COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME
ICT PSP Fifth Call for proposals 2011 - Pilot Type A

Towards a single European electronic identification and authentication area

ICT PSP call identifier: CIP-ICT-PSP-2011-5
ICT PSP Theme/objective identifier: 4.2

Project acronym: STORK 2.0
Project full title: Secure idenTity acrOss boRders linKed 2.0
Grant agreement no.: 297263

D5.3.5 eGov4Business Pilot Final Report

Deliverable Id :	**D5.3.5**
Deliverable Name :	**eGov4Business Pilot Final Report**
Status :	**Final**
Dissemination Level :	**PU**
Due date of deliverable :	**September 30th, 2015**
Actual submission date :	**November 6th, 2015**
Work Package :	**WP5.3**
Organization name of lead contractor for this deliverable :	**IC**
Author(s):	**H. Leitold, B. Suzic, P. Saartee, V. Kalogirou, S. Tsiafoulis, R. Rán Samper, P. Fabbrizi, D. Mitzman, H. van der Burght, I. Vennekens, ATOS**
Partner(s) contributing :	**All eGov4Business Pilot partners**

Abstract: This deliverable reports the results of the STORK 2.0 eGov4Business piloting activities. The achievements have been measured and evaluated with an eye towards planning the sustainability of future service provision, deployment and development. In spite of delays in the launch of services and limitations in piloted functionalities, significant positive benefits were achieved. An in-depth gap analysis comparing expectations with realised benefits was performed and is summarised, here, along with a reporting of lessons learned to pass on to future adopters.

Project co-funded by the European Community under the ICT Policy Support Programme

History

Version	*Date*	*Modification reason*	*Modified by*
0.1	12/08/2015	Initial draft	Chapter editors
0.2	20/08/2015	Consolidated and commented Initial Draft	David Mitzman, ATOS
0.3	05/09/2015	Second draft	Chapter editors
0.4	14/09/2015	Updated feedback form metrics, lessons learned	David Mitzman, ATOS
0.5	28/09/2015	Updated SP Questionnaire metrics, costs/benefits analyses, graphs	All partners, ATOS
0.6	15/10/2015	Redacting of final contributions from partners	David Mitzman, ATOS
0.7	30/10/2015	Final Draft	David Mitzman,
0.8	4/11/2015	Revised Final Draft based on ATOS comments	David Mitzman, ATOS
0.9	6/11/2015	Quality check	ATOS
1.0	6/11/2015	Revised version after quality check	ATOS
1.1	6/11/2015	Final quality check	ATOS
Final	6/11/2015	Final deliverable	

Table of contents

List of figures

List of tables

List of abbreviations

AP	Attribute Provider
AQAA	Attribute Quality Authentication Assurance
AU or AuthN	Basic personal authentication
AUB	Authentication on behalf of (a legal person)
B-IDP	Business Register
BRIS	Business Register Interconnection System
CEF	Connecting Europe Facility
e-CODEX	e-Justice Communication via Online Data Exchange
EBR	European Business Register
ECRF	European Commerce Register Forum
eGov4Business Pilot	Public Services for Business Pilot (of STORK 2.0)
eID	Electronic Identity
epSOS	Smart Open Services for European Patients
IDP	Identity Provider
LSP	Large Scale Pilot
MoU	Memorandum Of Understanding
MS	STORK 2.0 Member State
MW	MiddleWare
PEPPOL	Pan-European Public Procurement Online
PEPS	Pan European Proxy Server
PSC	Point of Single Contact
PV	Powers Validation
QAA	Quality Authentication Assurance
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SME	Small & Medium Enterprise
SP	Service Provider
SPOCS	Simple Procedures Online for Cross- Border Services
SSO	Single Sign-on
STORK 2.0	Secure idenTity acrOss boRders linKed 2.0
V-IDP	Virtual Identity Provider

Executive summary

This Final Report relates the results achieved by the STORK 2.0 Public Services for Business Pilot ("eGov4Business pilot") during the last twelve months of running phase activities. The results consolidate the project-long experiences in integrating existing eGovernment services for businesses with the STORK 2.0 cross-border authentication infrastructure in order to allow foreign businesspersons to access the eGovernment services as easily as do domestic users. Since we are dealing with services for businesses, the STORK 2.0 interoperability infrastructure not only helps the businesspersons identify themselves using their national electronic identity (eID) system, but it also actively assists them in retrieving valid credentials to act on behalf of a company registered in a foreign country. The Service Provider receives the credentials, via STORK 2.0, in machine-processable format, and can immediately determine whether or not to grant the businessperson access to the requested service.

The achievements of the Pilot have been carefully measured and evaluated using metrics established in the course of the project to capture benefits in four different categories: Use, Business Value, Learning and Adoption. Input to the metrics came from end-users, Service Providers, Member State representatives and the STORK 2.0 server logs. The periodic application of the metrics helped focus the pilot's efforts on those activities which maximised benefits to stakeholders and created the best premise for the future sustainability of project results. The structure of this report reflects these four categories, and achievements and the related metrics are reported accordingly.

Ten of the thirteen Member State (MS) partners participating in the Pilot succeeded in "Going Live" by bringing into real, production environments their existing online eGovernment Services for Businesses adapted to and integrated with the STORK 2.0 infrastructure.. Examples of such services were official sectorial registers, national business registers and also eGovernment portals such as one-stop shop Business Services Portals and Points of Single Contact (PSCs) created by the EC Services Directive. These ten Service Providers (SPs) successfully tested with real end-users the STORK 2.0-enabled, cross-border authentication service. Six of the ten piloting SPs integrated the full "Authentication on behalf of a company" process, and this was validated by businesspersons from eight different MS. This is truly a first in European interoperability in eGovernment and Business Register services.

Delays in the deployment of some MS infrastructures as well as in the implementation of some SPs caused four of the SPs to "Go Live" in the last six months of piloting, and limited to some extent the total amount of effective piloting. However, in spite of delays, significant piloting was performed and positive benefits were achieved. Over the course of piloting about 300 real end-users accessed the official eGovernment services of other countries, and registered close to 1,000 successful transactions. Documented benefits to businesspersons included:

- easier access to information and procedures across borders through quicker and easier logon process,
- reduced time for EU-wide business administration procedures,
- reduction of paper in cross-border administrative procedures,
- lower travel costs abroad and for national documentation (e.g., business credentials),
- more direct contact between businesspersons and foreign public administrations and at the same time more efficient use of local intermediaries and representatives,

- greater security in the access to eGovernment portals (with respect to portal-specific logon mechanisms) and access to a potentially larger number of services thanks to the greater security

Other stakeholders – the eGovernment SPs, the STORK 2.0 MS infrastructure providers, nearby public administrations – also received benefits from the STORK 2.0 integration:

- improved security and efficiency of PSC portals and eGov for business portals,
- acceleration of public administrations compliance to eIDAS regulation, the Services Directive and other measures aiming to reinforce the European economy and promote the Digital Agenda,
- the integration of national Business Registers, Commerce and Mercantile Registers as Business Identity Providers, B-IDPs, that is, as Attribute Providers of Legal Person identity information and mandate information (powers of company representation) and a commitment on their part to become permanent actors in the national eID infrastructures, in synergy with the EC Directive on Business Register Interconnection and the eIDAS implementation,
- greater harmonisation and re-use of national eID schemes towards the establishment of European solutions (CEF),
- exploitation of the portals' multiplier effects to achieve an increased user base of companies and a wider usage of the underlying eID technology,
- a better understanding of the costs vs. benefits of services,
- clearer ideas about the organisational needs and governance mechanisms necessary to achieve sustainability for a national eID infrastructure with cross-border capabilities

Overall, end-users expressed good levels of appreciation of the benefits of STORK 2.0. In particular time savings – measured comparing the administrative procedures with and without STORK 2.0 integration – and administrative simplification were the most appreciated features. Interestingly, end-users placed cost savings in third place, confirming perhaps the fact that businesspersons and end-users in general are willing to pay for convenience.

Around two thirds of the users confirmed that the quality of the STORK 2.0-enabled services was improved with respect to the previously available service, and about the same number of end-users declared their willingness to recommend the STORK 2.0-enabled services to other businesspersons.

The overall end-user experience – ease of use, user interfaces, mechanisms guaranteeing data privacy and security – did receive a certain amount of criticism which is feeding the discussion of future improvements.

Service Providers were even more positive about benefits, immediate and future, and enthusiastically endorsed continued adoption of STORK 2.0 with commitments to ensure near and mid-term sustainability of the platform and services.Of course, not all project or pilot objectives were fully achieved. Using the metrics as an aid to analyse the overall piloting experience, a gap analysis was performed to determine the root causes of the most serious and/or complex gaps between partially achieved objectives and measured results. The gap analysis was often useful in the identification and consolidation of "lessons learned", the project experience in dealing with problematic issues. The gaps have also spurred new initiatives to improve STORK 2.0 functionality, to increase usage and usability of the procedures and to study some of the barriers to cross-border interoperability that were encountered.

These issues are being addressed by STORK 2.0 partners and new collaborators as project results are being transferred and carried over into other European and national initiatives such as the LSP e-SENS, and the continued development of the eID building block in the context of CEF. Take-up of some of the more advanced features of the STORK 2.0 solutions and further development of other innovations, like the representation of mandates, for example, will be pursued in future projects in the context of ISA^2 and similar programmes.

Pilot partners are confident that the legacy of STORK 2.0 is well-prepared to find its place in the next generation of Digital Agenda actions and infrastructures.

1 Introduction

1.1 Scope and objectives

This Deliverable is created within the framework of Task T5.3.6 "Running Phase Reporting" of Workpackage 5.3 "eGov4Business – Public Services for Business Pilot". The aim of the Deliverable is to provide consolidated final results and assessments of benefits and knowledge achieved by the Pilot and reflects its contribution to overall project goals. The future sustainability of the STORK 2.0 infrastructure and services are assessed and planned, taking input from prior interactions with the EC and other external initiatives as well as from an internal Gap Analysis summarised in this document.

The Benefits Logic approach to (self-)assessment of project achievement focuses on three main categories of benefit of the STORK-enabled services: Use, Value and Learning. As a response to specific requests of the EC Reviewers this system of evaluation was further refined to emphasize the dimension regarding adoption of STORK 2.0 and the sustainability of the infrastructure. These categories are reflected in the organisation of this document which is structured as follows:

- Chapter 2 addresses the final status achieved by the pilot.
- Chapters 3, 4 and 5 explore the pilot from the perspectives of use, value and learning, respectively.
- Chapter 6 mainly faces the adoption of the services focusing on a roadmap for sustainability of the pilot beyond the termination of the project and promotion towards service providers; it also cover the status of convergence between STORK and eIDAS and the assumptions on CEF and ISA developments
- In chapter 7, the dissemination of results and marketing phased strategy are addressed.
- Chapter 8 reports general conclusions and a description of the pilot's major achievements.
- Chapter 9 is about project references.

Appendixes I and II contain WP6 Summary table of all metrics and lessons learned respectively.

1.2 Methodology for pilot results

This final report follows the previous eGov4Business deliverables which have established the objectives and activities of the piloting period:

- D5.3.1 Technical Business Objectives and Specifications [1]
- D5.3.2 Go-Live Planning [2]
- D5.3.3 Running Phase Planning [3]

Moreover, the final report completes the preliminary assessment of Piloting results as already reported in the Mid-term Pilot Progress Report, D5.3.4 [4]. In particular, the present report identifies the contributions of the eGov4Business Pilot to the overall success of the project STORK 2.0 and describes how this contribution has been quantified in metrics, underscoring satisfaction of the pilot objectives.

The process for producing the final report elaborates on the status, use, value, learn principles established in the D5.3.4, and is outlined in the following the steps:

- Gathering information from the running phase tasks:
    - Collection of results from all sources of evidence.
    - Monitoring status of services and providing support as they were progressively put in production and published as interoperability increased (as common code was released and common infrastructure updated).
    - User engagement and feedback.
    - SP questionnaire feedback.
    - Marketing, dissemination and communication activities.
- Pilot coordination on the structure and contents of the deliverable.
    - Structure expanded from status, use, value and lessons learned to capture the pilot´s gap analysis and future adoption / sustainability.
    - Reviewed and agreed with pilot leaders.
- Writing the contents of each chapter:
    - Analysis of final pilot status, results, user and SP feedback in order to report on final achievement of pilot objectives and goals, status, use value and lessons learned with gap analysis reported.
    - Additional focus and analysis of pilot adoption and sustainability added.
    - Distribution of reporting tasks among partners.
- Review and quality control

Concrete tasks have been assigned through periodic audio meetings and in the face-to-face meetings held during the STORK 2.0 General Assemblies that took place in Turin in February and in Athens in October 2014, in Lisbon in March 2015, in Ljubljana in September 2015 and also at the Pilots workshop meeting held in Stockholm in June 2015.

