveness and growth strategy. The European eGovernment Action Plan 2011-2015 identifies eSignatures, eIdentification and interoperability as clear pre-conditions "to improve the conditions for development of cross-border eGovernment services provided to citizens and businesses"[9](The European eGovernment Action Plan 2011-2015, 2010).

The Action Plan focuses on those key cross-border services that enable citizens and businesses to set up a business anywhere in Europe, and to study, work, reside and retire anywhere inside the EU. For this "electronic identification (eID) technologies and authentication services are essential for the security of electronic transactions (in both the public and private sectors)." The Action Plan therefore calls for the Member States to "apply and roll out the eID solutions, based on the results of STORK and other eID-related projects" between 2012 and 2014 (The European eGovernment Action Plan 2011-2015, 2010). Cross-border eID and authentication services thus become essential building blocks for other services.

The implementation of the first European eGovernment Action Plan has already resulted in a number of large-scale pilot projects – besides STORK – which are developing concrete solutions for rolling out high-impact cross-border eGovernment services. They include PEPPOL, SPOCS, epSOS and eCODEX.

While the pilot projects in themselves seem to be successful, there is not yet an organised strategy in place on how to implement them across Europe. There is currently a risk that the solutions that have been developed will not be implemented. It is very important for all the relevant EU initiatives to evaluate the legal requirements and decision-making procedures to make large-scale pilots more sustainable. This is mitigated by commitment from the EC and the MS, in the case of STORK to keep common STORK infrastructures and the majority of services running beyond the end of the project and through the ISA STORK Sustainability and ECAS Integration actions. For longer-term sustainability several aspects are under discussion.An integrated strategic plan for the different large-scale pilots will be needed.

2.2 THE BUSINESS CASE FOR A EUROPEAN EID SYSTEM

The perspectives, needs and expectations of key stakeholders need to be taken into account if a sustainable eID environment is to be achieved. The proposed sustainability model distinguishes between different stakeholders and their roles: "relying parties"[10] or service providers, identity providers or attribute providers, end-users and solution providers. The business cases or value propositions for these stakeholder groups are developed. For each of them, the key trends and challenges are first outlined, the drivers and possible business cases are laid out and some examples of applications are given.

First the key trends, benefits and potential applications are listed for **relying parties or service providers** (whether in government, the private sector, eCommerce, eBanking).

[10] A Web site or other entity on the Internet that uses an identity provider to authenticate a user who wants to log in.

The observed key trends and challenges are:

- There is a significant growth of online services both in the public and private sectors. Each party is looking at how to identify its end-users;
- Each party needs to find a way to register, authenticate and identify its end-users (although to do it on a national basis leads to a scattered non-interoperable eID landscape);
- Currently service providers either need to build their own system or they rely on systems built by other providers (this results either in unnecessary costs or raises questions about the terms and conditions involved);
- Another major challenge for all service providers is the increasing demand for mobile authentication.[11] This results in numerous challenges and lots of investments which hamper the rapid deployment of new initiatives.

The benefits of a federated European eID system for service providers relate to the fact that they will:

- Have access to large numbers of European consumers to whom they will be able to offer their services in larger and cross-border contexts;
- Know that their pre-registered consumers are equipped with eID tokens that are all certified;
- Be able to lower their costs for user-registration and user-authentication;
- Be able to avoid legal uncertainty, possible liabilities and fraud when delivering their services cross-border;
- Provide to industry common specs, standards and building blocks for better and interoperable products and services capable of handling eID-related info across borders, applications and sectors.

Examples of possible applications of interest to service providers of different sorts are that they can:

- Register their clients fully electronically and in a legally compliant way e.g., this could be done by a banking or insurance service that operates cross-border with clients that are SMEs;
- Enable a foreigner who is not resident in the country or whose business is not registered in the country to access governmental services remotely e.g., to fulfil relevant administrative obligations in time or submit proposals to public tenders.

The following are the key trends, benefits and potential applications in context of **identity providers or attribute providers** (whether it is government owned, government endorsed, or Euro-ID-accredited) with regard to a EU Federated eID system:

The key trends are:

- Solutions exist which range from self-asserted identity systems (e.g., webmail accounts), self controlling systems (e.g., eBay), payment-based environments (e.g., credit cards) to government-endorsed identities;
- Several certification authorities exist, and there is a growing interest in mobile identity and payment systems.

Benefits for identity providers are that:

- Private sector players will be interested in becoming identity providers in a federated European government-endorsed eID system if certain conditions are fulfilled: they need to have a vested interest, a clearly identified legal and secure environment should exist;
- The banking sector and mobile operators could be interested in stimulating re-use of identities issued by them for their customers to access their own services.

[11] STORK also detected this demand in countries where this is possible as it is perceived as more convenient by users. In addition, ENISA has also studied risks related to mobile IdM (http://www.enisa.europa.eu/act/it/eid/Mobile%20IDM)

Examples of possible applications:

- Mobile operators may step in and be willing to have their identity systems recognised and, as a result, sell more capacity and value-adding online services.

The following are the key trends, possible business cases and potential applications in the context of **end-users** (whether as a private citizen, government representative, or employee) with regard to an EU Federated eID system.

The key trends and challenges to be reckoned with for end-users are that they are:

- Looking for a reliable, trustworthy, low-cost, easy-to-use means of obtaining online access;
- To a greater or lesser extent privacy sensitive and increasingly enamoured of mobile devices.

The most important benefits for end-users would be:

- A clear EU eID ecosystem brand, easy access to a trusted electronic identity, and user-friendly credentials could be basis for larger popular acceptance of online services;
- To enable European citizens to identify themselves when living and studying abroad and when "travelling" as online consumers in the virtual market;
- Increased mobility opportunities for physical and legal persons across Europe through cross-border eID apps;
- Administrative simplification reducing red-tape and saving time and money for citizens and public administrations while achieving increased efficiency;
- Enhancement of the Digital Single Market and of commercial services;
- Enhanced user control and better addressing of privacy and data protection issues.

Examples of possible applications of interest are:

- Access by non-nationals to eGovernment online procedures;
- Access to health and other care records while abroad;
- Cross-border registration for e.g., a banking or insurance service online;
- Support to various forms of citizen and student mobility.

2.3 CRITICAL SUCCESS FACTORS FOR A SUSTAINABLE EID SYSTEM

Three critical success factors for a future European federated eID system were developed. There needs to be: a sound governance structure, a strong enterprise architecture and a reliable service management.

These critical success factors range from the more strategic to the more operational. They will often need a considerable degree of specification about the details involved in planning and running them. Structurally, the different parts of the proposed system can become quite complex. Hence, a governance structure which will oversee the whole process is of considerable importance.

Here, the three critical success factors are described sequentially: they range from governance to enterprise architecture and service management.

2.3.1 Governance model

The first critical success factor is the existence of a sound governance structure supported by solid coordination. In general, the governance structure should ensure the long-term sustainability of the platform. It should guarantee the quality level of the services offered, and the data used and provided by the eID platform. This requires agreement between European States and the European Commission, also for respective responsibilities and costs and considering trust and liability implications.

To accomplish these tasks, a Governance Model was developed. The Governance Model includes three elements that relate to legal aspects, strategic governance, and stakeholders' interests:

- **Legal Aspects, Regulations and Compliance.** When a European Federated eID system is created, relevant regulations and best practices should be taken into account. Assurance needs to be provided that the system is operating in conformance with European legislation and that it operates by using accepted good practices. To facilitate the proper level of trust to be provided by a European Federated eID system, it would be useful to have and maintain a legal European framework with regard to electronic identities and cross-border authentication and for it to be enforced e.g., through accreditation.
- **Strategic Governance and Coordination.** The sound organisational aspect of a sustainable Federated eID system is of the utmost importance for the services offered by it. The strategic governance will ensure the long-term survivability and quality of the identification and authentication services of the Federated eID system. Four different organisational bodies are needed.
    - The first organisational body needed is the **Strategic Governance Body** which ensures the high-level steering of the system;
    - The second organisational body is the **Architecture and Standards Body** which is responsible for defining the Federated eID system higher-level architecture and standards and ensures that these standards are respected; It should also take responsibility for maintenance of common reference code and common specifications, i.e. distribution of new versions, patches, technical support to IdP’s, etc.
    - The third organisational body is the **Service Level Management Body** which safeguards the intended service levels of the environment It should handle questions like the acceptance of monitoring by the service providers of the service levels, the management of a growing ecosystem of services, and the question whether the common level of services should be mandatory.
    - The fourth organisational body is the Information Security and Accreditation body which maintains the trustworthiness of the system.

  Each of these individual bodies needs to be well-coordinated and to be coordinated among each other.
- **Stakeholders Interests and Management**. A procedure should be put in place to enable stakeholders that want to suggest changes or new features to propose them and discuss them with their peers. Such propositions could be brought to the governance and coordination level.

2.3.2 Enterprise architecture

The second critical success factor for a sustainable European Federated eID system is the existence of a **strong enterprise architecture** and the appropriate solution architectures and technical standards. The existence of a reference implementation will also be of considerable, additional added-value:

- The European Federated eID system and the architecture that is used to create the system will certainly evolve over time. It is thus essential that the architecture is created and evolves in such a way that it remains flexible and can deal with changes and technological future evolutions. To create such flexibility, components defined in the architecture should be created through a modular design. By using modularity in the design, the features implemented are isolated in terms of the different components and services. These components should communicate using market-wide, accepted, standardised message-formats and protocols.

- The second architectural element is the availability of a “cookbook” and a reference implementation. Such a reference implementation guides future identity, attribute or service providers when connecting to the European eID system.

STORK has delivered a reference implementation which has been further validated in practice by six pilots and by the development and operation of cross-border interoperability components and satisfies both conditions.

2.3.3 Service management

The third critical success factor for a sustainable European Federated eID system is **reliable service management**. The service management aspect needs to guarantee that the day-to-day operation and the expected services can be offered to customers.

- A first element in this context is the Operational Service Management. The service management should, first, guarantee that the European eID Services comply with the required operational conditions, second, that the European eID Services cannot be interrupted when connecting new identity providers or attribute providers and, third, should prevent a malfunction of one of these parties. This activity should not be under-estimated as it will also have to handle various security operations. It therefore should be set up as a Security Operations Centre / TrustCentre.
- A second element in this context is the on boarding of new parties into the System. It should maintain the trustworthiness and reliability of the system up to required levels. It is recommended to foresee, plan and prepare the necessary procedures, templates and tests before allowing any party to hook up to the system.
- A third element in this context is Training and Knowledge Transfer. By documenting and sharing past experiences with integrating identity, attribute or service providers, the repetition of past mistakes made can be avoided. The knowledge and experience of former projects and initiatives can be leveraged for the benefit of new connecting parties.