2 Pilot status

2.1 Overview and major findings

By the end of the piloting period ten out of thirteen Public Services for Business ("eGov4Business") pilot services had gone into production with live piloting of STORK-enabled cross-border authentication by real or near-real end-users. Given the fact that pilot services depended on the availability of common STORK 2.0 functionalities deployed and tested in production environment of the common interoperability components of the MS with which they need to interact (including their own country), the pilot services had to follow a gradual Go Live process and some (four) of the Service Providers (SPs) went live in the final 6 months of piloting, therefore limiting the total amount of effective piloting. Not all expected results were fully achieved, but in spite of delays and other difficulties, nearly all partners deployed a truly significant amount of new STORK 2.0 functionality. Moreover, the fact that the STORK 2.0 infrastructure was successfully integrated into ten different pre-existing eGovernment services was a valid demonstration of the power and broad effectiveness of the STORK 2.0 approach to cross-border eID management.

Over the course of piloting, 250-300 real end-users accessed official eGovernment services through cross-border STORK 2.0 interoperability, registering more than 1050 successful transactions.

Six SPs implemented the main new STORK 2.0 procedure for the authentication of an authorised representative on behalf of a company, and this procedure was successfully tested across borders of eight of the thirteen MS participating in the Pilot.

Several legal, organisational and semantic barriers were encountered which still pose the greatest threats to the sustainability of some key STORK 2.0 results:

- The legal value of cross-border e-mandates is not universally recognised;
- The harmonised STORK 2.0 taxonomy of company powers, designed to provide end-to-end automated processing of the most common forms of powers of representation of a legal entity, found project approval but has no formal legal basis in the MS represented in the pilot;
- Language and character-set issues only partially addressed in recent eIDAS Regulation Secondary Legislation [16];
- Other more complex mandate issues such as the representation and handling of joint or chained mandates.

The above aspects have not been fully considered or developed in the eIDAS design, and should therefore receive particular attention in the desired convergence between STORK 2.0 and eIDAS implementations. Such aspects are covered in more detail in Chapters 5 and 6.

2.2 Achievements against project and pilot goals

2.2.1 Pilot breakthroughs

The eGov4Business pilot has implemented and tested, for the first time in Europe, the main new STORK 2.0 procedure "authentication on behalf of" (AUB) in real-life, production environment services published in official, national eGovernment portals. This particular procedure exceeds the specifications of the eIDAS Regulation in several respects:

- It establishes a unified process flow adapted to different MS-specific organisations of the actors involved and implementations of the single steps in identity authentication and gathering of relevant legal person attributes and powers credentials;
- In particular, it includes intelligent invocation by the national STORK 2.0 gateways, the PEPS, of the Attribute Provider for business representation credentials, the so-called B-IDP;
- It is based on a harmonised taxonomy of "powers to represent a Legal Person", in particular, an agreed method for establishing the "authorised representative of a legal person" and the encoding of this information as a "mandate attribute" in a SAML2 authentication token;
- It includes detailed, extensive end-user controlled gathering and transfer of personal information and of other attributes for natural and legal persons;

The unprecedented level of cross-border interoperability between administrative registers that was achieved in the eGov4Business piloting raised - for the first time in most cases - the issue of character set interoperability. In fact, the laws of several MS limit the admissible character sets used in certain national registers thus creating barriers to cross-border interoperability. Bilateral and national agreements based on automatic transliteration were established to (partially) solve these problems, and to permit piloting, but permanent solutions are still not in place in all cases and MS.

Other important advances regarded several new features and variations of the originally planned AUB procedure, which were specified and implemented in order to simplify the end-user experience and to follow more closely the usage patterns of eGovernment portals. Not all of these features were released in time for sufficient testing and piloting, but nevertheless they represent important considerations for future evolutions of the infrastructures implementing the eIDAS regulation. These features include:

- a persistent authentication and login procedure at SPs (loosely called STORK 2.0 single sign-on, SSO),
- a flexible AUB procedure which allowed credentials to be gathered from three or more different MS.
- a powers validation procedure for the back-office verification of the continued validity, in time, of previously authenticated company representation credentials which have been stored locally at the SP site and are invoked, as needed, by the end-user. This functionality is particularly useful in those cases where a single end-user may represent several companies at the same eGovernment service, and repeated explicit validation of credentials would interrupt and disturb the service workflow. The feature is also needed to verify the credentials of a representative who is not the current end-user, for example when verifying the intermediate links in a chain of mandates. Finally, some SPs also requested the possibility to check powers as part of back-office procedures after the close of the main STORK 2.0 authenticated work session. Such uses would require separate and explicit forms of end-user consent not fully explored from the legal point of view nor implemented technically.

2.2.2 Pilot technical and business goals fulfilment

On a national level, eGovernment initiatives are making significant progress towards reducing administrative burden on companies by cutting back on physical meetings, eliminating paper forms and documents and by simplifying and speeding up mandatory bureaucratic

procedures. Obviously, citizens and governments alike benefit from the greater efficiency and quality of these services. Key enablers have been the back-office integration and the process interoperability of administrative services. Administrative silos, once completely isolated, are becoming service archipelagoes and communities: still not perfect, but significantly improved.

However, cross-border users of eGovernment services, foreign businesses and their representatives are almost always at a disadvantage when compared to domestic users. They have problems from the start, registering for the services, because establishing their identity is more difficult than for native users. Analogously, information about their companies which are usually registered in foreign Business Registers, and the credentials which establish the foreign businessperson as "authorised company representative" are also more difficult to retrieve and process.

The eGov4Business pilot objectives as stated in the project DoW and further described in D5.3.1 [1] were designed to reduce or eliminate these differences and can be summarized as follows:

- Adapt or extend existing online Public Services for Businesses (enrolment in official registers or some of the services offered at the one-stop shop Business Services Portal or PSC) to cross-border services based on the exchange of identity attributes of the legal representative of the business (or legal entity) or of some other duly mandated person.
- Encourage the use of Public Services for Businesses by foreign users and legal entities by promoting the enlargement of the STORK 2.0 circle of trust to directly include Attribute Authorities for legal persons, such as Business Registers and other institutional Mandate providers.
- Demonstrate and validate the effectiveness of STORK 2.0 facilities for user control of eID and strong data protection as extended to Public Services for Businesses and legal persons.

These three objectives have not changed over the course of the project, and the eGov4Business pilot has achieved them in the following ways:

For the first point, out of the 13 MS participating in the eGov4Business pilot, ten SPs (from AT, EE, GR, IS, IT, LT, LU, NL, SI and SK) successfully integrated their portals into production environments and officially "went live" by announcing and making accessible their pilot services at the STORK 2.0 Pilot micro-site (https://www.eid-stork2.eu/pilots/public_services) implemented by the Project Dissemination team (WP8). Six SPs (from AT, EE, GR, IT, LT and SK) successfully implemented the new STORK 2.0 procedure for the "authentication of a person on behalf of" (AUB) a company (or other legal person), and this procedure was successfully tested across borders of 8 of the 13 MS participating in the Pilot (AT, EE, GR, IS, LT, IT, SI and SK). See metrics F.1 and F.2, in Appendix I.

The eight MS involved in testing the AUB procedure all successfully integrated a business or trade register or, alternatively, a Mandate Provider capable of issuing a STORK Mandate token for qualified businesspersons. This represents an important step in the EU-wide implementation of a complete eID management infrastructure. See metric BV.10 in Appendix I.

The integration of Business Registers brought out several interoperability issues which were not completely resolved. The use of restricted character sets, mentioned in the previous section, was one such issue. The use of different personal eIdentifiers across administrations was another issue complicating the creation and portability of mandates. The necessity to perform local "identity reconciliation" is a problem that all SPs have in associating STORK eIDs

with known users, but in the case of the B-IDP, the Business Register or the Mandate Register, this operation takes on additional legal implications.

A deeper more pervasive problem lies in the interoperability of the representations of powers used in the STORK mandate token. No European-wide standard exists for the description of company powers. No harmonising ontology maps one countries scheme of powers to another's. Thus the powers taxonomy used by STORK 2.0 lacks a legal basis in national or European law. As a compromise, in order to achieve the highest possible degree of automatic processing of authentications, only a partial use was made of the taxonomy. Only three values of the "type of powers" attribute were used expressing full company representation powers, partial powers (and therefore requiring human evaluation to complete the credentials validation and SP access evaluation) and no powers.

These problems and others are discussed in Chapter 5, Pilot learning, below, in particular in Section 5.3. The fulfilment of the metric associated with this aspect of interoperability, metric I.5, was reached with incomplete success as legal and semantic obstacles were found (as could have been expected); partial solutions were found to permit piloting, but permanent solutions are still lacking in some cases.

Regarding the second pilot goal, the eGov4Business pilot did succeed in attracting new service providers to join the network. Even though the Belgian SP, the Limosa Portal, has been held in pre-production environment for legal issues (dictated by the data protection policy of the national Privacy Commission) another Belgian administration running the Flemish Fisheries Portal has adopted STORK 2.0 and is using the project infrastructure for its cross-border transactions with businesspersons from the Netherlands. Similarly, Lithuania has extended the STORK 2.0 authentication to a much broader set of public services for business than originally planned and Estonia and Italy, as well, are also in the process of extending STORK 2.0 services to other services housed at or accessed through the STORK-enabled eGovernment portal. Such developments are naturally pushed by, but also conditioned by, the national eIDAS implementations.

The goal of maintaining a user-centred and user-controlled eID management met with mixed, but decidedly more positive results. As reported in Section 3.3, below, as well as in 0, the user oriented metrics for Data Protection & Privacy, DP.1 and DP.2, showed relatively strong user approval and appreciation of the data protection and safety of personal data as well as for the control of the processing on the part of the user him/herself. Of course, a price was paid for this– "I'm asked to confirm too many times", wrote one user in the feedback form – but this was limited.

2.2.3 Validation of STORK 2.0 common functionalities

The functional needs of the eGov4Business Pilot were largely, but not entirely, satisfied by the software released by the technical development team. Some key features were developed, tested and reworked, only to be released too late to be implemented in the piloting, production PEPS and SPs. These functionalities are indicated in red in the following figure. Green blocks show STORK 2.0 common core functionality successfully employed by the pilot in production, and amber blocks show functionality that was partially employed. Grey blocks are functions not used by the pilot.

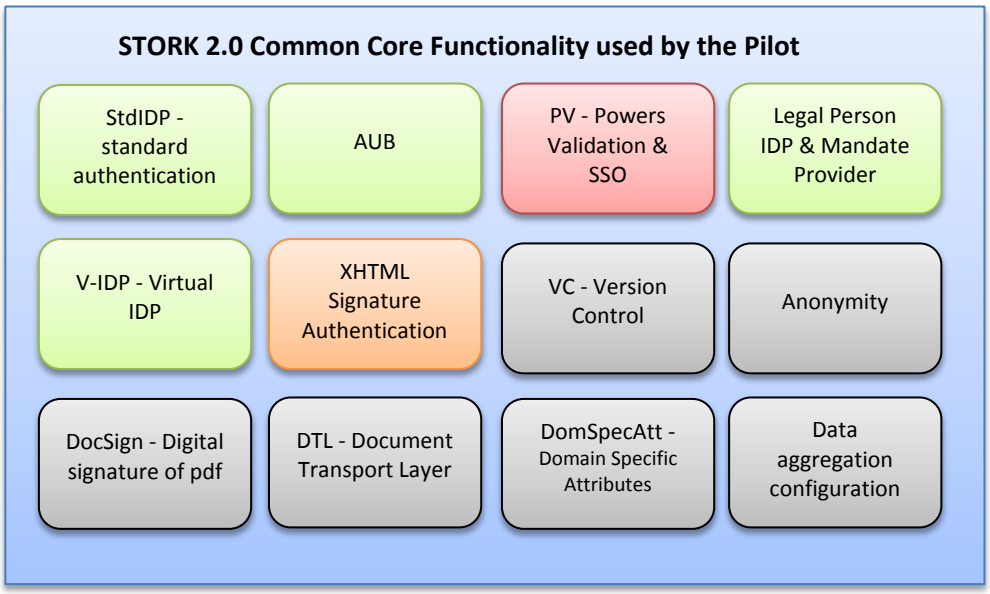

Figure 1: Common Functionality used by eGov4Business Pilot

Use Case 1: Common STORK 2.0 Functionality used by Enrolment to public registers

StdIDP -standard authentication: All eGov4Business pilot services require authentication of the individual end-user at his/her national IDP at some point in the use of the eGovernment portal with (at least) the retrieval of basic personal attributes (eIdentifier, givenName, surname).