2.4 A POSSIBLE ROADMAP FOR A SUSTAINABLE EUROPEAN FEDERATED EID SYSTEM

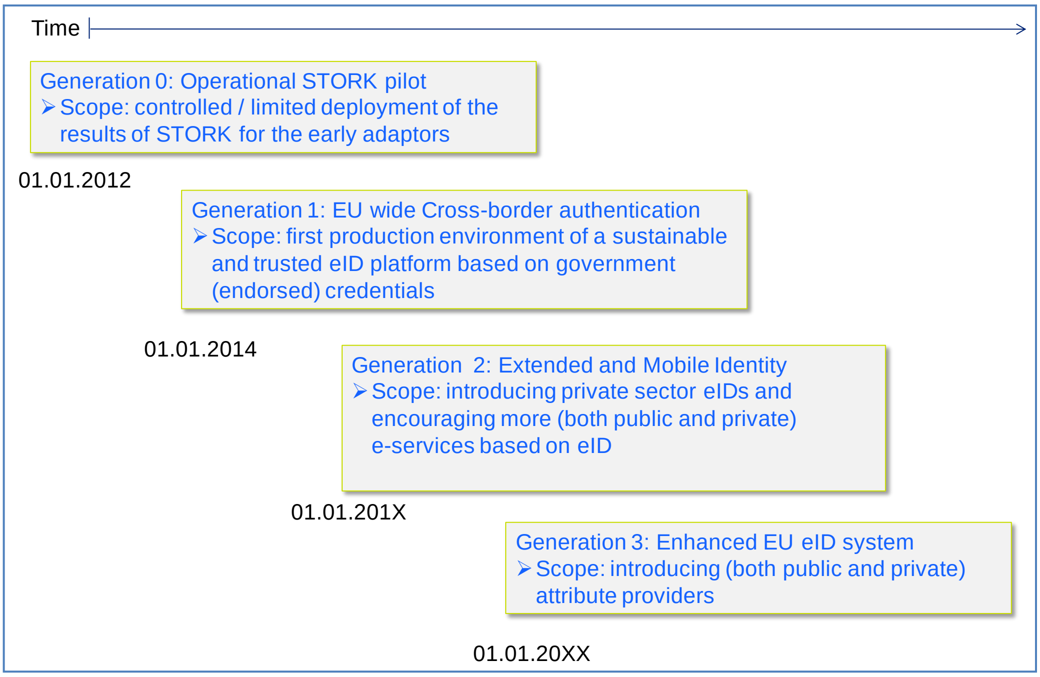
In this section we present a possible roadmap to enable a shift towards a European federated eID system and provide a good foundation for its continuation and sustainability. The suggested roadmap has four generations. The way in which the roadmap is governed is of considerable importance. Obviously the European Commission and the member states participating in the STORK pilot should be involved in the final definition of the roadmap. It should consider the views on sustainability provided by the STORK Consortium, the medium-term actions envisaged in ISA 2011 WP and future work by a new Pilot A of the CIP ICT-PSP 2011 WP (Objective 4.2) which already considers a number of the points proposed in some of these generations.

The arguments for the roadmap's general underpinning principles, its four generations, and how the governance is to start, are presented here.

2.4.1 General Reasoning and set-up of the Generations

“Rome” was not built in a day nor will a European eID system. To ensure the steady and reliable growth of a European eID system, advance planning and preparation is needed. This planning and preparation needs to be understood by the relevant European institutions but also by the individual Member States. The involvement of a wide variety of stakeholders is also crucial to build this understanding and commitment more widely. Therefore, a phased approach is recommended and the concept of “generations” to the roadmap that is proposed is introduced. Four generations of a roadmap are outlined. See figure 3.

Figure 3: Roadmap


Time
Generation 0: Operational STORK pilot
➢ Scope: controlled / limited deployment of the results of STORK for the early adaptors
01.01.2012
Generation 1: EU wide Cross-border authentication
➢ Scope: first production environment of a sustainable and trusted eID platform based on government (endorsed) credentials
01.01.2014
Generation 2: Extended and Mobile Identity
➢ Scope: introducing private sector eIDs and encouraging more (both public and private) e-services based on eID
01.01.201X
Generation 3: Enhanced EU eID system
➢ Scope: introducing (both public and private) attribute providers
01.01.20XX

2.4.2 Short description of the Generations

For each generation of the four generations of this roadmap, a short description of what type of functionality is being targeted in each is offered.

More targeted descriptions of each of the four generations of a proposed roadmap are outlined in annex 1 and annex 2 to this report.

Table 1: Short description of the generations

Generation 0: Extended STORK pilot	The deployment of the results of STORK by the early adopters so that it can be used as an authentication platform for applications that can accept the current setup and deem the current “guarantees” sufficient. Simple authentication services based on recognised government (endorsed) electronic identities. No legal framework or guarantees.
Generation 1: Cross-border trust(eID authentication)	Authentication services are offered to public and private sector service providers. A solid EU eID system based on existing government issued (or government endorsed) eIdentities. Founded on an architecture that has further matured and that has evolved closer to generally accepted standards, and supported by a strong and rigid governance body and decent service management.
Generation 2: Extended and Mobile Identity	Allow private industry (e.g., banks (including non government endorsed), mobile operators) to act as identity providers, subject to the necessary standards and specifications so as to maintain the level of trustworthiness and quality of an EU eID system. Service providers can benefit from the involvement of additional private sector identity providers (e.g., due to the entrance of mobile operators as identity providers onto the market or due to identity providers that attest to a person’s quality).

Generation 3: Enhanced eID system	A full-scale European cross-border identification and authentication platform which also supports attribute services. Attribute services will allow service providers to obtain complex additional information about an asserted identity (for example: is this natural person the managing director of company X and authorised to sign contract Y, is the party allowed to approved transfer above an amount X, ...).

2.4.3 The Governance Dimension

Since the governance element of the roadmap will be of particular interest to policy-makers the roadmap's governance aspects are described here. The roadmap illustrates the importance of phased decision-making, expansion and enhancement of the steps needed step-by-step, the integration of activities between the public and private sector, and the importance of a more reliable and organised legal, regulatory and standardisation set of environments.

The study team has not identified all the timelines needed for transition between each generation of the roadmap or its end-point for achievement. It is considered that decision-making on this point will be of keen interest to, and should be a matter for collaboration between, the European Commission, Member States, industry and relevant stakeholders.

Table 2: The governance of the generations

Generation 0: Extended STORK pilot	Governance aspects: An initial generation is the *de facto* starting position for a European EID system. It involves the deployment of the results of the STORK large-scale pilot for early adopters. It can be used as an authentication platform for applications that can accept the current set-up and which deem the current “guarantees” to be sufficient.
Generation 1: Cross-border trust(eID authentication)	Governance aspects: As the environment now grows towards maturity, and as third parties start to rely on the system (and, hence, possible liabilities start to occur), the governance mechanism must also mature. Preferably, a legal framework should be put in place which provides a solid foundation to this aspect of governance. “Contracts” should be organised with all members and service providers, so that all the parties are sure that everybody adheres to the rules of the system. In this context, the option to develop formal memberships, and include in those memberships the possibility for the Member States to audit periodically the local service providers to ensure compliance (e.g. with privacy legislation) could be foreseen. However, the exact way in which a compliance system can/will be implemented will have to be decided at a strategic/governance level. In this phase, it will also be important to start resolving any loose ends which still exist such as QAA-level-matching, and cross-borders identifiers. It will also be important to start preparing for the future through technical aspects such as further standardisation of the semantics and a taxonomy of assertions.

Generation 2: Extended and Mobile Identity	Governance aspects: For the second generation of the Euro-ID Authentication Services, the governance requirements will be based on the first generation. Given, however, that this generation of the Euro-ID Authentication Services will integrate private industry as identity providers, it is highly recommended that the appropriate legal basis (such as a Directive) would be in place by this stage. This legal basis would then result in clear obligations for non-governmental identity providers that want to be members of Euro-ID. To validate the practices used by new, private industry, identity providers, a Euro-ID accreditation scheme should be defined.
Generation 3: Enhanced eID system	Additional effort will be required to ensure that the taxonomy and the associated semantics remain under strict control and that attribute providers comply with the Euro-ID, quality and accreditation requirements. As with the introduction of private industry identity providers, an accreditation scheme for attribute providers will also have to be created that defines the Euro-ID requirements. Legal considerations, such as compliance with the Data Privacy Directive, will also have to be taken into account. These elements are closely associated with the concept of European Base Registries.

3. CONCLUSIONS, RECOMMENDATIONS AND ACTIONS

A set of conclusions and recommendations are laid out which follow logically from the assessment made in this study on the path towards a trusted and sustainable European federated eID system. Considerations are targeted on the first two of the generations of the roadmap (Generation 0 and Generation 1).

3.1 MAIN CONCLUSIONS AND RECOMMENDATIONS

A number of main conclusions can be drawn as a result of this study. They relate to the need for eIDs and the business case which underpins this development. Several important recommendations are highlighted.

The establishment of recognised and trusted electronic identities that can be used for different online services in a reliable and legally certain way across the EU is a key enabler for the development of cross-border e-services12.

- **The European Commission and the Member States have to play a steering role in the further development and governance of a EU federated eID system.**

Good **governance and coordination** that involves different stakeholders at both European and national levels, public sector and industry – balancing their mutual interests and ensuring transparency, and mechanisms that ensure the delivery of the system targets – is essential. This governance cannot be based any longer on the accidental composition of a consortium in a project. It is the study team's advice that it is important to:

- **Oversee the establishment of a European eID council or governance body** that represents all the key stakeholders that can then consult with the larger group of stakeholders.

The STORK large-scale pilot has delivered a number of key building blocks to achieve such an eID platform that operates across borders. It has delivered common specifications, assurance levels and common codes. It is the study team's advice to

- **Build further on the achievements of the STORK pilot** and start with a controlled and limited deployment (for early adaptors not needing hard assurances).
- **Start to implement a proposed four-generation roadmap** so that the system increases in functionality and maturity in a controlled manner.

The **financial aspects of the system** will evolve with its development. Once the real production stage has been accomplished, governance, architectural and operation costs will increase since the system will become more complex and more services will have to be managed. The costs could then be supported by a combination of approaches: free membership for government identity providers and service providers, and a membership fee for commercial stakeholders. At the initial stage, however, during which there are only a low number of commercial partners, EU and Member State-funding will still be required to maintain the system. Further research will be needed to develop the financial aspects more in depth.

[12] It must be considered that not all EU-27 countries will be able to participate in the system depending on their respective maturity in the field of eID.

3.2 CONCRETE ACTIONS FOR GENERATION 0 AND GENERATION 1

The eventual roadmap is four generations in length. However, clearly, the most urgent and important stages of the roadmap are its first two generations. The first generation is referred to as Generation 0. The second is called Generation 1.

The precise actions that would need to be accomplished in each of these two, immediate and shorter-term time-horizons, are outlined here.