AUB - Authentication on behalf of: Several of the eGov4Business pilot services require authentication of the individual end-user on behalf of a company. In all cases this requires the gathering of the mandate attribute containing identity information on the represented person and on the representative and also detailed information on the relative powers of representation. The common structure and characteristics of this attribute (including which information would be mandatory) were discussed at length with Pilot partners and the technical team and the final specifications are given in D4.9 [10] and D4.11 [11]. Additional personal identity information about the representative or the company not contained in the mandate attribute was also sometimes needed.

Legal Person IDP & Mandate Provider: The attribute provider, called the B-IDP, furnishing identity information about the represented company to the eGovernment pilot service was in most cases the national Business or Companies Register. The same Business Register was also, often, the attribute provider furnishing mandate information. B-IDPs were successfully integrated into the national infrastructures of 8 MS (AT, EE, GR, IS, IT, LT, SI, SK).

PV – Powers Validation: A variation of the AUB procedure was also implemented and tested (but not piloted for lack of time) to accommodate those pilot services that required verification of the continued validity of previously registered powers of representation. This functionality posed some new data privacy issues as its deployment was envisioned in different service contexts some of which involved offline users, a situation not previously encountered or foreseen in STORK-enabled services.

Use Case 2: Common Functionality used by One-stop-shop Business Service Portals and Points of Single Contact

StdIDP -standard authentication: same as above
AUB - Authentication on behalf of: same as above
Legal Person IDP & Mandate Provider: same as above
PV – Powers Validation: same as above
V-IDP and XHTMLSign: Needed to access the AT and SI Service Providers

2.2.4 Pilot contributions to STORK 2.0 goals

2.2.4.1 Accelerate the deployment of eID for public services

The eGov4Business pilot has contributed in a significant way to the spread of eID services in eGovernment, in particular, in administrative services for businesses such as the Points of Single Contact created by the EC Services Directive [17] and other one-stop-shops for business lifecycle services. A very important step was the demonstration that business representation credentials could be requested by a service and fulfilled by a distributed, cross-border network of Competent Authorities integrated in the STORK 2.0 MS infrastructures. A number of obstacles to interoperability were encountered (see Section 5.3, below, for example) and brought to the attention of the Attribute providers and national MS Infrastructures. The lessons learned through the STORK 2.0 experience are being reviewed by the e-SENS large-scale project (see [25]) in order to extract the key functionalities which will be incorporated into the Connecting Europe Facility, CEF, Building Blocks (see [21]) and which would consequently make their way into future implementations of the eIDAS nodes.

On the other hand, the settings of eGov4Business portals (in both Use Cases) provided excellent visibility of the advantages of cross-border eID management to potential Service Providers in nearby administrations. This publicity was multiplied through collaboration with national interoperability programmes and through presentations at eGovernment conferences and workshops.

2.2.4.2 Maximize the take-up of its scalable solutions throughout the EU

As mentioned, above, the STORK 2.0 experience is contributing strongly and actively through the national actors involved to the implementations of the eIDAS Regulation [15] and the recent implementing acts [16]. Wide-spread participation by STORK 2.0 partners in EU work groups and, more concretely, in the e-SENS project and in different implementations funded through CEF Digital Programme, ensure the continuity of STORK 2.0 results and a return on investment for participants.

2.2.4.3 Seek and showcase the convergence of private and public sectors

Although all actors in the eGov4Business Pilot were government agencies or their third party developers, the variety of the different specific services integrated in the Pilot permitted the testing of different authentication levels (QAA) and attribute quality levels (AQAA) resembling to a strong degree the variety of service offers in an “ecosystem” of private and public service providers such as is envisioned to evolve in the near future. The mechanisms of user-oriented eID management and data privacy were thus validated in a realistic environment and were proven to be suitably robust.

2.2.4.4 Test, in real life environments, secure and easy-to-use eID and attribute solutions

The eGov4Business pilot services all involved real eGovernment services that were already offered at national web portals. Some of these services already offered cross-border access to foreign enterprises and their representatives which, prior to STORK 2.0, relied on specific offline procedures for the registration of foreign users. Thus a good part of the pilot users were able to compare the differences between access to a cross-border service with and without STORK 2.0 (see Sections 4.3 and 4.4, below), that is, with different service-specific authentication procedures or with a single domestic eID mechanism. The feedback concerning security, ease-of use and other benefits of STORK 2.0 are reported in the coming chapters (Section 4.3).

2.3 Achieved status of use cases & services

The status as of early August 2015 saw ten out of thirteen SPs in production

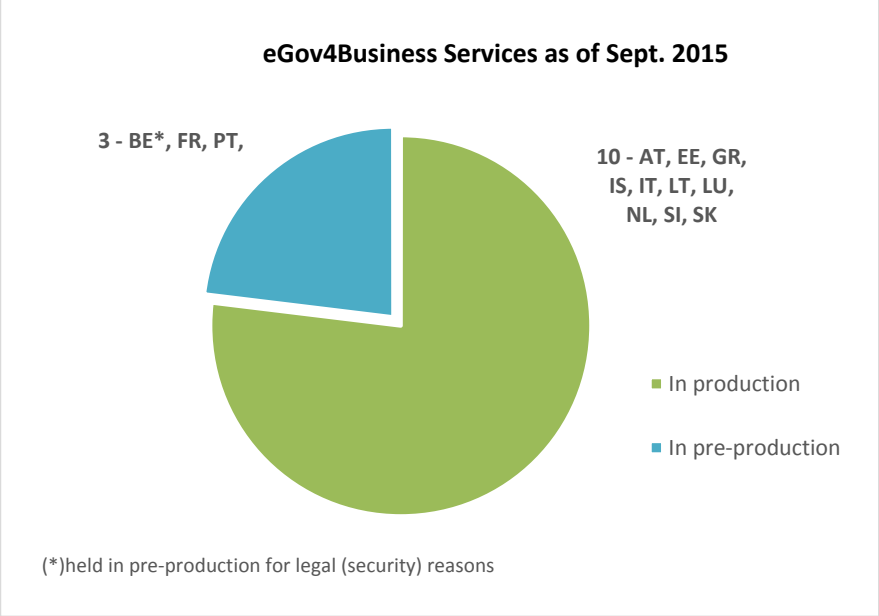

Figure 2: Ten out of thirteen eGov4Business Services GoLive by end of piloting period

We note that the BE-SP has been held in pre-production for legal reasons imposed by the national infrastructure data protection policy (Privacy Commission authorization required).

With thirteen different Pilot services in thirteen different MS the “goLive” status of piloting was in continuous evolution due to deployment delays of both the common and MS-specific infrastructures and Service Provider implementation delays according to the complexities of integration and interoperability encountered. Delays in the release of common software and infrastructure affected all pilots, and late deployment of individual MS infrastructure was the cause of over half the specific SP delays. The next major reason for delay was the difficulty in obtaining technical resources – often through external procurement – for the adaptation of SP services. Finally, the unexpected complexity of the service adaptations, and the need to develop common solutions for issues such as mandate representation and handling, other interoperability problems and also workarounds for missing functionality were also common causes of delay.

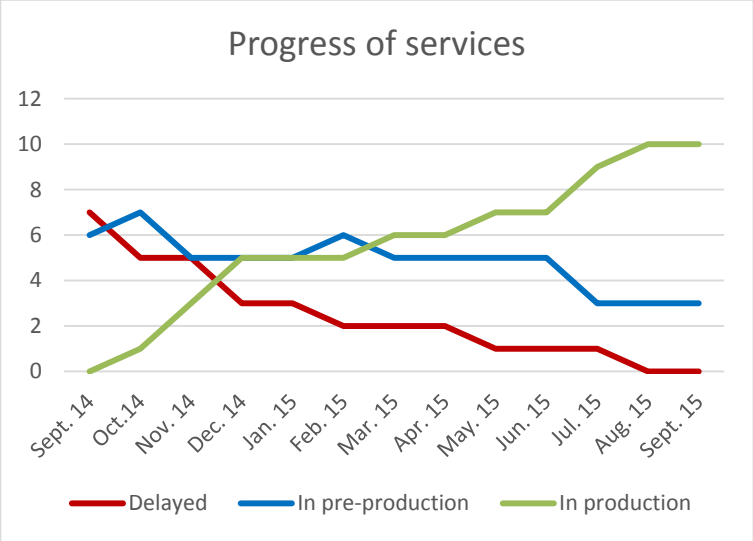

Figure 3: Progressive development of eGov4Business Pilot services

2.3.1 Use case 1: Enrolment to public registers

This Use case groups those SPs which represent specific eGovernment Registers (as opposed to one-stop-shops of Use case 2). In the cases BE, IT and NL the registers represent Labour sector, Environment sector and Agriculture, while the EE service is the online national Business Register.

The following table provides an overview of the deployed services in this use case, the access URLs and the dates they went into pre-production and production state:

Service Provider	***Service***	***URL***	***Pre-prod date***	***Go-Live Prod date***
BE-NSSO	Limosa	***N.A. – pending authorisation by national data privacy Commission***	07/10/14	-
EE-RIK*	Company Reg. Portal	https://ettevotjaportaal.rik.ee/index.py?chlang=eng&sess=&kood	10/10/14	Mar 2015
IT-IC*	impresa.gov	https://strk.infocamere.it/servizi_impresa/home.html	31/05/14	Nov 2014
NL-MEAI	DR-Loket farmers portal	https://mijn.rvo.nl/	29/09/14	Nov 2014
* Authentication on behalf of company, AUB, is implemented				

Table 1: Use Case 1 Service Status

2.3.2 Use case 2: One-stop-shop Business Service Portals and Points of Single Contact

This Use case groups those SPs which represent one-stop-shop portals such as the Point of Single Contact, PSC, established by the EC Services Directive [17].

The following table provides an overview of the deployed services in this use case, the access URLs and the dates they went into pre-production and production state:

Service Provider	***Service***	***URL***	***Pre-prod date***	***Go-Live Prod date***
AT-ARGE*	USP Bus. Serv. Portal	https://www.usp.gv.at/stork	Dec 2014	Mar 2015
FR-ANTS/ CASSIDIAN	Guichet Entreprise Bus.Reg.	http://188.165.144.177/	14/06/14	
GR-HMI*	company registration portal	http://www.promitheus.gov.gr/webcenter/faces/oracle/webcenter/page/scopedMD/sd0cb90ef_26cf_4703_99d5_1561ceff660f/Page122.jspx	Dec-2014	May 2015
IS-SKRA	PSC-Netskil	https://www.island.is/eugo/en/upload/	10/08/14	Oct 2014
LT-IS/MOI*	PSC-Bus. Gateway	http://viisp-test.insoft.lt/portal/en	24/05/14	Aug 2015
LU-TUDOR /CTIE	"Your Guichet"	https://176.65.73.44/gaas_info/index.php	15/06/14	Nov 2014
PT-AMA	PSC, Portal da Empresa	https://bde.portaldocidadao.pt/evo/landingpage.aspx	29/5/15	
SI-MIPA	Slovenia Business Point	http://eugo.gov.si/en/starting/business-registration/limited-liability-company-doo/	29/5/15	Aug 2015
SK-MoF*	PSC, Portal of Ministry of Interior	https://portal.minv.sk/wps/wcm/connect/sk/site/top/uvod	March 2015	July 2015

Table 2: Use Case 2 Service Status

2.4 Achieved interoperability status

The following tables report the achieved interoperability of cross-border authentication in production environments, only. Wider testing was performed in pre-production, but the additional data is not reported.