To establish a "Generation 0: Operational STORK pilot" which would offer a controlled and limited deployment of the results of the first STORK large-scale pilot for early adopters, the following actions would need to be implemented:

- **Governance actions:** the Commission should set up a Service Level Management Body and Information Security (and Accreditation) Body to document and formalise the minimum set-up required by an "extended" STORK Pilot. Its responsibilities would be to limit the environment to government identity and service providers and to clearly state the conditions of use. These service level conditions and security aspects can be worked out by national or external experts but will need to be confirmed by the "bodies" staffed by mandated representatives of the Member States and the Commission.
- **Architecture actions:** work with the current conceived STORK architecture which would have all its key elements under government control so as to ensure a level of trust and privacy assurance, and ensure conformance to the established conditions of use.
- **Operations actions:** the operations of the environment can be delivered under the best efforts of coordination by a central operations centre and under the responsibility of each of the participating Member States for its national components or services. The central operations centre (e.g. the organisation now responsible for maintaining ECAS) should manage changes in the infrastructure and software versions as well as handle incidents and problems.
- **Costs and financing aspects:** the cost of these governance bodies and central operations should be supported by the European Commission. The costs of national components or services should be supported the individual Member States.

To establish a "Generation 1: EU-wide Cross-border authentication" which would offer the first production environment of a sustainable and trusted eID platform based on government-endorsed credentials, the following actions and points of attention need to be observed:

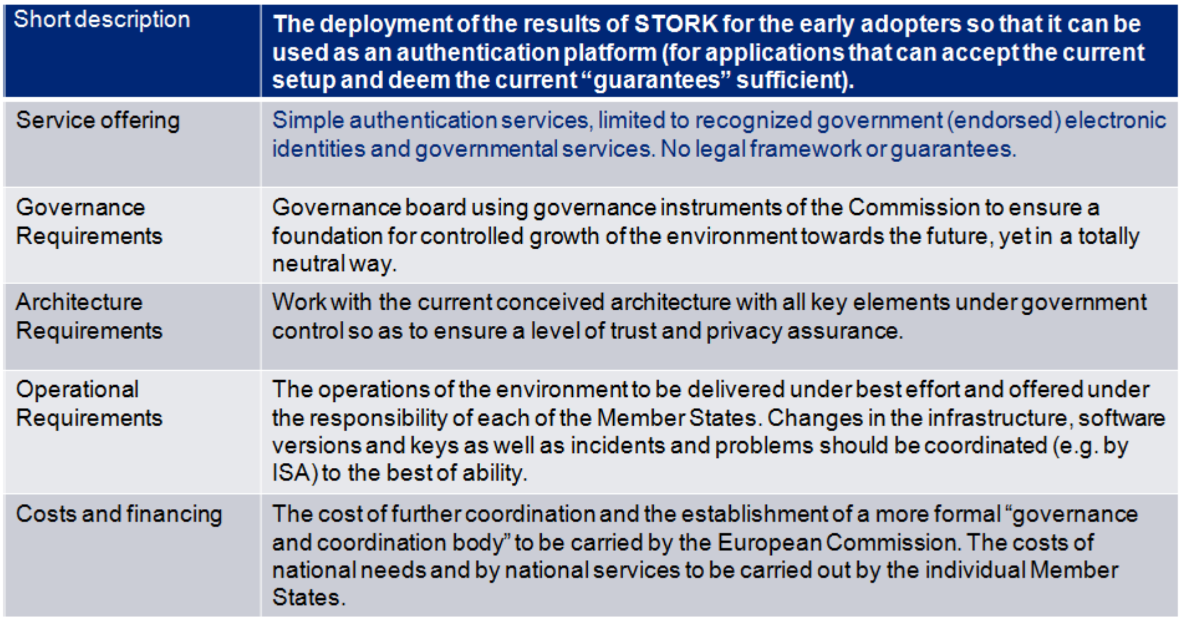
- Governance actions under control of the Strategic Governance Body: all the relevant governance bodies should be put in place to steer and control the further evolution of the roadmap: Strategic Governance Body, Architecture and Standards Body, Service Level Management Body, Information Security and Accreditation Body. These bodies should be staffed with mandated Member State-officials and supported by independent experts. A legal framework (or clear "conditions of use") should be put in place which provides a solid foundation for the participation of all European countries.
- Architecture actions (under control of the Architecture and Standards Body): elaboration of next generation architecture that moves more in line with dominant standards and more-widely accepted initiatives. Establishment of agreements on standards with regard to cross-border identifiers, assurance levels and semantics.
- Operational actions (under control of the Service Level Management Body): will move the central operations center to a mature service organisation. Trust, list maintenance and key management services for secure cross-border communication should possibly be added to its responsibilities. A knowledge centre for training, knowledge transfer, and the development of cookbooks to integrate and support service providers should be envisaged.
- Costs and financing aspects: the cost will consist of the funding needed for the governance bodies, the hiring of independent experts to elaborate the next generation architecture and standards and the associated security and service management environment. The costs will

also consist of the necessary funding to set up the trust list, the key management environment, and the staffing of the central operations centre and knowledge centre.

4. ANNEX 1 – GENERATIONS DESCRIPTION AND ILLUSTRATIONS

This annex contains a detailed explanation of each of the four generations of the roadmap that are suggested (see Descriptions) and an illustration of possible applications that could be introduced at each stage of a generation (see Illustration of Application).

Generation 0: Extended Stork Pilot

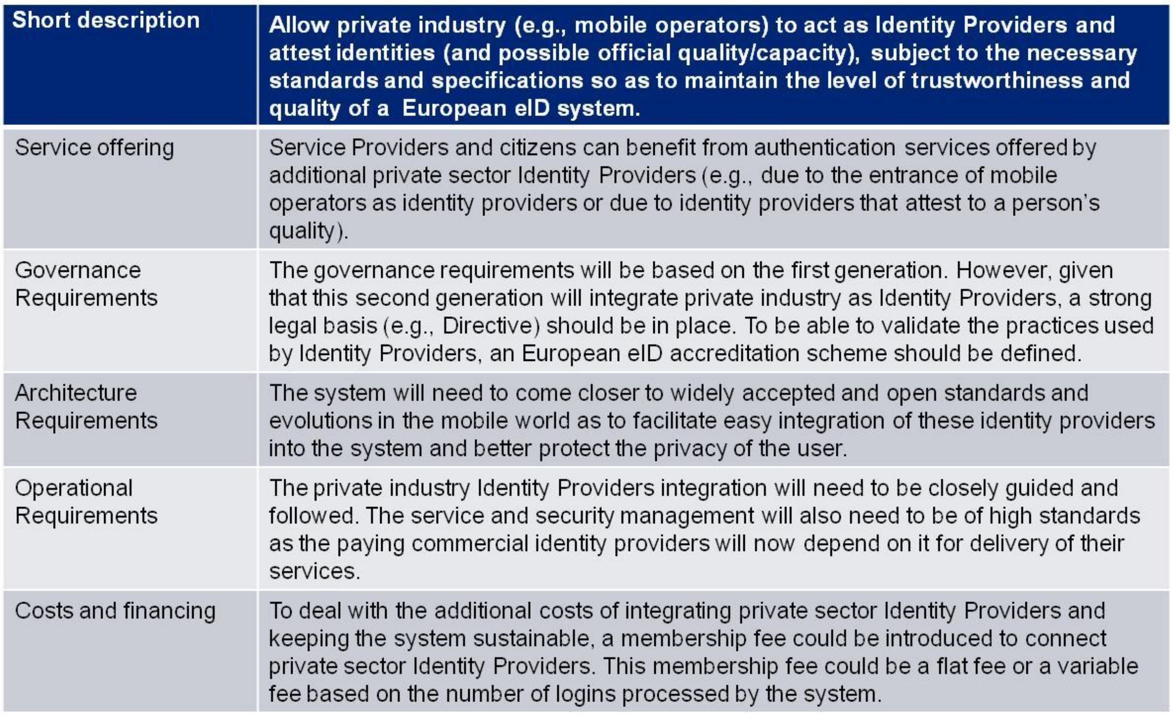


Short description	**The deployment of the results of STORK for the early adopters so that it can be used as an authentication platform (for applications that can accept the current setup and deem the current "guarantees" sufficient).**
Service offering	Simple authentication services, limited to recognized government (endorsed) electronic identities and governmental services. No legal framework or guarantees.
Governance Requirements	Governance board using governance instruments of the Commission to ensure a foundation for controlled growth of the environment towards the future, yet in a totally neutral way.
Architecture Requirements	Work with the current conceived architecture with all key elements under government control so as to ensure a level of trust and privacy assurance.
Operational Requirements	The operations of the environment to be delivered under best effort and offered under the responsibility of each of the Member States. Changes in the infrastructure, software versions and keys as well as incidents and problems should be coordinated (e.g. by ISA) to the best of ability.
Costs and financing	The cost of further coordination and the establishment of a more formal "governance and coordination body" to be carried by the European Commission. The costs of national needs and by national services to be carried out by the individual Member States.

Generation 1: Cross-border trust(eID authentication)

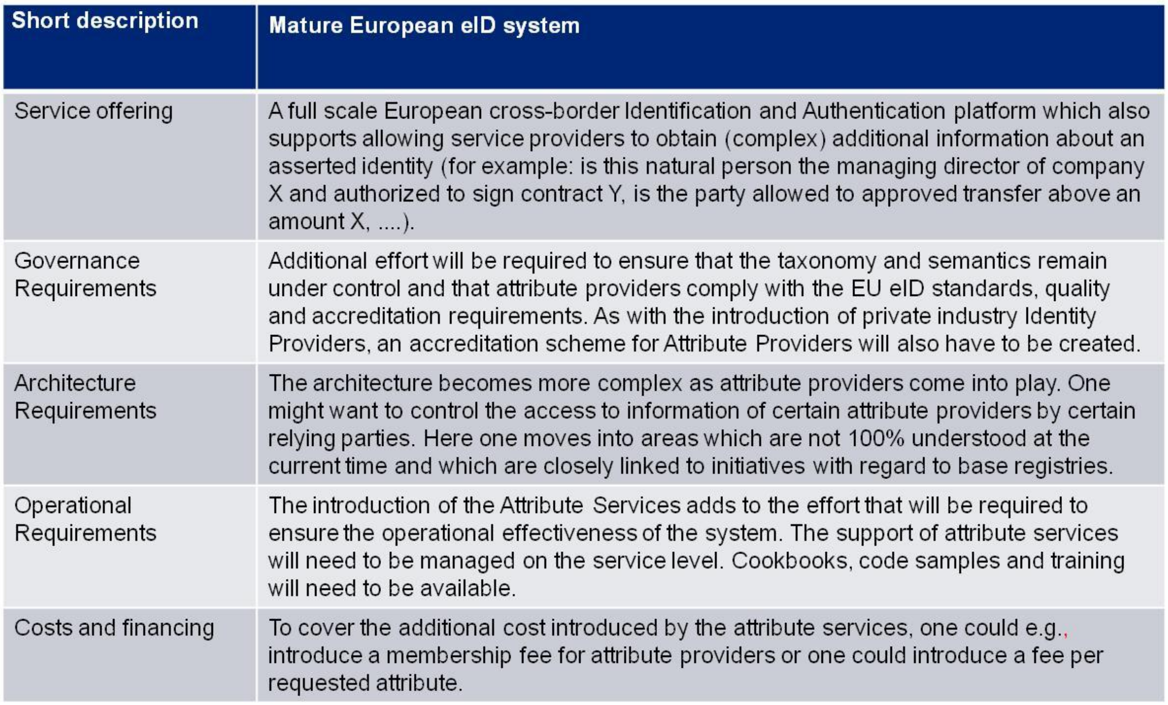
Short description	Authentication services are offered to public and private sector service providers.
Service offering	Solid European Federated eID system based on existing government issued (or government endorsed) eIdentities, and on an architecture that has further matured and that evolved closer to generally accepted standards, and supported by a strong and rigid governance body and a reliable service management.
Governance Requirements	For this generation, the governance must grow to maturity. Preferably a legal framework should be put in place which provides a solid foundation for the participation of all European countries. At least “contracts” should be closed with all members and service providers. Also, for this generation it becomes important to further agree on / standardise cross-border identifiers, assurance-levels, semantics and architecture in line with main trends in the market.
Architecture Requirements	For this generation, it is important that the system is in line with dominating standards and more-widely accepted initiatives so as to facilitate easy integration of service providers into the ecosystem and further improve privacy protection.
Operational Requirements	Service management and operations, training, knowledge transfer, cookbooks with common specifications and code samples will need to be available to integrate and support service providers.
Costs and financing	The financing of the first “production” generation European eID system can be a combination of free membership for government Identity Providers and Service Providers and a membership-fee for commercial Service Providers. In an initial stage (possibly with a low number of commercial service providers), EU/Member State funding will still be required to maintain the ecosystem.

Generation 2: Extended and Mobile Identity



Short description	Allow private industry (e.g., mobile operators) to act as Identity Providers and attest identities (and possible official quality/capacity), subject to the necessary standards and specifications so as to maintain the level of trustworthiness and quality of a European eID system.
Service offering	Service Providers and citizens can benefit from authentication services offered by additional private sector Identity Providers (e.g., due to the entrance of mobile operators as identity providers or due to identity providers that attest to a person’s quality).
Governance Requirements	The governance requirements will be based on the first generation. However, given that this second generation will integrate private industry as Identity Providers, a strong legal basis (e.g., Directive) should be in place. To be able to validate the practices used by Identity Providers, an European eID accreditation scheme should be defined.
Architecture Requirements	The system will need to come closer to widely accepted and open standards and evolutions in the mobile world as to facilitate easy integration of these identity providers into the system and better protect the privacy of the user.
Operational Requirements	The private industry Identity Providers integration will need to be closely guided and followed. The service and security management will also need to be of high standards as the paying commercial identity providers will now depend on it for delivery of their services.
Costs and financing	To deal with the additional costs of integrating private sector Identity Providers and keeping the system sustainable, a membership fee could be introduced to connect private sector Identity Providers. This membership fee could be a flat fee or a variable fee based on the number of logins processed by the system.

Generation 3: Enhanced eID system



Short description	Mature European eID system
Service offering	A full scale European cross-border Identification and Authentication platform which also supports allowing service providers to obtain (complex) additional information about an asserted identity (for example: is this natural person the managing director of company X and authorized to sign contract Y, is the party allowed to approved transfer above an amount X, ...).
Governance Requirements	Additional effort will be required to ensure that the taxonomy and semantics remain under control and that attribute providers comply with the EU eID standards, quality and accreditation requirements. As with the introduction of private industry Identity Providers, an accreditation scheme for Attribute Providers will also have to be created.
Architecture Requirements	The architecture becomes more complex as attribute providers come into play. One might want to control the access to information of certain attribute providers by certain relying parties. Here one moves into areas which are not 100% understood at the current time and which are closely linked to initiatives with regard to base registries.
Operational Requirements	The introduction of the Attribute Services adds to the effort that will be required to ensure the operational effectiveness of the system. The support of attribute services will need to be managed on the service level. Cookbooks, code samples and training will need to be available.
Costs and financing	To cover the additional cost introduced by the attribute services, one could e.g., introduce a membership fee for attribute providers or one could introduce a fee per requested attribute.

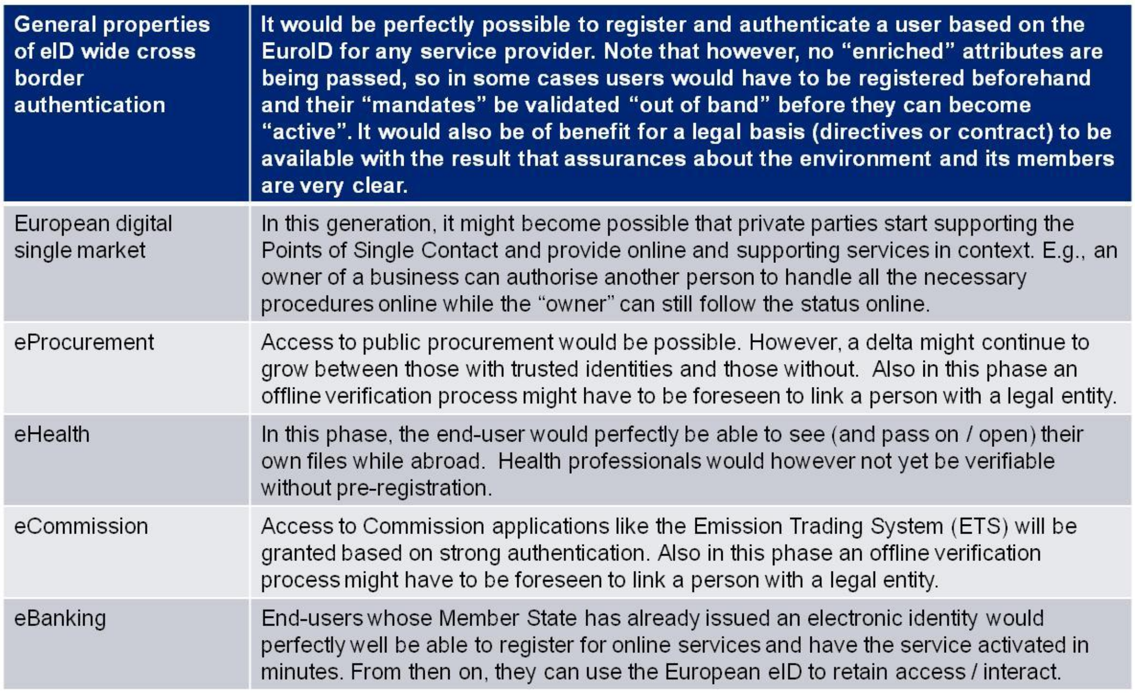
5. ANNEX 2 – ILLUSTRATION OF APPLICATION

This annex contains an illustration of the application of each of the four generations of the roadmap that are suggested. The examples proposed are four distinct services: a public procurement service provision scheme; a health-related scheme (basic patient summaries and ePrescription), an electronic authentication system, and a banking system.

Generation 0: Extended Stork Pilot

General properties of Operational Stork Pilot	In this generation, it would be perfectly possible to register and authenticate a user based on STORK. However, it needs to be noted that there is not yet a concerted system for creating cross-national identifiers, so a public procurement service provider would need to build one itself based on the assertion it receives. Also, no "enriched" attributes are being passed so users would have to be registered beforehand and their "mandates" be validated "out of band" before they can become "active".
European digital single market	Citizens to whom a Member State already has issued an electronic identity will be able to access cross-border services in the Member State which has placed transaction procedures online on its Point of Single Contact and have it "STORK-enabled". A delta may occur between member states with an eID, those with a "STORK-enabled" PSC and the others.
eProcurement	Access to public procurement would be possible, however a delta might grow between those with trusted identities and those without. Also an offline validation process might have to be foreseen to link a person with a legal entity.
eHealth	The citizens would perfectly be able to see (and pass on / open) their own files while abroad. Citizens will be able to identify themselves strongly towards systems holding patient information related to themselves, e.g. Basic patient summaries and ePrescriptions
eCommission	The Commission Authentication system (ECAS) will be able to authenticate users from the participating Member States based on their national eID tokens. Information about the authentication level is available for the relevant Commission applications themselves.
eBanking	N/A (non government controlled service – no clear guarantee with regard to privacy / trust / reliability).

Generation 1: Cross-border trust(ed authentication)



General properties of eID wide cross border authentication	It would be perfectly possible to register and authenticate a user based on the EuroID for any service provider. Note that however, no "enriched" attributes are being passed, so in some cases users would have to be registered beforehand and their "mandates" be validated "out of band" before they can become "active". It would also be of benefit for a legal basis (directives or contract) to be available with the result that assurances about the environment and its members are very clear.
European digital single market	In this generation, it might become possible that private parties start supporting the Points of Single Contact and provide online and supporting services in context. E.g., an owner of a business can authorise another person to handle all the necessary procedures online while the "owner" can still follow the status online.
eProcurement	Access to public procurement would be possible. However, a delta might continue to grow between those with trusted identities and those without. Also in this phase an offline verification process might have to be foreseen to link a person with a legal entity.
eHealth	In this phase, the end-user would perfectly be able to see (and pass on / open) their own files while abroad. Health professionals would however not yet be verifiable without pre-registration.
eCommission	Access to Commission applications like the Emission Trading System (ETS) will be granted based on strong authentication. Also in this phase an offline verification process might have to be foreseen to link a person with a legal entity.
eBanking	End-users whose Member State has already issued an electronic identity would perfectly well be able to register for online services and have the service activated in minutes. From then on, they can use the European eID to retain access / interact.

Generation 2: Extended and Mobile Identity

General properties of Extended and Mobile Identity	**With the availability of additional identity information (official quality / capacity), registration in or access to online cross-border online services could be further simplified as information with regard to quality/capacity could be embedded in the electronic identity. Also, with the coming of mobile identities, new mobile online services could emerge.**
European digital single market	In this generation, every citizen in Europe will be able to obtain a trusted electronic identity and access the Points of Single Contact The potential availability of the quality/capacity of the user in the identity can speed up the procedure. From the electronic identity, it will be clear in what capacity/quality (e.g., for which organization) this persons is acting.
eProcurement	From this generation on, it will be possible to bridge the digital divide as all persons will be able to have a digital identity and to access public procurement. Depending on the existence of quality/capacity information additional offline verification can be eliminated.
eHealth	In this phase, a health professional identity might emerge. Once established in a trusted way, subject to rigid privacy controls, health professionals could get access to patient data on a need-to-know basis.
eCommission	More sophisticated access to Commission applications integrating official quality/capacity and mobile possibilities. Depending on the existence of quality/capacity information additional offline verification can be eliminated
eBanking	This second generation will allow mobile banking to expand in a trusted way and link mobile-identities, online services, and online payments.