In general, the achieved level of interoperability is quite satisfactory; the original objective was for each SP to achieve interoperability with at least two other MS. Seven of the ten production SPs achieved this level, and on average, each SP in production has performed successful authentications with three other MS. Six of the ten SPs have also successfully piloted the AUB procedure with transfer of company representation credentials using the STORK 2.0 mandate attribute.

The colour key used to express the interoperability status achieved by the eGov4Business Pilot is given below.

Colour Key:

Functioning	Expected to function	Pending	Prohibited / Not available	Not Planned

- **Functioning**: Interoperability has been successfully proven in real production environment.
- **Expected to Function**: Interoperability is expected by proxy of the interoperability already proven to be "Functioning" for another MS in production and also based on pre-production tests. Full interoperability test coverage is not feasible in production, as we would need real and focus group users from all MSs accessing all services.
- **Prohibited / Not available**: Interoperability not currently possible due to national regulations or due to some technical reason e.g. the required QAA level is not supported by that IDP.
- **Pending**: Tests still need to be performed but are held up by infrastructure delays or partner service or AP deployment delays.
- **Not Planned:** The service is not planned in this scenario due to certain limitations e.g. attributes currently served or planned to be served by this AP does not fit the needs of the service.

The following sub-sections will indicate the interoperability achieved between SPs and national eID infrastructures in production environment.

2.4.1 Use case 1: Enrolment to public registers

IDP / *SP*	AT	BE	EE	FR	GR	IS	IT	LT	LU	NL	PT	SK	SI
EE-RIK													
IT-IC													
NL-MEAI													

Table 3 : Use Case 1 EU-wide service interoperability

Further Notes:

1. BE SP not currently available for legal reasons, but is working closely with NL with whom special bilateral agreements are in place
2. NL SP currently available only to BE
3. NL does not have V-IDP necessary for AT end-users

2.4.2 Use case 2: One-stop-shop Business Service Portals and Points of Single Contact

IDP / *SP*	AT	BE	EE	FR	GR	IS	IT	LT	LU	NL	PT	SK	SI
AT-ARGE													
GR-HMI													
IS-SKRA													
LT-IS/MOI													
LU-TUDOR /CTIE													
SI-MIPA													
SK-MoF													

Table 4 : Use Case 2 EU-wide service interoperability

Further Notes:

1. LT and SK do not have V-IDP necessary for AT end-users
2. GR SP requires mandate attribute (which is not available from some MS)
3. SI SP requires placeOfBirth attribute (which is not available from some MS)

3 Pilot use

3.1 Overview and major findings

Cross-border eID management is undoubtedly a "killer enabling technology", but it is by no means a "killer app". The usage of the STORK 2.0 pilot services was completely conditioned by the normal usage patterns of the underlying services offered to cross-border users. In the case of the Public Services for Business pilot ("eGov4Business") these services deal with business obligations at eGovernment registers and at one-stop-shop portals for businesses such as the Points of Single Contact (PSC) established by the EC Services Directive [17]. In the case of some specific sectorial services or registries (for example, the NL Farming portal or the Italian WEEE Registry for Waste of Electronic and Electrical Equipment) the piloting target consisted mainly of known service users with yearly or seasonal duties to perform. The appeal of participating in STORK 2.0 pilot was therefore to a large degree tied to the demands and deadlines of the end-users' normal bureaucratic operations.

Other general purpose eGovernment portals serve a wider public of businesspersons interested in expanding across borders, but as was seen in the LSP SPOCS [34], and through direct participation in the PSC network EUGO, these portals are chronically under-publicised and under-utilised by the potential market. Cross-border business development still travels very much along traditional channels, and cross-border eGovernment for business is in general no more advanced. There is a marketing effort in place in the EUGO network group that will improve the future situation, at least for service companies, mainly SME's and sole proprietorships (individual business), but the potential for reducing administrative burden even for larger firms is still great and under-developed.

So with this in mind, and with a limited real potential user base, we accept the fact that it is not a feasible primary goal to lure large numbers of users to our services, but rather to make each experience with the portals a pleasant and profitable one, aiming for simplicity, speediness and security in every step of the way.

Other factors also contributed to the difficulty in engaging larger numbers of pilot users, notably the delays in the rollout of the common infrastructure features, which did not allow a full interoperability between pilot MS and therefore for all pools of potential end-users to be tapped into. Also spot shut-downs of the infrastructure for version upgrades, bug-fixes or summer holidays also affected the willingness of SPs to organise focus groups and the commitment of focus users, themselves. Delays in SP development also had a role in limiting the piloting period for most partners.

In spite of all these negative factors, the overall results of piloting were indeed quite positive, As previously seen in Table 3 and Table 4, pilot testing was even more wide-spread than planned, in terms of "number of borders crossed" – i.e., number of MS pairs involved. Even in terms of successful cross-border transactions, the following Figure 4 shows that both number of transactions and geographic diversity ("EU dimension") were thoroughly experimented in the piloting period.

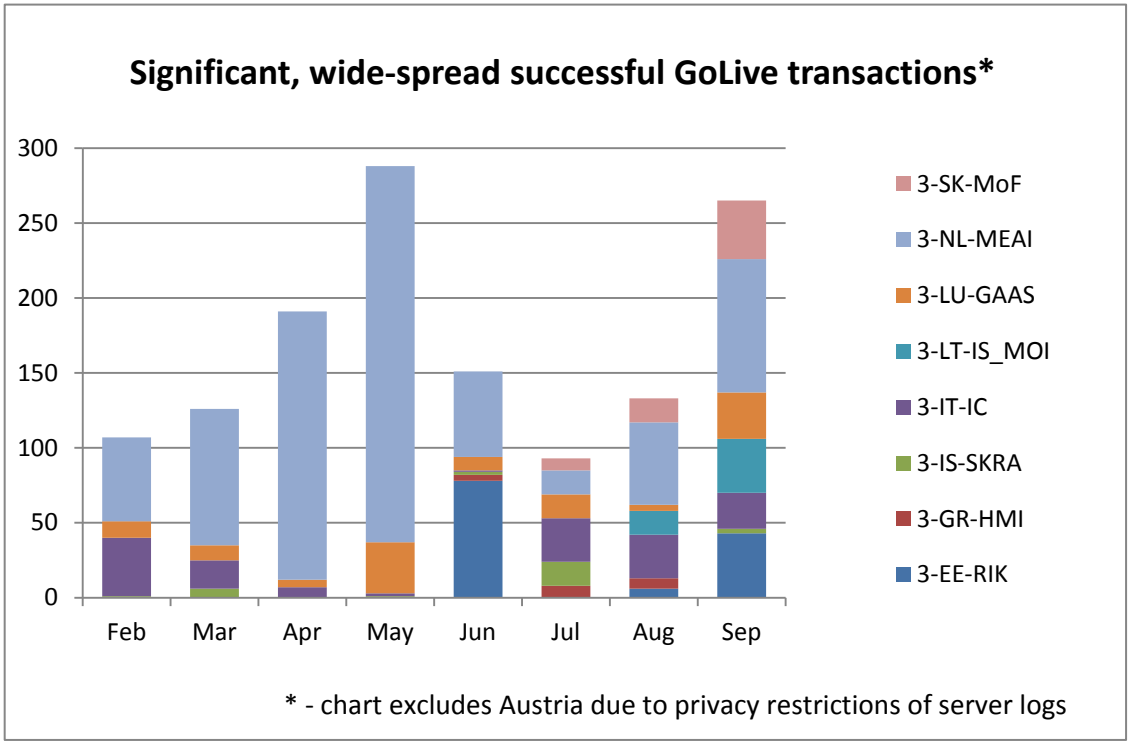

Figure 4: Significant, wide-spread successful GoLive transactions (metric BV.12, PEPS logs)

Clearly, the numerically most significant piloting was held at the NL Farmers Portal where over 250 distinct, real, end-users from Belgium successfully accessed the portal for their farmland registration obligations. But several other SPs, also managed to achieve significant pilot usage, both over time and in conjunction with seasonal activity or specific focus group promotion.

3.2 End-users engagement

The ideal eGov4Business pilot end-user is a natural person who is an individual entrepreneur or businessperson who directly represents a small or medium companies or legal entities. End-users may also be indirect representatives, company employees or business service professionals, accountants and lawyers or professionals employed by service companies engaged by the SME company to handle all administrative procedures, including the eGovernment procedures offered at the Pilot portals. Engaging such users was not always easy or possible. In some cases the users did not possess adequate national eID credentials as required by the minimum data and security requirements of STORK 2.0. In particular, possessing mandates which were both valid and available for real-time online processing proved a not simple task. Other problems arose when individual SPs required specific attributes to satisfy national laws or the policies of other collaborating ministries and agencies – such as SI requirement of placeOfBirth, AT requirement of online digital signature feature, SK requirement of registeredAddress.

The Netherlands achieved the most numerically significant piloting experience using only real, end-users. In the case of the farmers' portal, all end-users were known Belgian businessmen-farmers already registered at the portal. They were contacted directly and invited to experiment the STORK-enabled access based on their domestic Belgian eID cards instead of the portal-specific authentication. A special "identity reconciliation" function was added to the SP pilot service in order to associate the end-user's Belgian identity to the previously

registered credentials at the Farmers portal. This was a common adaptation across SPs of almost all STORK 2.0 pilots.

SP ***Pilot end-user type***	AT	EE	GR	IS	IT	LU	NL	SK	SI
Individual businessperson representing a legal person									
Business service professional hired by legal person									
Indirect representatives (SP employees, STORK partners etc)									

Table 5 : Pilot End User Types involved in the pilot countries

To mitigate the low availability of real end-users, all SPs fell back on the engagement of special focus group users. In most cases these were STORK 2.0 colleagues, but company or organisation colleagues were always preferred for their more objective points of view. Several SPs (IS, SK, GR, LU) were able to recruit pilot users among employees of other public administrations, thus performing useful dissemination at the same time as gathering qualified feedback from eGovernment and business administration professionals. A specific example of this was the Iceland PSC which worked closely with its chamber of commerce business association to engage both businesses and public servants in pilot testing.

The piloting period lasted for one year, but because of a variety of factors including the gradual deployment of SP and common STORK 2.0 functions it did not reach a sufficient number of (potential) end-users to have the impact on the SP user-base that was hoped for. Although the Benefits Logic metric SF.1 (see Appendix **I.**5: Scalability/Flexibility) established a success criterion of a 25% increase in the piloting user-base, the growth in the general user base was limited. Even in the case of the very successful NL Farmers Portal, almost all the piloting users were previously registered, known farmer-businesspersons.

As seen in Figure 7 in Section 3.3.1, half of the eGov4Business pilot SPs reported some or significant growth in the number of users during the pilot period, with others indicating that they expected growth over the medium period.

If recruiting pilot users was difficult, then getting them to fill in usable piloting feedback forms was even more so. Yet again, the eGov4Business team of thirteen SPs was able to produce useful results. The user feedback and metrics relevant to measured Pilot USE are reported in the following section.

3.3 User feedback and metrics

Before considering the specific metrics and results of end-user evaluation of Pilot Use criteria such as usability, satisfaction, experience using the services, etc., we insert a premise.

Although authentication is an operation that we all perform, usually several times per day with several different eIdentities, it is an operation which seeks to interrupt the application flow as little as possible, or as little as necessary to assure the end-user that an adequate level of security is governing the procedure. Thus its presence should comfort the end-user, but not disturb or inconvenience him/her. For this reason, the end-user is largely unaware of the complexity of authentication procedures and is not familiar with the language or

technicalities involved. This makes evaluating the user experience difficult, because such evaluation necessarily brings the authentication operations into "front and centre stage" a place it usually tries to avoid.

This was even seen in a few end-user comments which indicated a difficulty in understanding the feedback forms themselves, for their use of unfamiliar Identity Management jargon and concepts. Moreover, it was seen that real end-users as opposed to focus group pilot testers, were more likely to leave feedback forms incomplete, giving up after a certain number of pages. By the end of piloting there were 71 complete feedback forms out of about 110 begun.

3.3.1 Usability-related metrics

As noted, authentication is a technical area that when brought to the fore risks being observed in a negative light. In fact, several comments about STORK 2.0 eIdentification did point out the detailed even annoying aspects of granting consent, for choosing Attribute Providers, etc. Also, some comments referred to the PEPS user interface which is too full of technical jargon to be fully understood: improving the language would make the process more clear and also contribute to building trust in the infrastructure.