Generation 3: Enhanced eID system

General properties of Enhanced eID system	**Further optimization of processes will become possible as many elements needed in registration processes (mandate to act on behalf of a legal entity) or during the execution of transactions (entitled to submit tax-declaration) can be validated online.**
European digital single market	When accessing a PSC service, pre-registration or offline verification of additional elements is to a large extent no longer necessary. Persons will be able to access simple-procedures-online directly and act on behalf of their organisation.
eProcurement	When accessing a eProcurement service, pre-registration or offline verification of additional elements is to a large extent no longer necessary. Persons will be able to access simple-procedures-online directly and act on behalf of their organisation.
eHealth	Fine-grained access (eg difference between different types of healthcare workers and depending on special permissions or affiliation) to patient-information will become possible for health professionals as specific medical activities / certification become verifiable online.
eCommission	The possibility to conduct procedures on behalf of another organisation towards the commission.
eBanking	Banks might share the financial celings or limits of a customer with service providers or other information which will enable or prohibit access to additional services.

6. ANNEX 3 – BUSINESS CASES

6.1 INTRODUCTION

Online service providers in the private and public sector (that are also called Relying Parties in the context of eID) stand to gain from the use of trusted eID in the development of their online services. Once private actors can begin to rely on an existing means of trusted eID, they can focus on their core business and provide higher value-added services to their customers. Their ability to carry the trust mark of a trusted and secure European eID platform would bring an advantage in terms of the trust shown to them by their customers when they use their online services. The use of cross-border interoperable eIDs can also open up new markets.

This argument is especially valid for the online sales of those products and services for which a proof of identity is generally required. This is particularly important for financial services (e.g. banks and insurance schemes), and telecom and other products and services (e.g. healthcare services). For example, banks that sell banking products (e.g. a bank account or a loan) are often required by law to verify the identity of the person *in person* when the sale is made. In practice, this limits the sales channel to a network of local offices instead of selling online. Being able to sell such products online would not only make the sales process easier, but it would open up new business opportunities and essentially enable the availability of a potential market to all citizens and businesses that have a recognised eID.

This argument could be extended to other similar services. A further assessment of the types of services that could be sold online based on eID could be made in the future. Indeed, "the services sector now generates 74% of gross value added and employs 70% of the workforce in the EU. That is why it makes sense to give serious consideration to how this potential can be tapped via the internet across national borders within the internal European market" (eIDS in Europe, 2010).

In order for eIDs to support the establishment of cross-border financial services within the Internal Market the legal stipulations and standard business practices should be harmonised" (eIDS in Europe, 2010). Indeed, legal requirements and limitations that reduce the potential of eIDs in different sectors should be considered and where possible or necessary revised in order to reap the benefits of eIDs within the internal market.

For any relying party, the ease with which it can connect its online services to eIDs is essential. The multitude of legacy systems that are used by the different online service providers for their services to function should not need to be adapted, rather they should be easily hooked-up to the eID system.

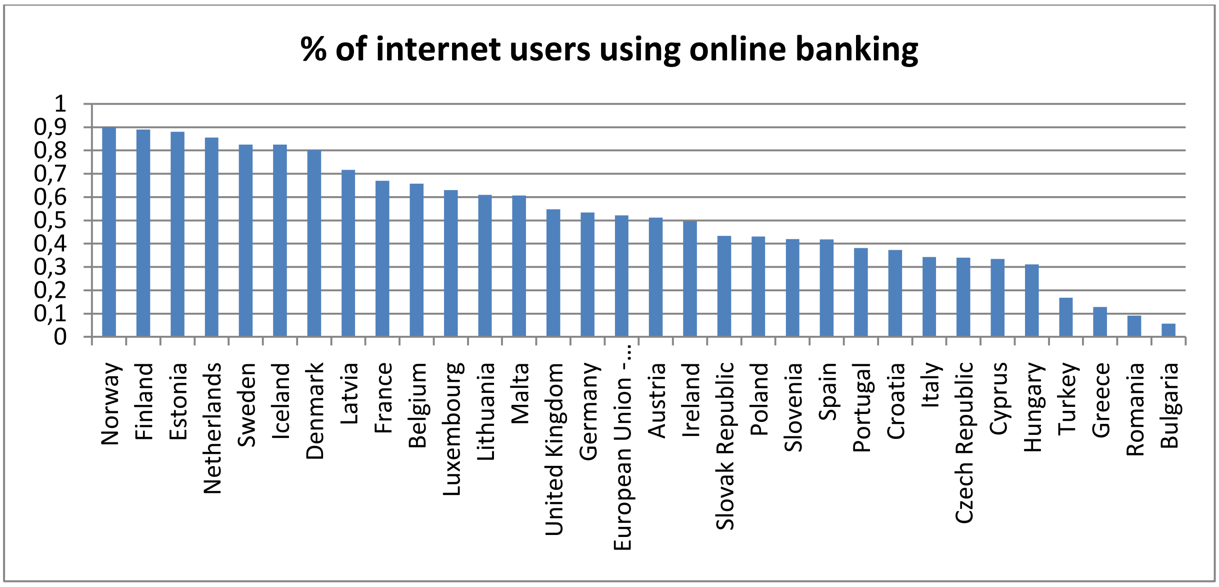
The sections below provide a closer look into the potential for eID in the banking sector and the telecom sector. Banks and telecom providers can play a role as identity providers as well as Relying Parties. This could result in a number of important benefits and added-value for them.

6.2 BANKS AS PRIVATE SECTOR IDENTITY PROVIDERS AND RELYING PARTIES

Online banking is becoming more and more common place in Europe, the adoption of online banking is particularly strong in Northern European countries (Denmark, Estonia, Iceland, Finland, Norway, Sweden, the Netherlands), where more than 80% of internet users use online banking. These 'Northern enthusiast' (as they are called in a recent report by Deutsche Bank) are followed by the adoption of online banking between 50-72% in 9 Member States (Austria, Belgium, France, Germany, Latvia, Lithuania, Luxembourg, Malta, and the UK) (also referred to as the 'European core'). Take-up in most Southern and Eastern European countries the is lagging behind at a level between 30-45%

(see **Error! Reference source not found.** 4 below), with a remaining three Member States below 3% (Bulgaria, Greece and Romania).

Figure 4: Adoption of online-banking in Europe[13]



The most well known example of high level security eID schemes are those implemented by banks for access to their online eBanking services. Most banks that offer such services provide card-readers to their clients that identify the client to their system by generating codes specific to the individual. Other channels may also be used such as text messaging or other types of non-card tokens such as One-Time-Passwords (OTPs).

On the whole the penetration of online banking in Europe differs per country, the EU average stands at 52,1%. A recent report by Deutsche Bank expects growth particularly in Southern and Eastern European countries, resulting in an estimated 60% of European banking online by 2020 (Online banking and research: the state of play in 2010, 2010). That makes about 430 million users in the European Union (based on the 2010 EU-27 population).

There are a number of countries where eIDs issued by banks for online banking are also accepted by government for eGovernment services:

- In Austria, the Citizen Card (Bürgerkarte) allows for different types of cards to be used for eGovernment services, these include bank cards as well as other cards (e.g. a health insurance card, a professional person's cards, a public official's service cards, and student services cards);
- In a number of Member States, banks are involved in providing non-PKI based eID services: e.g. the Finnish Bankers' Association provides an authentication service; Estonian banks; nine commercial banks in Lithuania; and BankID in Sweden:
  - BankID: this leading eID is based in Sweden. With a market share of 75%, it was developed by nine banks in a consortium, the telecom company TeliaSonera and the computer company Steria for use by members, authorities and companies. Services that rely on this eID include services in the private sector (banks and companies) as well as national government and municipalities e.g., eBanking, eTrade, online tax declaration. BankID is made available in the form of a smartcard, soft certificate and on mobile phones (Toby, Elliott, Hoikkanen, Maghiros, & Lusoli, 2010);
  - TUPAS: the paper-based TUPAS token (PIN-TAN) is issued to eBanking customers by their bank (all Finnish banks are obliged to authenticate their users) and is used by both

[13] Source: European Commission: Digital Agenda Scoreboard

natural persons and businesses in nearly all eGovernment applications that rely on this token for authentication of users alongside the Finnish eID card (FINEID);
- In Estonia, in internet banking the most used eID is eBanking eID, Estonian banks provide authentication services to third parties including eGovernment systems, an estimated 90% of eGovernment services relies on their authentication services;
- In Lithuania, eBanking authentication services are used in the Government Electronic Gates portal and in a number of separate eGovernment applications.
- LuxTrust S.A. is a certification authority established by the Luxembourg government and the Luxembourg Chambers of Commerce as well as major private sector players, (particularly the financial sector, banks) and other public entities.

Given the expected growth in the use of eID for online banking, these users could be an important user base for a European federated eID system particularly if eBanking eIDs become more and more accepted by governments and other third parties.

For private banks to act as an identity provider can be an important advantage for them. Offering eIDs is not only an additional service that offers them a competitive advantage, it is also a means of keeping loyal clients. The example of BankID in Sweden provides an interesting case. The Nordea bank has recently decided to join the BankID infrastructure, offering its online banking service based on common BankID certificates through shared technology in a shared environment. There are several reasons why banks such as Nordea decide to work together:

- **Cost**: the costs of development of the secure BankID were shared among banks, and therefore lowered the cost for each member;
- **Focus on core business**: the business of the bank is in banking and selling financial instruments not on dealing with technology, eID management and PKIs. By outsourcing these activities to the central BankID, organisations' banks can focus on their core business;
- **Reduce risk and need for support**: the risk of security threats is reduced in the shared BankID environment and is dealt with centrally. In addition, the support to clients is provided centrally;
- **Security**: BankID offers the same infrastructure to different banks and therefore harmonises the security standards provided to the client;
- **Business opportunities**: the added value for the banking sector is that the BankID can be used between banks (i.e. a customer of one bank can identify him/herself to another bank by using just one bank card). This provides opportunities for banks to compete on single financial products without requiring customers to switch from one bank to the other entirely. This makes competition easier and allows banks to position themselves much better for online sales of financial products by being able to rely on the certainty of the identity of the customer through BankID.