Metric UU.1 - End-users' perception of usability.

Overall, however, end-users were satisfied with the usability of STORK and with the way it is integrated into pre-existing eGovernment services. This is shown in the following figure:

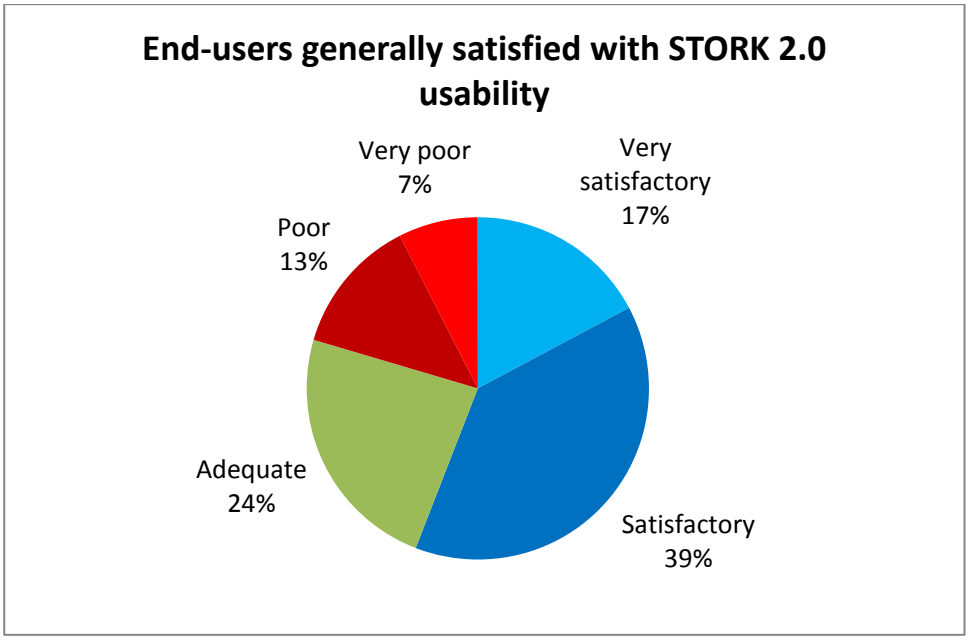

Figure 5: STORK 2.0 "ease of use and understanding" (metric UU.1, Feedback Form Q6)

Not surprisingly, end-users with less experience with eGovernment procedures – end-user who never used eGov or who used it about once per year – were less satisfied than end-users who use eGov procedures at least on a monthly basis. In fact, experienced users were a third less likely to rate the STORK 2.0 end-user experience negative than less-experienced users. As can be seen in the following figure, all of the "Very poor" ratings were cast by inexperienced users and all of the "Very satisfactory" ratings were given by experienced users.

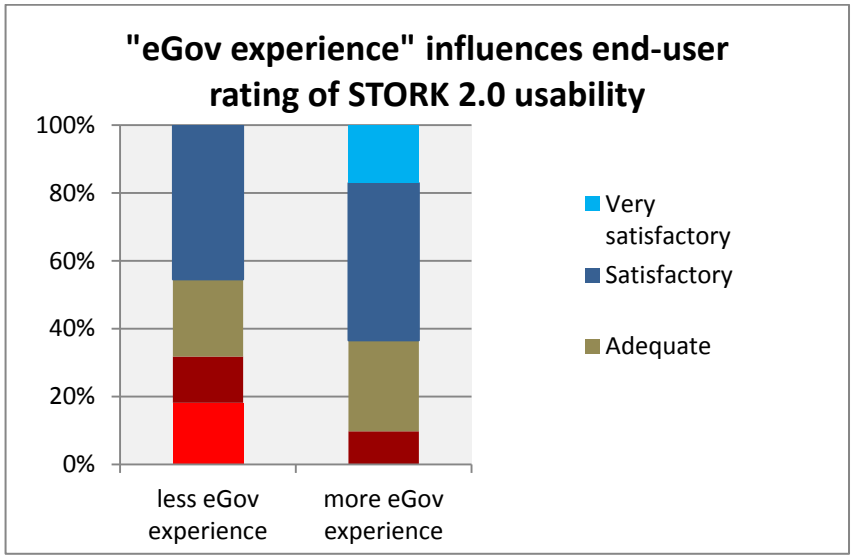

Figure 6: Frequency of use of eGovernment services influences the rating of the STORK 2.0 end-user experience (metric UU.1, Feedback Form Q6 and Q7)

Metric BV.12 - Successful cross-border eGov. service transactions

The number of successful transactions registered at the PEPS logs illustrated above in Figure 4 was over 1000. Since a target of 500 successful transactions had been established for the Business value metric associated with this USE category this target was achieved.

Metric BV.11- Increase in number of users by the end of the project (Qualitative SP viewpoint).

However, as seen in Figure 7, half of the eGov4Business pilot SPs did report at least some growth in the number of users during the pilot period, with others indicating that they expected growth over the medium period. Interestingly, because pilot users were all previously known, The Netherlands and other successful pilots reported no noticeable growth in the user base.

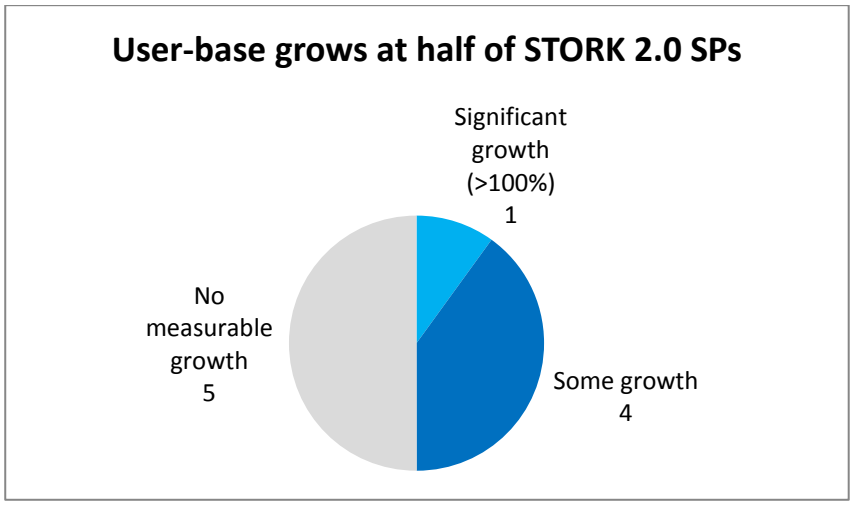

Figure 7: Growth in the user base at STORK-enabled SPs (metric SF.1, SP Questionnaire Q22)

Metric SF.1 - Increase in number of users by the end of the project. (Quantitative server logs viewpoint).

Moreover, as seen in the PEPS logs in Figure 4 there was more than 100% growth in the monthly users with respect to the beginning of piloting.

Metrics UU.3 - Successful access to SP services.

Of the 71 completed feedback forms the number of successful transactions reported was about three times the number of failures due to STORK error (i.e., excluding cases where the user abandoned the procedure because of forgotten PIN or similar problems) giving a success rate of 64%, and a "non-failure" rate of 79%, substantially meeting, or above, the pre-established success criterion of 66%.

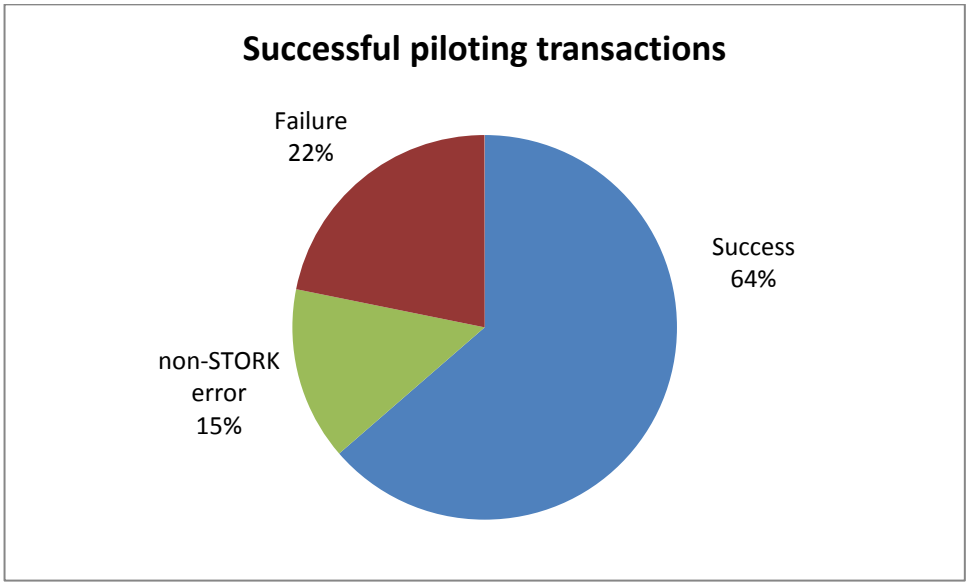

Figure 8: Success and failure rates for STORK 2.0 authentication (metric UU.3, Feedback Form Q5)

Metric P.1 - User verified portability on different browser platforms.

In the interest of promoting the widest possible availability and usage of the services, two metrics indicating the portability of the services have been employed: User verified portability on different browser platforms (metric P.1) and the SP verified server platform portability (metric P.2, see Section 3.4, below).
End-user browser compatibility required that at least three browsers be supported by STORK-enabled services. The responses to Q22 of the end-user feedback form did indeed confirm that at least five different browsers were successfully used in the piloting. (in both Mac and MSWindows operating systems): Chrome, Firefox, MSExplorer, Opera and Safari.

Metric UU.2 - Microsite and feedback form available in MS languages.

Finally, we note that the feedback forms were available in all MS languages as required by metric UU.2. Interestingly, besides English only Spanish and Dutch languages were actually used in the piloting.

3.3.2 Other end-user evaluations of USE: STORK 2.0 makes sense, is trustworthy and secure (F.4, S.2, DP1, DP.2)

Metric F.3 - Successful authentication procedures, individual and "on behalf of" a company or a person.

Of the 71 completed feedback forms the number of successful transactions reported was about three times the number of failures due to STORK error (i.e., excluding cases where the user abandoned the procedure because of forgotten PIN or similar problems) giving a success

rate of 74%, above the pre-established success criterion of 66%. There was no significant difference in the success rate of basic authentication operations with respect to AUB.

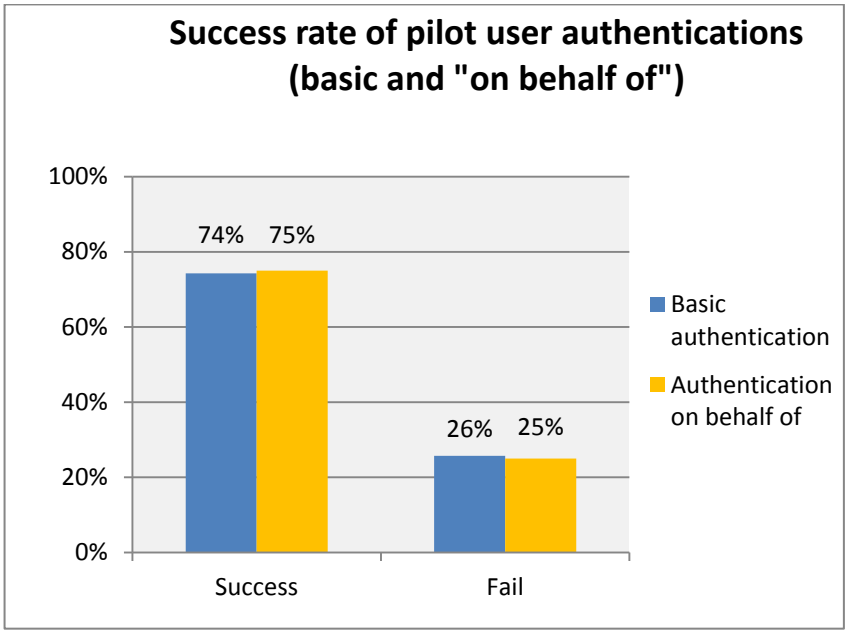

Figure 9: Relative success and failure rates for the two main STORK 2.0 authentication procedures (metric F.3, Feedback Form Q4 and Q5)

Metric F.4 - Perceived usefulness (by end-user).

End-users were asked their impressions about several aspects of using STORK-enabled services. Regarding the usefulness of the basic functionality of cross-border interoperability they were asked to agree or disagree with the statement that "STORK 2.0 eID management makes good sense". 72% of respondents agreed or agreed strongly and 20% disagreed or strongly disagreed. Unfortunately none of these end-users added comments to explain their views or to give indication of how to improve the situation.

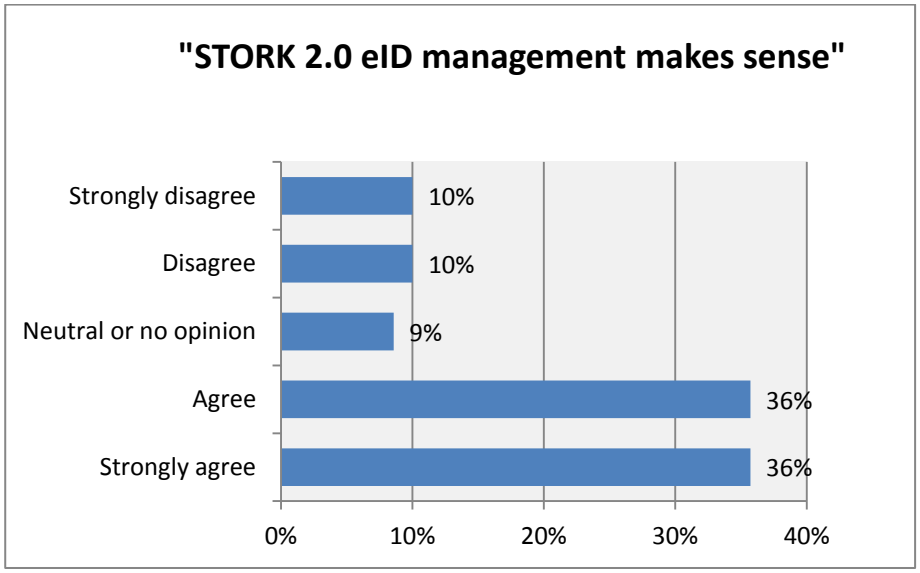

Figure 10: End-users feel that STORK 2.0 eID management "makes good sense" (metric F.4, Feedback Form Q10a)

A similar, but more concrete question requested users once again to agree or not with the statement that the "STORK-enabled service was in some way better than the previous service: easier, more convenient, time saving and/or reliable". The positive replies were 52% of the responses, considerably less than for the previous question. Negative replies were slightly higher, at 26%, and the undecided more than doubled.

Metric F.4, the average of these previous two values, aimed to achieve a success criterion of non-negative response rate of over 80%. The average achieved, 77%, is 96% of the target, a non-critical gap.

Metric DP.1 – Users' perception of privacy protection (safer, smarter, more trustworthy)..

Some other features of the STORK-enabled pilot services which were tested by the feedback form were the user's perceptions of STORK 2.0 Security, Privacy and Trust. As can be seen in the following graph, responses to the three questions were highly correlated and strongly, but not overwhelmingly positive.

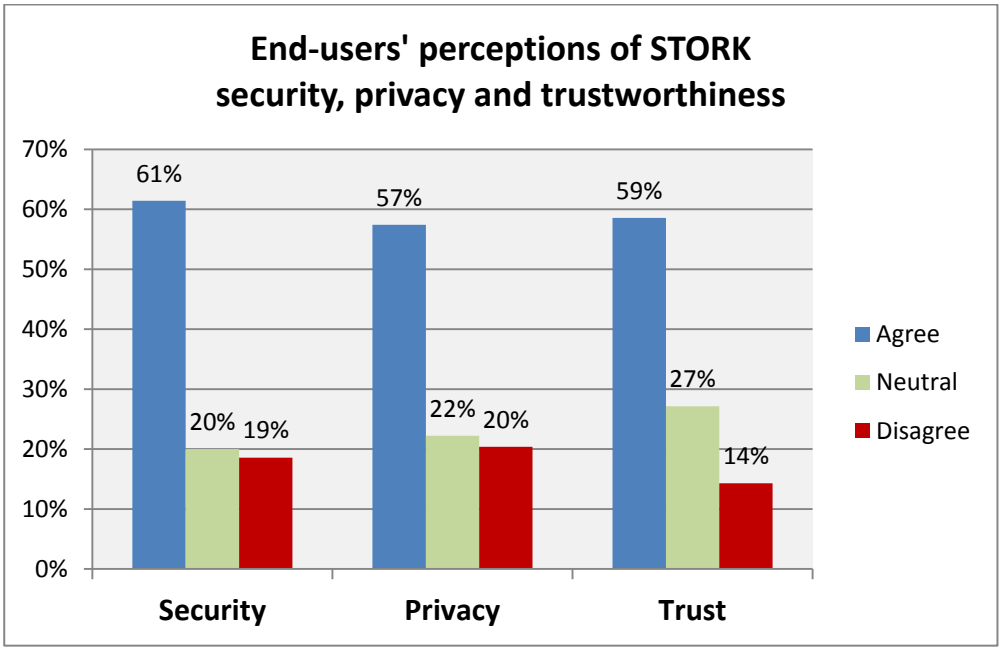

Figure 11: End-users' perceptions of STORK security, privacy and trustworthiness (metric DP.1, End-user Feedback Form Q10)

The fact that end-users perceptions are neutral or of "no opinion" is not worrying – on the contrary, security, privacy and trust are usually more felt when they are lacking or breached than when they are present. But the negative feeling at a level around 20% is a cause of concern, and has triggered some "lessons learned" in terms of measures to reinforce trust (see Section 5.4.3).

Metric DP.2 – Users' perception of being in control over the handling of their own personal data.

The eGov4Business End-user Feedback Form had an optional set of "advanced" questions for more interested users. Two of these questions further explored the user's perception of the data privacy mechanisms implemented as part of the authentication processes. Users were asked if they felt "fully informed about" and "in control of" the use of their personal data in STORK-enabled services: 77% of respondents felt informed; 67% of respondents felt in control.

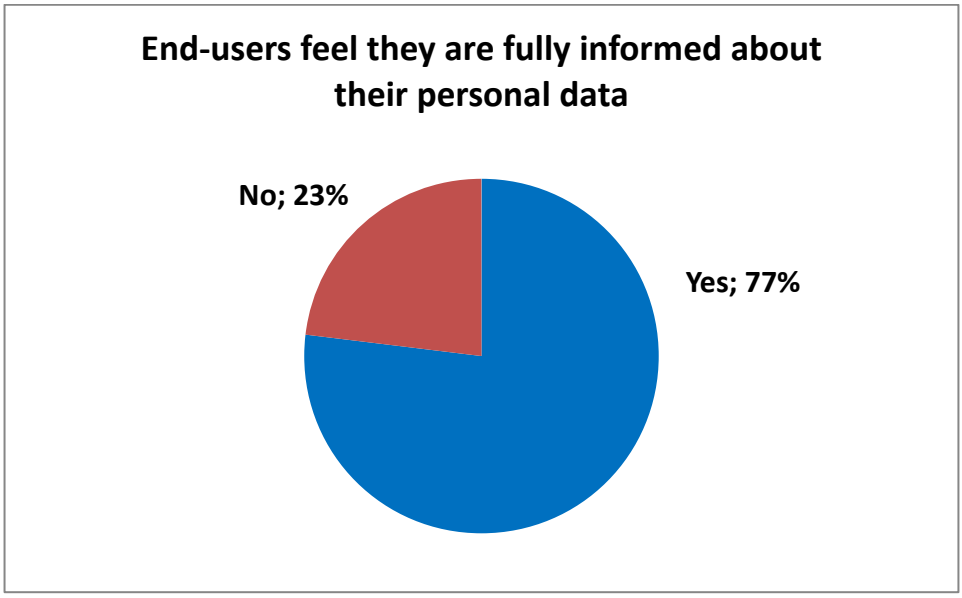

Figure 12: More than ¾ of users feel informed about the processing of personal data (Metric DP.2, End-user Feedback Form Q14)

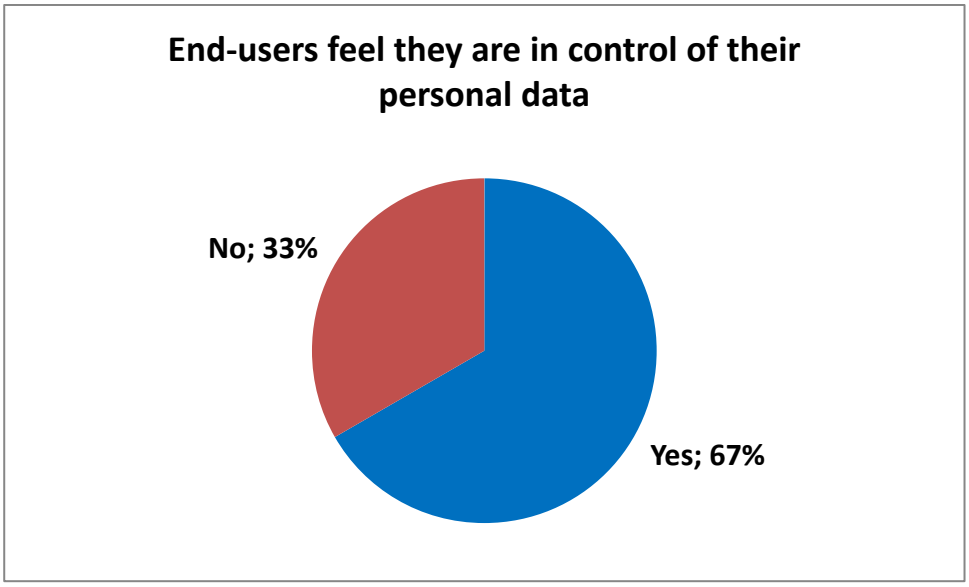

Figure 13: Two thirds of end-users feel in control of their personal data handled by STORK 2.0 (metric DP.2, End-user Feedback Form Q15)

As before, the responses are unquestionably positive, but the level of negative response is both puzzling and a cause for concern. The puzzling aspect is the doubt as to how to reconcile the need to keep procedures simple and the need to raise the perception of control. Already the STORK 2.0 procedures for user-requested consent to gather attributes and consent to transmit them, configured at the MS level, are seen as excessive or at least disturbing for the smooth flow of the SP procedures.

Unfortunately feedback form responses provided no indications of why users did not feel in control: one user furnished the complaint that there were too many requests for confirmations, an obtuse reason to feel lack of control.

Metric S.2 - User perception of security.

Partly as a control for the previous series of questions measuring DP.1 in the first part of the feedback form, a general opinion on security was repeated in the “advanced” section of the feedback form. The overall replies confirmed a positive evaluation, but with reserves which certainly need to be addressed in order to raise the level of comfort of users of STORK-enabled services. Additional testing should be performed to gauge whether the negative responses are typical of all security-related questionnaires or if they are truly indicative of a lack of trust in STORK 2.0.

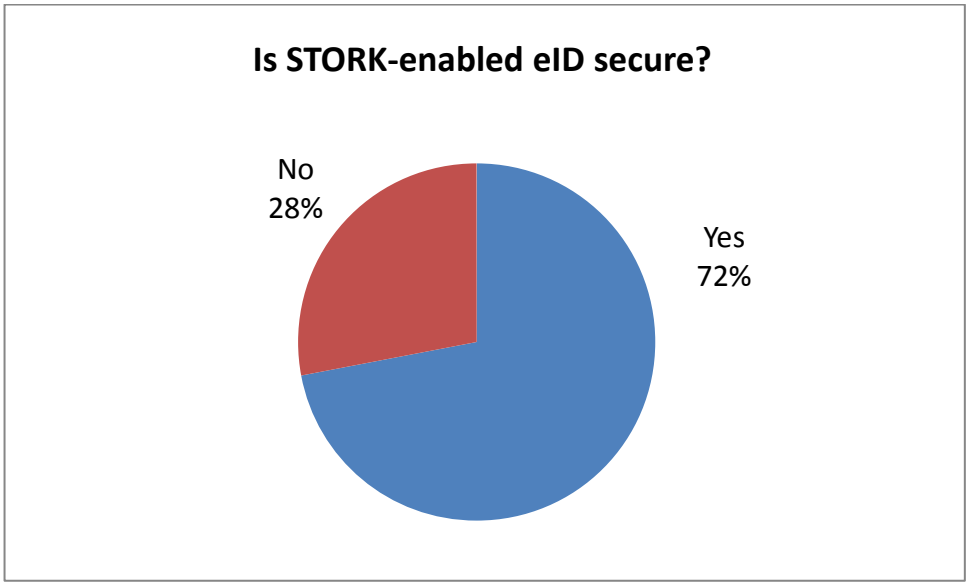

Figure 14: Pilot users feel secure (metric S.2, Feedback Form Q16)

3.4 Results of USE-related metrics from SP & PEPS points of view

We now consider those metrics related to the benefits category Use and measured by the SPs through the SP Questionnaire and by analysing the PEPS logs.