These business opportunities provide an important added-value for banks as they often cannot offer their full range of products online due to the obligation to validate a person’s identity, e.g. to open a bank account, proof of identity and the physical presence of the customer are often required. Indeed, “to date, it has been effectively impossible to ‘buy’ financial products via the internet, as identifying oneself is compulsory” (eIDS in Europe, 2010). This essentially limits the expansion of banks, unless they open up local branches. Being able to rely on European eIDs as a proof of identity, could mean that banks could offer a range of products online throughout the European Union; “machine-readable identification documents and digital signatures has the potential to overcome this hurdle” (eIDS in Europe, 2010).

In order for eIDs to support the establishment of cross-border financial services in the Internal Market “the legal stipulations and standard business practices when an account is opened would also have to be harmonised” (eIDS in Europe, 2010).

6.3 MOBILE OPERATORS AS IDENTITY PROVIDERS AND RELYING PARTIES

The use of mobile phones for authentication for eGovernment services is established in some form in eight countries (Austria, Estonia, Lithuania, the Netherlands, Norway, Poland, Slovenia and Turkey). In only two of these countries (the Netherlands and Norway) are these intended for the use of multi-factor authentication. In the other countries, they are primarily used as signature solutions. Mobile operators are involved in providing eID on mobile phones. In Finland, three mobile phone operators (DNA, Elisa, and Suo Neila) offer eID services. In Estonia, the Mobiil-ID is provided by three telecom operators (Elisa, EMT and Tele2).

Telecom providers who can offer eID services on mobile phones stand to gain a competitive advantage by providing their clients with the ability to use eID-based services on their mobile phone. Thus, they offer their customers more possibilities in terms of the use of their mobile device.

This can also be a strategy for keeping customers. By building eID into the SIM-card, customers can make use of online services based on eID directly from their mobile phone. Indeed, telecom operators offer mobile identity services to "attract high value contents for financial services and reduce customer churn".[14] For most telecom operators, however, there is an important requirement for them to reap the benefits of investing in offering mobile eIDs. Online services that make use of eID should be sufficiently available and frequently used, particularly given the necessary investment they need to make in providing the appropriate SIM-cards to their customers.

The Estonian Mobiil-ID can now be used to login to a number of online services:

- **DigiDoc Portal**: available for Estonian ID-card and Estonian and Lithuanian Mobile-ID users and allows digital signing, verification of validity of digital signatures, forwarding documents to other users of the Portal and receiving documents from other users of the Portal;
- **Citizen's portal**: a portal where citizens can find information about various areas of everyday life and access useful e-services (e.g. e-Tax, application for child-care allowance, land registry application);
- **e-Tax**: application for online tax declaration;
- **Online banking**: online banking applications for different banks (e.g. Swedbank, SEB);
- **EMT self-service**: the self-service of the EMT telecom operator.

Providing eID on mobile devices also opens up new business opportunities for telecom providers. The huge popularity of mobile phones (125 mobile subscriptions per 100 inhabitants in the EU 27)[15] has resulted in the use of mobile devices for payments. For telecom operators "the benefits of mobile payments include increased volumes of chargeable data communication and improved attractiveness of the subscription, in addition, they can provide value-added services by acting as payment mediators" (HYPPÖNEN, 2009).

On the other hand, similar to the banking sector, in many cases telecom providers are required to ask for proof of identity to sell their products or services (e.g. a new subscription requires proof of identity). Being able to rely on an reliable eID system (whether provided on the mobile phone or otherwise) allows telecom providers to sell their products and services more easily online.

[14] Financial Services Technology, FST, http://www.fsteurope.com/article/European-e-ID-Services-future-trends-and-Nordic-experiences/

[15] Possession of mobile phones lies at more than 100 since individuals may have more than one mobile phone subscription. Source: Eurostat

The majority of countries (21 out of 32 countries) there is no need for a form of identification and authentication on mobile phones. This is important since this essentially limits the use of the eID for online services; services offered on mobile phone platforms may not be able to rely on eID. An important aspect of using mobile phones for eIdentification and eAuthentication is that the registration process of mobile phone operators is not always considered trustworthy enough. This results in cases where the mobile eID is confirmed using the national eID on activation. (Study on eID Interoperability for PEGS: Update of Country Profiles, 2009)

7. ANNEX 4 - VALUE ADDED SERVICES

There are a number of "basic/fundamental" services that a European federated eID system can supply. An indication of the level of importance that a service would provide for each stakeholder is explained in the table below:

Table 3: Value added services

	End-Users	Relying Parties	Identity / Attribute Providers	Industry / Solution Providers
Part of a widely accepted, legally certain and user-friendly European Federated eID System	Must	Must	Must	Must
European Federated eID System accredited and privacy protecting eIdentity-eco-system	Should	Could	Should	Nice
European Federated eID System accredited (and privacy protected) eIdentity attribute services	Should	Could	Could	Nice
Standardised and standards-based integration within a trusted European eco-system		Must	Must	Must
Assertions according to clearly established criteria		Must	Must	Should
Membership-administration and TrustList-maintenance (Security Management)	Must	Should	Must	Should
Service Level Management, as well as Certificate Management Services		Should	Must	
Ability to receive a European Federated eID System-conformity seal	Could	Nice	Must	Must
European Federated eID System-Stakeholder Board membership		Could	Could	Could

* Must Have, Should Have, Could Have, Nice-to-have

In the next section the services are developed in detail.

- A first service to be supplied to its members is to be **part of a widely accepted, legally certain and user-friendly branded European federated eID system.** A intangible yet fundamental service of a European Federated eID System is its **brand**. A key critical success factor is the acceptance of the eco-system by the end-user. When the eID-ecosystem becomes known, end-users will obtain a brand that they recognise and dare to use. A core service for a European Federated eID System would be to ensure the trustworthiness-level of the relying parties, the identity and attribute providers, and the trustworthiness of related solutions. In this context, a key element that should emerge is the availability of European Federated eID System-credentials and European Federated eID System-compliant devices which are omnipresent, easy-to-use and whose reputation and trust-level is beyond doubt for the end-user.

- A second service should be **a European Federated accredited and privacy-protecting eIdentity-eco-system**. A key service of the European Federated eID System- would be the existence of a consistent, trustworthy and privacy-protecting authentication and identification system which would be usable with both personal computers and mobile devices. The target is to offer the end-user a consistent experience by which they can "authenticate" at a reliable identity provider and get access to a service provider with the asserted identity. They can easily themselves control which data and attributes are shared with the relying parties so that their privacy is well protected (and under their own control).

A third service should be the future existence of **European accredited (and privacy protecting) attribute services**. An optional, yet very valuable, service that should be added to the European Federated eID System, on top of pure “identification”, is the extension of the eco-system with attribute services supplied by trusted third parties that adhere to European Federated eID System-criteria. These could attest to certain attributes, criteria and mandates for the end-user (which might be necessary to be able to access certain services). This would allow relying parties to provide more focussed services without the burden of having themselves to register and manage specific user-attributes or characteristics[16].

- A fourth service should be the ability to **integrate with a standardised and standards-based trusted and secured European eco-system** A clearly tangible service of a European Federated eID System would be its ability to offer a standardised interface for identity or attribute providers and relying parties to connect and become part of an European-wide identity ecosystem. Such standardisation will give identity or attribute providers and relying parties clear instructions on how to come on board, how to handle identity assertions, and indicate what the legal or trust implications are for them when asserting or consuming identities and attributes in this ecosystem. A European trusted ecosystem will simplify the technical burden and the legal or liability concerns that players face when they want to deliver services across Europe.

- A fifth service that the European Federated eID Systemshould supply to its members is the availability of identity and/or attribute **assertions according to clearly established criteria**. Once connected to the ecosystem, relying parties will receive standardised assertions which are not only clear about their technical characteristics but also with regard to the way in which the data can be consumed (both in respect of the data and the assurance levels). By connecting to a European trusted ecosystem, the technical burden would be reduced as would also be the liability concerns that service providers face when they want to include a large number of persons especially if this is across Europe.

[16] It will be essential that the user is informed of the attributes that would be made available from the attribute services to the relying parties, and that explicit consent is required.

- A sixth service that the European Federated eID Systemshould supply to its members is strict **Membership administration and TrustList maintenance (Security Management)**. A key success factor for the ecosystem would be the reliable administration of the members and the registration, activation, suspension, and revocation of “memberships/connections”. This would be greatly facilitated by a central “ecosystem trust centre” which administers these “memberships/connections”. The parties involved could be assured that members of the ecosystem adhere to the standards of the ecosystem and can be considered trustworthy.

- A seventh service that the European Federated eID Systemshould supply to its members is **Service Level Management and Certificate Management Services**. An important element to guarantee the memberships/connections between identity/attribute providers and/or relying parties and the working eco-system would be the support of the (technical) security aspects of those “memberships/connections”. This would be greatly facilitated by a central “eco-system trust-centre” which provides the necessary cryptographic certificates to the players. A central TrustCentre would ensure that trusted parties can be off-boarded and disconnected at all times if needed.

- An eight service that the European Federated eID Systemshould supply to its members is the **ability to receive a conformity seal**. When organisations want to hook up to a European Federated eID System it would be important for them to find solutions in the market which are compatible. Thus, their integration effort could be limited to a minimum. When end-users are seeking a device to allow them to be authenticated in the European Federated eID System-space they will look for a European Federated eID System-stamp on the device they wish to buy. A conformity seal would therefore be seriously advantageous for any vendor or solution provider wanting to sell its products or solution to the market.

- A ninth service that the European Federated eID Systemshould supply to its members is **membership of a Stakeholder Board**. It would be highly recommended to give end-users, relying parties, identity providers and solution providers a means through which they can provide input to the governance board of European Federated eID System. Through this board, they could raise concerns and bring forward items which might further facilitate or speed up the launch of new services. An overly centrally-driven ecosystem might not foresee certain requirements or new possibilities that can be offered by relying parties, identity providers or solution providers. Therefore, it is crucial to involve these stakeholders on a regular basis to assess the system and to determine the specifications of a next generation of the eID ecosystem.

8. ANNEX 5 – STORK DESCRIPTION AND LESSONS LEARNED

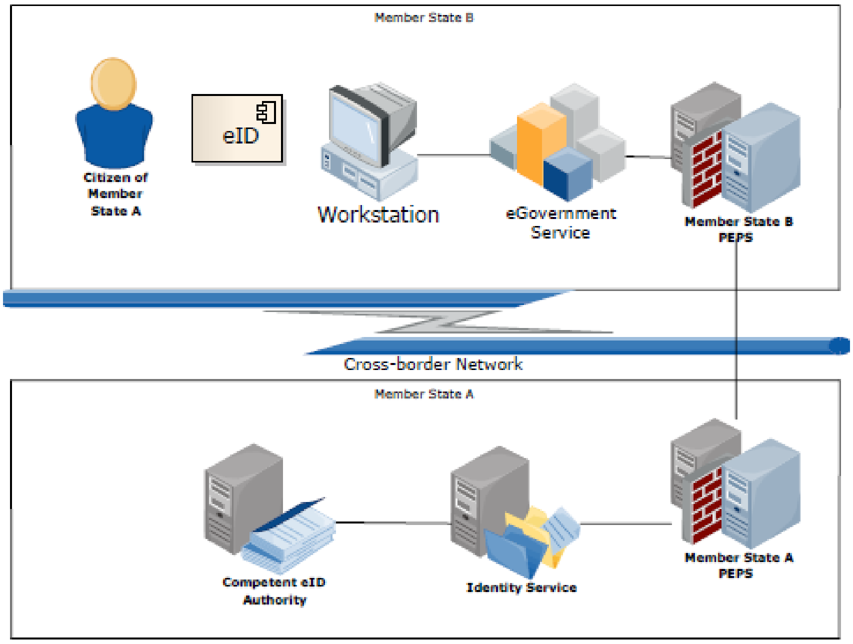
This annex contains a description of the STORK large-scale pilot, how it was established, what its main strengths and weaknesses are still has to be established to achieve a European Federated eID system.

8.1 STORK OVERALL DESCRIPTION

8.1.1 Objectives and Main Results

In 2008, the European Commission launched the CIP ICT PSP Large-Scale Project for the establishment of a European eID Interoperability Platform named STORK (Secure identiTy acrOss boRders linKed). The basic principle underlying STORK is that existing identification and authentication systems in the Member States can be linked through an EU-wide eID management (eIDM) platform, leaving intact the national approach to identification and authentication (see figure 5).[17]

Figure 5: Cross border eID Authentication (Hartmann & Körting, 2010)



The STORK project runs until halfway through 2011.[18] It has delivered a number of key building blocks in order to achieve a piloted eID platform that operates across borders. The key building blocks of STORK include:

- Common specifications: minimum requirements on legal, organisational and technical matters have been defined to establish a cross-border authentication platform between participating Member States. This resulted in an architecture based on an interoperable Pan European Proxy Service, middleware models and various other materials on non-technical

[17] Figure 5 pictures the PEPS architectural model. In addition to it, STORK also integrates the architectural middle-ware model.

[18] An extension in time until December 2011 is under approval process by the European Commission.

issues. These non-technical issues are currently not yet all resolved[19]. Examples include national legislation on national identifiers and a legal basis for cross-border identification/authentication.

- Quality Authentication Assurance (QAA) levels: eID and authentication credentials, registration and lifecycle processes have been defined on the level of the Member States' identity providers: they depend on the issuer of the electronic identity. As a result, there is a variety of policies and procedures used to identify and authenticate the establishment of credentials during the lifecycle management. To align this range of policies and procedures, QAA levels were defined. These permit a common interpretation of the different identity and authentication credential policies and procedures.

- Common code: to facilitate the integration of identity providers and service providers i.e., those who are the main parties who deliver services in an online system, a common code was created by STORK. It eases the integration of the providers and creates interoperability between connected parties. This common code was provided to STORK participants so as to achieve a certain level of integration. It will also be provided to the STORK Sustainability action financed by ISA that will maintain this common code after the project termination and will be made publicly available as open source.

- The STORK Pilots: a number of pilots were put into production: they demonstrate that such an environment can work in a user-friendly way. The six pilots are: Cross-Border Authentication for Electronic Services, Safer Chat, Student Mobility, Electronic Delivery, Change of Address and the European Commission Authentication System “ECAS” Integration.

8.1.2 Short description of the set-up

Detailed descriptions of STORK can be found in the pilot's reports and materials. Here, however, one of the possible scenarios or set-ups for a person trying to log in to a cross-border service is outlined[20].

[19] However, it must be noted as can be seen from the given examples that such matters were not for STORK to resolve.

[20] Source: D5.7.2_Functional_Design_for_PEPS_MW _models_and_interoperability Figure 5 pictures the STORK PEPS architectural model. STORK also integrates the architectural middle-ware model.

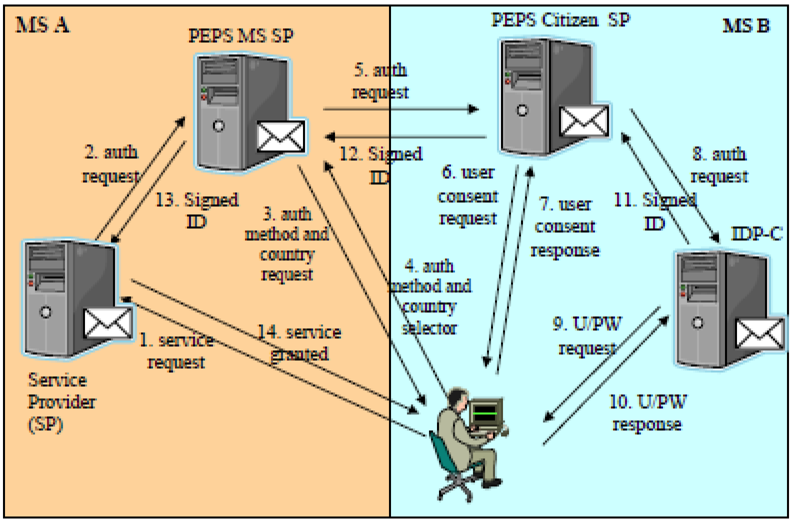
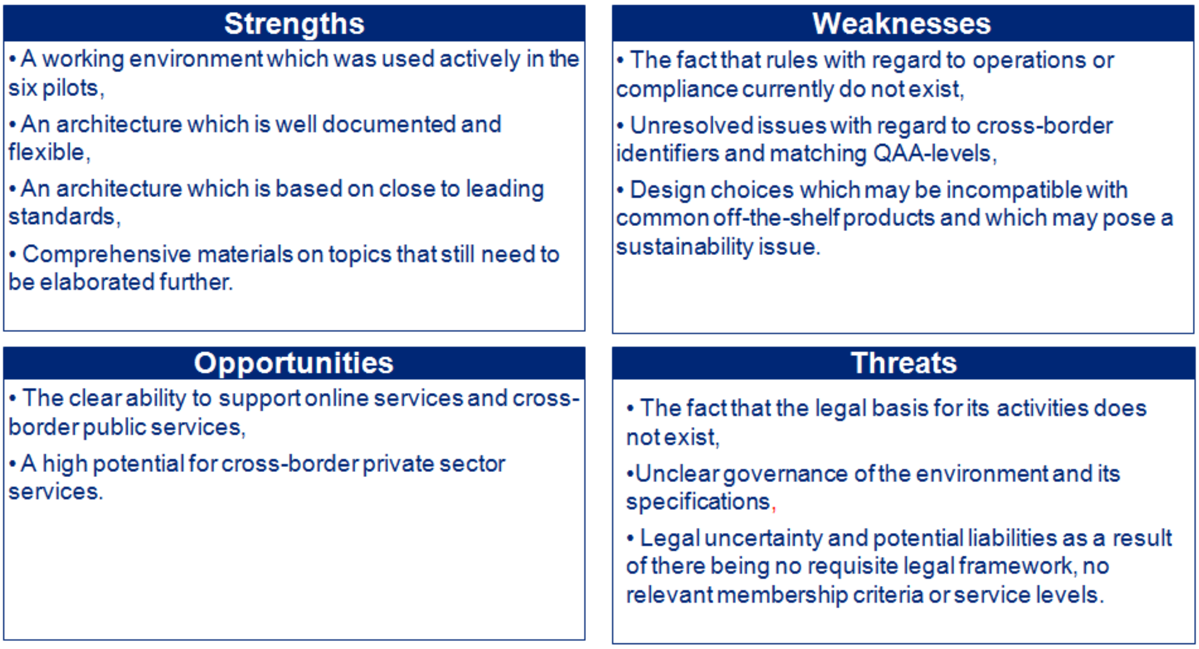


Figure 6: STORK workflow for eID transfer involving several STORK components.

8.1.3 A short SWOT analysis of STORK's achievements

As a pilot, STORK has accomplished a technical proof of concept for the creation of a cross-border European authentication platform. The figure below gives an overview of the strengths, weaknesses, opportunities and threats of the STORK large-scale pilot project. They describe especially those restrictions which limit it from being deployed as a European Federated eID system. It must be noted that the ‘Weaknesses’ should not be considered as failings of the STORK as a project as such, as the aim of the project was not to solve the legal framework and the rules with regard to operations or compliance that a Federated European eID System would need to follow, nor issues related to cross-border identifiers and QAA levels. They should be seen as existing gaps that must be overcome to move towards a Federated European eID System. These various elements are later described in detail.

Figure 7: SWOT analysis



Strengths

- A working environment which was used actively in the six pilots,
- An architecture which is well documented and flexible,
- An architecture which is based on close to leading standards,
- Comprehensive materials on topics that still need to be elaborated further.

Weaknesses

- The fact that rules with regard to operations or compliance currently do not exist,
- Unresolved issues with regard to cross-border identifiers and matching QAA-levels,
- Design choices which may be incompatible with common off-the-shelf products and which may pose a sustainability issue.

Opportunities

- The clear ability to support online services and cross-border public services,
- A high potential for cross-border private sector services.

Threats

- The fact that the legal basis for its activities does not exist,
- Unclear governance of the environment and its specifications,
- Legal uncertainty and potential liabilities as a result of there being no requisite legal framework, no relevant membership criteria or service levels.

STORK's main strengths can considered to be:

- A working environment which is used actively in the six pilots: the Stork large-scale pilot has been tested and has completed some very practical pilots. These are the Cross-Border Authentication for Electronic Services, Safer Chat, Student Mobility, Electronic Delivery, Change of Address and the European Commission Authentication System "ECAS" Integration.

- An architecture which is well documented and flexible: the documentation provided by STORK is very clear; the pilot has established an architecture into which Member States and other identity or attribute providers can hook in at any time that they want (or are ready), and into which service providers can link with a degree of flexibility.

- An architecture which is based on close to currently leading standards: STORK was developed at the same time-period that a number of standards were evolving so that, while the large-scale pilot's standards are not fully compliant with the latest evolutions in the market, its environment is quite close to widely accepted SAML2-standards/architectures.

- A comprehensive set of materials on topics that still need to be elaborated further: requirements on legal, organisational, technical matters and quality assurance levels have been defined. These act as a very good basis for further elaboration, standardisation and decision-taking.

The main weak points of STORK are:

- The fact that the legal basis for its activities and rules with regard to operations or compliance, do not currently exist: STORK was operating in an European context. Different national legislations exist within that European context and are not always aligned in the Member States. This implies that, in order to be legally compliant, STORK should adhere to national legislation (for example Member States' national privacy legislation or use of specific national identity numbers).