Metric SF.3 - Ease of integration for SPs.

The metric SF.3 measured the SP impressions of the ease of integrating with the STORK 2.0 infrastructure. Of the ten SPs in production status, six rated the task of integrating their services with the national STORK infrastructure as “no more difficult than expected”. Thus the target for success, 66% was substantially achieved by the rating of 60%.

The unexpected difficulty of implementing the AUB procedure made itself felt in the fact that no SP that implemented AUB rated the integration as easy, and that all of the SPs that rated integration as “somewhat difficult” had implemented AUB.

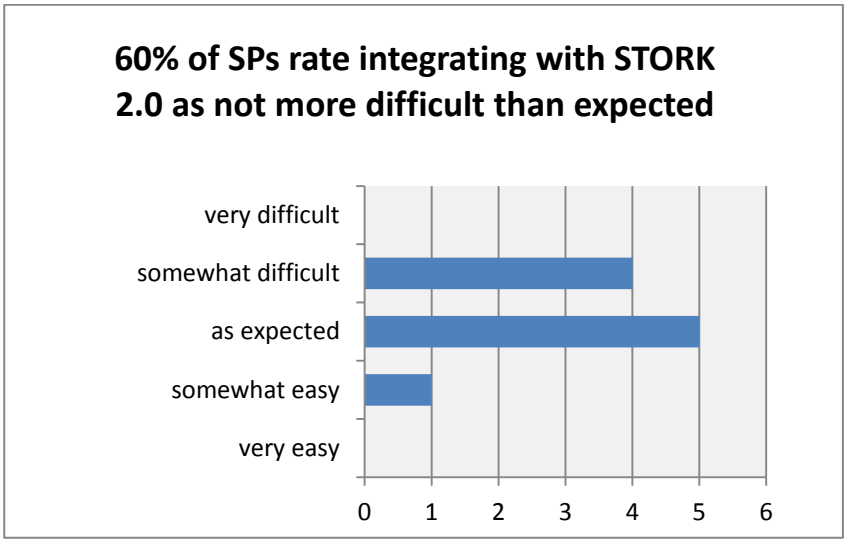

Figure 15: SP rating of the ease of integrating with the STORK 2.0 infrastructure (metric SF.3, SP Questionnaire Q27)

To get some additional insight into the unexpected difficulties we report the direct comments of some of the eGov4Business Pilot SPs themselves. It goes without saying that they represent individual opinions and not a general consensus

> *The overall delays in the release of the AUB procedure and Signature functionality created extra efforts for SPs.*
>
> *The SP pilot service is a national register which is part of the courts system. This means that all documents, data etc. submitted to the registrar must be trustworthy and checked since once registered they become legally valid information. Integration of STORK services was more difficult than expected since it did not correspond to internal rules and regulations directly.*
>
> *Different types of interoperability problems arose around the meaning of powers and the legal validity of STORK 2.0 tokens.*
>
> *It took considerable effort to adjust the service infrastructure for a proper solution for identity reconciliation between the native user ID scheme and the STORK eID. Strictly speaking, connection to the national PEPS infrastructure was no bottleneck.*

Metric DP.3 - Privacy policy present on SP site.

A metric regarding the respect of end-user Data Privacy set the goal that all SPs should have published a Data Privacy Policy on the service website. Eight out of the ten GoLive SPs in production did, indeed publish such a policy creating a gap of 20% with respect to the target, although relatively large, the gap is easily repaired.

A reasonable reply to this objection might be that it is better to be redundant and to comfort the end-user, rather than to just leave him/her with doubts which could undermine the trust in the service.

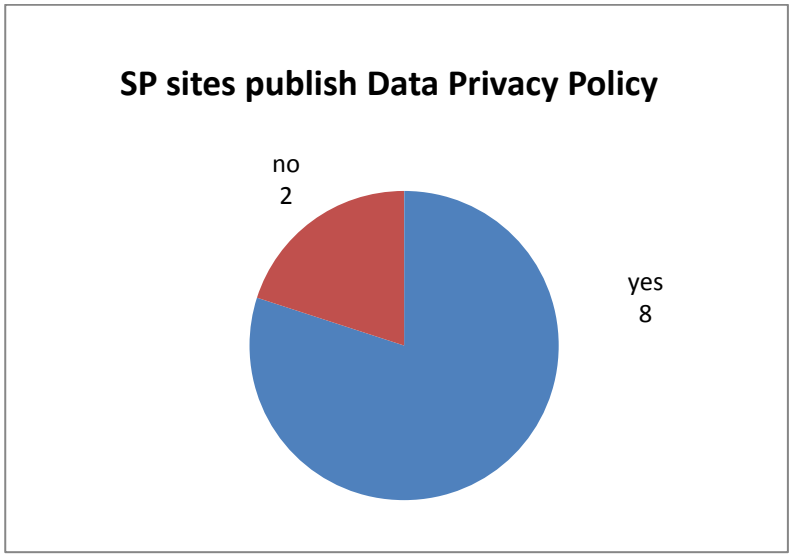

Figure 16: All but two SPs publish a Data Privacy Policy (metric DP.3, SP Questionnaire Q34)

Metrics RM.1 and RM.2 - Availability of STORK 2.0 common and national interoperability layers.

The SPs were asked to evaluate the impact that being integrated with STORK had on their own Quality of Service in terms of reliability and availability of the STORK 2.0 infrastructure. No SP felt that the quality was below expectations.

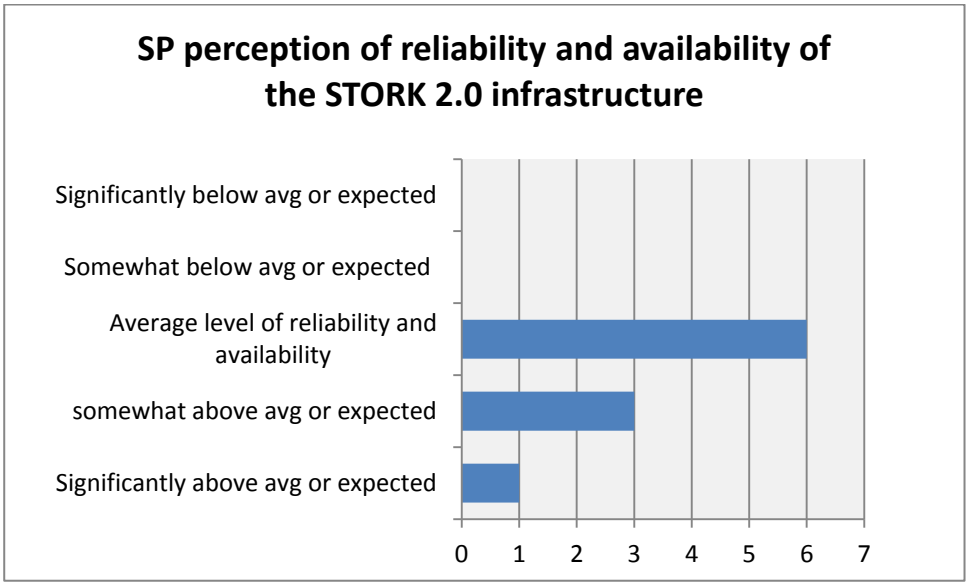

Figure 17: No SP evaluated negatively STORK 2.0 reliability (metric RM.1, RM.2, SP Questionnaire Q29)

Again, some comments from the SPs shed light on this point.

> *Given the innovative nature of the piloting the expectations on reliability and availability of the infrastructure are lower than for a commercial service, but the lack of a SLA for STORK 2.0 should be corrected in the near future.*

In the pilot running phase there have been no issues at all with regard to the reliability or availability of both the national S-PEPS and the foreign C-PEPS. This may be related to a very cautious STORK software upgrade policy and a focus on portal usage rather than service features.

Metric RM.3 - Availability of STORK 2.0-enabled SP pilot services.

Similarly, on the topic of quality of Service and availability, the specific metric RM.3 addressed the availability of the integrated SPs, themselves. The established success criterion of more than 85% service for 6 months continuously was more than reached by the SPs who according to their questionnaire replies reported an overall average of 94% uptime.

3.5 Results of use related metrics from the PEPS/V-IDP transaction logs

This section reports some additional statistics from the PEPS logs at the very end of the project to give a final indication of the wide-spread end-user and focus group activity of overall attempted authentications.

The following figure shows the distributed geography of piloting users and their authentication attempts. After that Figure 19 gives the month-by-month breakdown of these attempted authentications. And finally Figure 20 reports the monthly breakdown of authentication attempts which took place at the Austrian SP – counted separately because AT follows the distributed architectural module.