- Unresolved issues with regard to cross-border identifiers and matching QAA-levels. The QAA document is merely a project deliverable without an official policy status. Member States are not bound by the criteria established in the QAA model, nor is the mapping of eIDs to quality levels on the basis of this model in any way guaranteed to be correct or required to be accepted. Outside of the STORK pilot context, Member States are not required to use or apply the model in any way, nor are there any consequences in terms of liability if an eID has been incorrectly classified. In short: the QAA model operates acceptably within the STORK pilot, but has no basis for its general application outside of that context. Also although initial QAA levels have been defined, they need to be defined at a more detailed level of granularity between identity providers and service providers. This would ensure that the identity providers' QAA level matches the expectation of the service providers with regard to the user registration method, lifecycle processes and the strength of the authentication method / token used.

- Design choices which may be incompatible with common off-the-shelf products and which may pose a sustainability issue: Although industry standards were chosen for the implementation of the STORK pilot, the way these standards are used and implemented may mean that common off-the-shelf products cannot communicate and be integrated with the authentication platform.

The opportunities that exist when transforming STORK into a trusted European Federated eID System are considerable. They are:

- The clear ability to support online services and cross-border public services: With the rise of eGovernment services, a trusted cross-border European Federated eID System creates the opportunity to enlarge the offering of these services within the EU so that users (both private persons and legal entities) from one country can use their national eID to access eGovernment services in a foreign country.

- A high potential for cross-border private sector services: Not only eGovernment, but eCommerce in general can benefit from the existence of a trusted European Federated eID System. Service providers who have the opportunity to use a trusted platform which ensures the identity of their customers in a European context.

The main threats perceived which arise out of the STORK pilot and which need to be resolved, are:

- Unclear governance of the environment and its specifications: Today, STORK has been created as a technical platform that offers cross-border authentication services. When the vision is, rather, to create a trusted and high quality information services in a sustainable ecosystem, that future environment and the specifications that it uses to operate will need to be governed well to ensure its high level of trust and quality.

- Legal uncertainty and potential liabilities as a result of there being no requisite legal framework, no relevant membership criteria or required service levels: STORK and its successor pilot(s) will be created and perceived as the European trusted source for identity and authentication services of European citizens. As a result, service providers will rely on information provided through the STORK platform by trusted member parties to establish the identity of its users. However, it is the future European federated eID system, and not STORK –which is a LSP- or its successor pilot(s) that will need to be the trusted source. Within that system identity/attribute providers might be held liable for the information they provide to service providers. Hence, above all, legal and operational mechanisms and quality assurance will need to be present to ensure liability conditions are well established.

8.2 STORK LESSONS LEARNED

A number of lessons learned have emerged from the STORK experience. With regard to a European eID system in general, they can be classified as its trust and liability aspects; architectural aspects; operations and security aspects

For each of these elements, there is an in-depth exploration of its various sub-elements. For example, in terms of trust and liability, the following six sub-elements are listed and investigated: a trust and liability framework, a reliable and trusted system, solid eID registration and lifecycle management, solid credential registration and lifecycle management, clear user identifiers and cross-border identification, and a clear definition of capacities, qualities and mandates. For each sub-element, observations are made and their relevance is commented on.

8.2.1 Trust and liability aspects of an EID system

This section examines the key elements which form the foundation for any trusted Federated eID system. It assesses STORK's status with regard trust and liability. It offers both a general understanding of the importance of an understanding of the gaps still are to be overcome to attain a European Federated eID system.

Trust and liability framework

Observation

In the context of the STORK proof of concept, agreements with regard to trust and liabilities on a European level not fully elaborated. Such agreements needs to be put in place in order to identify clearly the trust and liability responsibilities of the parties involved and governed by a truly mandated body.

Relevance

Aspects like trust, liability and privacy play an essential role when it comes to the undisputed eIdentification and eAuthentication of end-users. A European Federated eID system will not be able flourish if no legal certainty exists.

Reliable and trusted system

Observation

The STORK project was defined as a technical proof of concept that offers the required technical infrastructure and functionality to enable cross-border authentication and integration of the different type of authentication mechanisms and tokens already used in the different Member States. STORK, however, does not involve the necessary trust, reliability or availability guarantees that would be needed if it were to form part of a production system.

Relevance

The following subjects should be part of any sustainable eIdentification and/or eAuthentication system: strategic, tactical and operational governance, the definition of a clear trust model, clear service levels, and clear security controls and baselines.

Solid eID registration and lifecycle management

Observation

Not only is the initial identity registration of a user’s electronic identity essential, but also any changes in information related to this electronic identity. Today, the electronic identity registration and lifecycle processes depend on the issuer of the electronic identity (whether it is government-issued, private sector-issued or self-issued). This creates a variety of policies and procedures used for electronic identity establishment in lifecycle management. Within STORK, an effort has been made to address this problem from the QAA-perspective.

Relevance

The level of trust allotted to an eID depends strongly on the kind of identity registration and lifecycle management policies and procedures used. STORK is dependent on these policies and procedures which, nevertheless, vary in terms of the function of the identity issuer. This also implies that the trustworthiness and reliability of any STORK-offered services are defined by factors which are external to the STORK services themselves. Therefore, there is a need for standardisation and provision of a minimum baseline.

Solid credential registration and lifecycle management

Observation

As with the electronic identity itself, credentials need to be subject to reliable lifecycle management to ensure trustworthy authentication. At the current time, every country and credential issuing party has its own credential lifecycle management procedures. These procedures are fundamental to the trust that can be allotted to the credential issued. Within STORK, an effort has been made to address this problem from the QAA-perspective.

Relevance

The level of trust given to an authentication credential varies depending on the registration and lifecycle policies and procedures applied to it. The credential issuer defines the applicable policies and procedures for registration and lifecycle management: hence, the level of trust in these authentication credentials varies. Since STORK makes use of these authentication credentials, STORK’s trustworthiness and reliability depends on the level of trust in the individual authentication credential providers. Therefore, there is a need for standardisation and provision of minimum baselines.

Clear user identifiers and cross-border identification

Observation

Citizens of the EU Member States are identified using different types of information. Within the European Union, no unique identification information exists and the national identifiers used in several Member States are often subject to national legislation and limitations.

Relevance

The ability to identify a person beyond any doubt is critical for a European eIdentification and eAuthentication platform. This requires an agreement on the minimum identification information or identifiers which could be used to enable such identification. Here, there is some standardisation work still to be executed.

Clear definition of capacities, qualities and mandates

Observation

In some countries, capacities, qualities and mandates information is becoming available in the national electronic identification platforms. Among others, Austria, Belgium and Spain are examples of such countries. These additional functionalities offer added-value to the platform and make it more interesting to use for the potential parties involved. The context of capacities, qualities and mandates is currently not addressed in every Member State and can therefore not be offered by the STORK services.

Relevance

Capacities, qualities and mandates are important pieces of information in context of online services. Moreover the concept of "context-aware identities" is becoming more and more accepted within the electronic identity community. Adding capacities, qualities and mandates to STORK functionality would provide an added-value which would strengthen the arguments for STORK's use.

8.2.2 *Architectural aspects of an EID system*

This section examines key elements with regard to the architecture and standardisation of any trusted Federated eID system. It assesses STORK's status in this regard so as to give the reader both a general understanding of the importance of architecture and standardisation and the gaps that still are to be overcome even at the end of the STORK large-scale pilot.

Reference architecture

Observation

STORK aimed to create interoperability between Member States' eIdentification and eAuthentication platforms. The local architectures of these Member States often use different approaches (both centralised and decentralised) to implement Identification and Authentication services. Member States are also free to use the technology and standards they desire to implement their Identification and Authentication services. This results in a multitude of technology and standards being used.

Relevance

Evolution has clearly shown that federated eID systems can work. Purely as examples, the Belgian federal authentication services and the STORK large-scale pilot illustrate the case clearly. It is, however, a key move to establish an enterprise architecture and a solution architecture that use fully open standards (following the general trends in the market). This would allow all parties to integrate easily into the system by using any open source or common off-the-shelf solution which adheres to these standards.

Standards and specifications

Observation

Easy and efficient interfaces to connect to eIdentification and eAuthentication services are recommended. These would allow interested parties to integrate their services easily with other environments such as STORK. In the six STORK pilot projects, some specification and testing was undertaken so as to facilitate the degree of integration with the STORK environment.

Relevance

The more standardised are the interfaces defined between STORK and the Member States, the easier it will become to integrate the STORK environment. It is, however, crucial to establish interfacing standards that use fully open standards (following general trends in the market) as to allow all parties to integrate easily into the system through the use of any open source or common off-the-shelf solution that also adhere to these generally accepted standards.

Consistent eID assertions

Observation

The STORK environment has aimed to be an open system in order to support multiple identity providers. In order to be able to interconnect service providers with these different identity providers, STORK developed the PEP/MW-model and standardised any assertions made between them. As the system evolves towards a European Federated eID system, the assertions exchanged (and the information in the assertions) might have to evolve.

Relevance

It is very important that the identity assertions exchanged are fully reliable and can be correctly interpreted by the relying parties. The assertions containing any information need to be sufficiently protected to ensure their integrity and authenticity and add to their trustworthiness.

Approved or standardised credentials

Observation

STORK allows considerable use of multiple types of credentials such as different national electronic identity cards. In most cases, these national eID cards require specific software to be installed on the client computer so as to be able to read the information stored on the cards and use of the card for authentication. **Although the study team makes this observation, it seems standardisation of the credentials itself to be out of scope of a federated system**

Relevance

The advantage of allowing different authentication credentials is that end-users can access available e-services from their usual environment and using known authentication credentials. The disadvantage of using multiple authentication credentials is that one nation's client systems might not be compatible with eID requirements in other countries. The software required for communicating with these authentication credentials is not available.

8.2.3 Operations and security aspects of an EID system

This section examines the key elements with regard to the operational and security aspects of any trusted Federated eID system. It assesses STORK’s status with regard to operational and security questions. It offers the reader a general understanding of the importance of these issues and an understanding of the gaps that still are to be overcome following the completion in mid-2011 of the first STORK large-scale pilot.

Minimum security requirements

Observation

The level of trust that can be placed in the STORK environment, and the assertions it produces, depends strongly on the level of trust and security of the local eIdentification and eAuthentication services provided by the Member States. The trustworthiness of any system is determined by its weakest link. A breach in a single link can pollute or damage the wider reputation of the entire and the whole ecosystem. In the case of STORK, this implies that STORK is dependent on individual Member States' security requirements for its more general level of trust and security.

Relevance

eIdentification and eAuthentication services should be considered as secure services. This security can only be assured if these services comply with minimum security requirements or some sort of security baseline. It is therefore highly recommended to introduce some sort of security baseline for all the parties involved in a European Federated eID system.

Reliable service levels and communications

Observation

STORK is the interoperability platform between several national identity providers that offer eIdentification and eAuthentication services. Relying parties depend on the Identification and Authentication assertions offered by the STORK platform. This means that, on the one hand, an agreement between STORK and the identity providers and, on the other hand, STORK and the relying parties needs to be made and the service level agreements to be respected. At the current time, there are however no clear service level agreements.