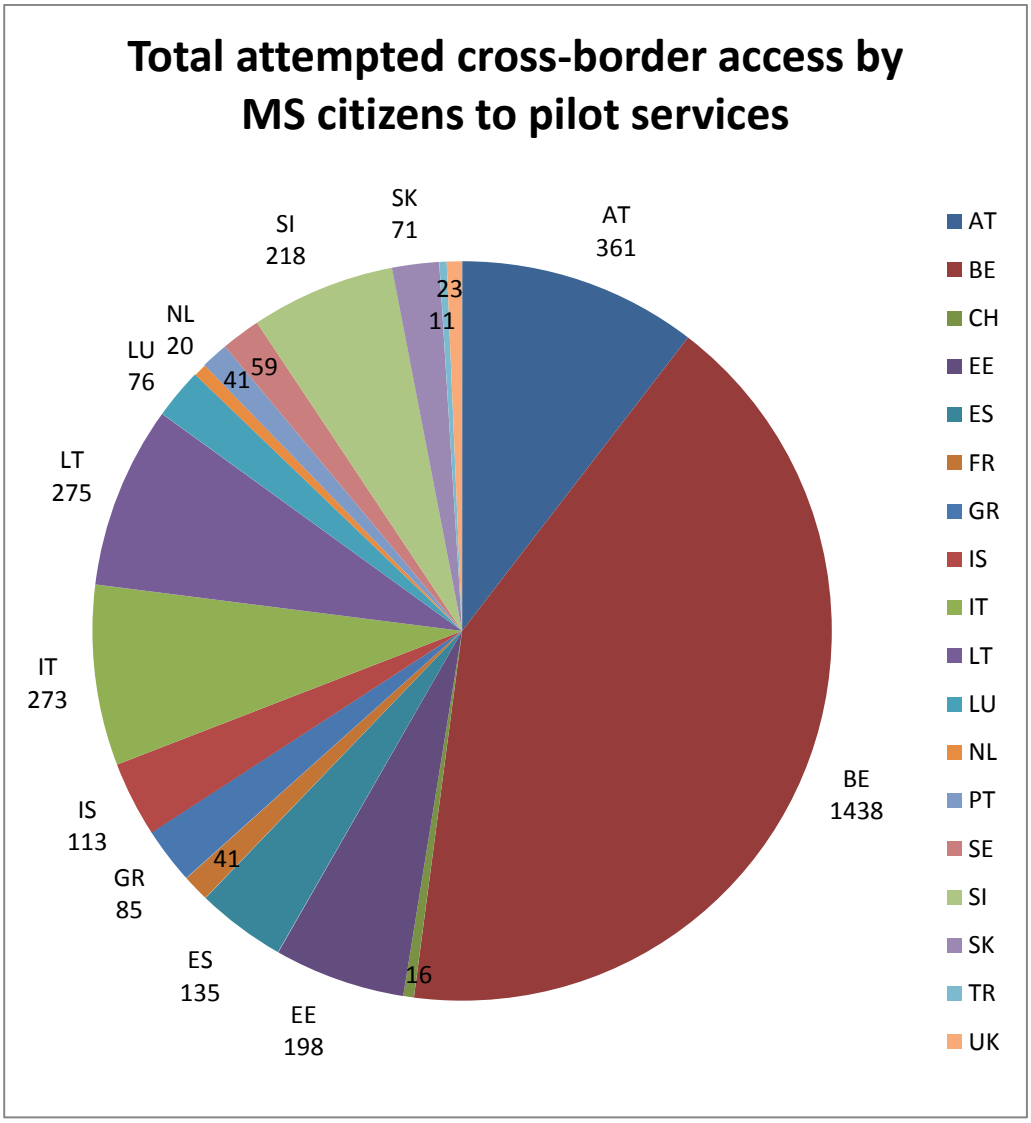

Figure 18: Total attempted cross-border access by MS citizens to pilot services

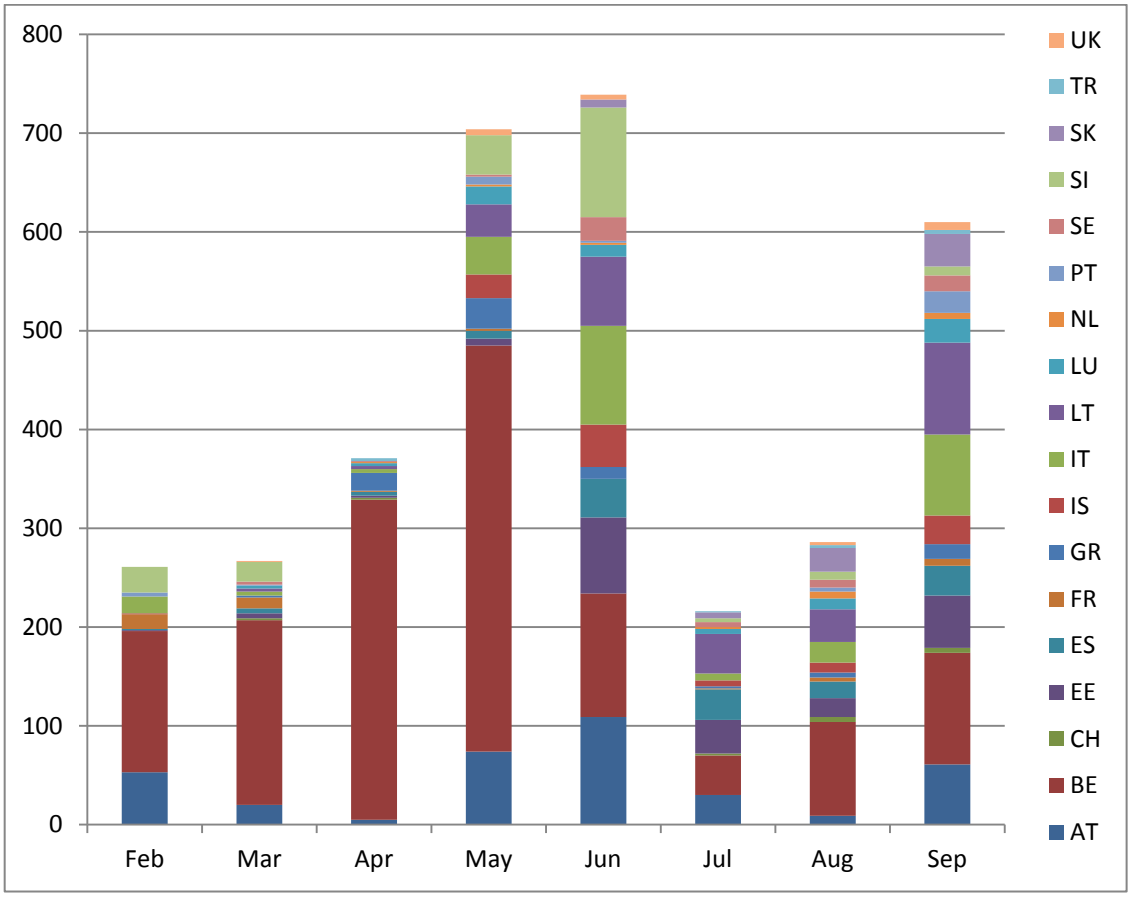

Figure 19: Total monthly cross-border attempted sessions in eGov4Bus Pilot

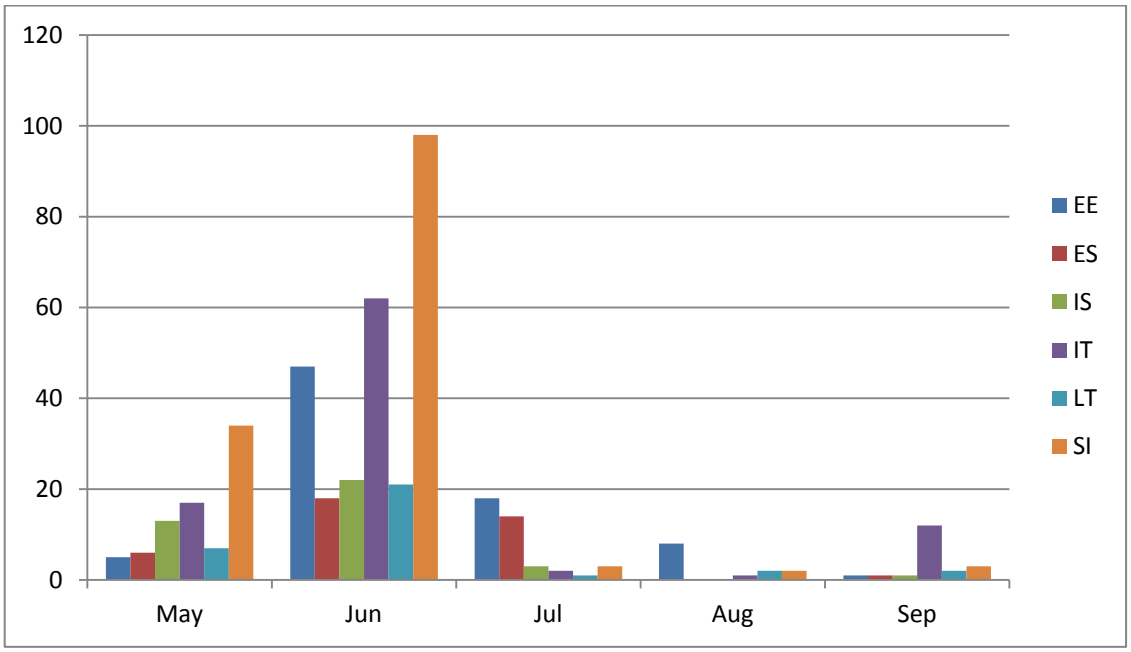

Figure 20: Total attempted monthly cross-border transactions to AT SP

4 Pilot value

4.1 Overview and major findings

The main operational objective of the STORK 2.0 eGov4Business pilot services was to facilitate cross-border access to administrative services by foreign businesses and their representatives. The achievement of this objective has been evaluated in terms of the benefits created by STORK 2.0 functionalities for all stakeholders involved for:

- The businessperson or individual entrepreneur end-user who directly represent a small or medium companies or legal entities,
- The professional service agent acting as end-user on behalf of a business client (e.g. indirect representatives, company employees or business service professionals, accountants and lawyers or professionals employed by service companies engaged by the represented company to handle all administrative procedures),
- The piloting eGovernment Service Provider (SP),
- The portal provider publishing the pilot service and
- Other nearby administrations that are considered potential future adopters of STORK 2.0 solutions.

The major benefits of STORK 2.0 as evidenced in the development and running phases of the eGov4Business pilot were expressed and measured as Value to stakeholders, in particular as Business Value:

- Bottom line savings of time, money or effort
- Improvements in the quality of service.

Value was also measured in the capacity of STORK 2.0 to:

- Open cross-border eGovernment services to a broader user base,
- Facilitate the development of new cross-border access to eGovernment services in line with EC Directives and strategic policy objectives,
- Improve, in any way, the overall user experience.

To determine the Net Value of the final results of the STORK 2.0 eGov4Business Piloting experience all the benefits produced by the pilot were examined – results which contributed to overall project goals and also pilot-specific benefits – as well as the costs incurred in pilot development, deployment and running phases. This involved a detailed review of 30 individual metrics as reported in Sections 4.2, 4.3and 4.4. These metrics take into account benefits and costs from quantitative and qualitative perspectives, collecting input from all participants in the piloting, including server logs of the STORK 2.0 infrastructure and the SPs themselves.

For each metric a success criterion was (pre-)established which served as a target. In retrospect, some criteria may have been too strict while others too loose, but they served as periodic monitors – on a biweekly, monthly or six-monthly basis – of Pilot achievement, and helped indicate where further investment was needed and useful as the piloting proceeded.

To this end, the recommendations of the Project Reviewers and of the internal Pilot Evaluation team (a specific project work package) were also invaluable in focusing energies and resources in those activities with the most potential for producing significant results –

aligning activities with original project objectives and managing adjustments when tactics shifted. This added focus was necessary given the fact that piloting was less extensive as hoped for in time, in number of piloted services, implemented use cases or specific features and in number of real end-users engaged and motivated to provide feedback.

While a considerable majority of metrics saw their success criterion achieved, for those where success was partial a series of gap analyses was conducted. This is reported briefly in the final section of this chapter (see 4.5.2) to shed light on the causes of late delivery or lack of deployment of certain functionalities in MS production infrastructures and SP pilot services, and on the unexpected procedural complexity, the interoperability issues and the opportunities for improvement in different aspects of the end-user experience.

The major findings can be summarised as follows:

Functional use case coverage by pilot partners was not fully complete, but nevertheless was extremely significant. The new STORK 2.0 "Authentication on behalf of" procedure (AUB) was implemented in six different SPs and eight MS. This is the first time that European eGovernment portals receive machine processable credentials from the Business Registers (or equivalent) of other countries in order to authorise the access (i.e., allow logging on) of a company Legal Representative.

The basic requirement of STORK 2.0 procedures that all authentication credentials be made available in real-time using machine processable SAML tokens created the most problems in terms of software development, data privacy and semantic and legal interoperability. The hidden complexity of these issues was at the root of many of the difficulties experienced by the pilot and by the project as a whole. The lessons learned, however, will prove very useful as MS infrastructures evolve in order to maximize impacts of the eIDAS Regulation (see Chapter 5). Some project experiences have already been taken up by the implementing acts of eIDAS (for example character set interoperability issues). The impulse given to Business Registers and Mandate Providers to integrate their services in the national infrastructure in eight MS will be a lasting result of the project, and all piloting SPs felt that STORK 2.0 gave a significant contribution towards compliance with EC regulations.

The basic authentication operation caused fewer problems and was successfully piloted by SPs of ten different MS. Over 1,400 successful transactions, over 1,000 of which were cross-border, took place during the piloting period involving focus group users and around 300 real businessperson clients of the SPs. Information kept in STORK 2.0 PEPS server logs is anonymous, but nevertheless furnished much useful data about the transactions and the achieved interoperability. During the piloting period PEPS logs were distributed and analysed on a monthly basis.

Around 110 end-user feedback forms were submitted (at the online Piloting "micro-site") of which 71 were complete. Again, though, the information gathered was significant, as were added comments by form respondents. Forms were gathered and analysed monthly in the first 3 months and then on a biweekly basis.

The general user experience was perhaps one of the more troublesome areas of the project: cross-border eID is not yet an everyday operation, even for cross-border businesspersons. Moreover, the demands of fully respecting, user-centred data, privacy principles and industry-strength eGovernment security levels also led to more complex aspects that had to be handled carefully. Finally, surveying end-users about such issues, issues which are usually hidden from view in the normal service application flow, is somewhat of a strain on end-users and tends to encourage critical responses.

Nevertheless, end-users did express good levels of appreciation for the benefits of STORK 2.0. In particular time savings – measured comparing the administrative procedures with and without STORK integration - and administrative simplification were the most appreciated features. Interestingly, end-users placed cost savings in a distant third place, confirming perhaps the fact that businesspersons and end-users in general are willing to pay for convenience.

Overall, around two thirds of the users confirmed that the quality of the STORK 2.0-enabled services was improved with respect to the previously available service, and about the same number of end-users declared their willingness to recommend the STORK 2.0-enabled services to other businesspersons.

The evaluations of STORK 2.0 by the piloting SPs was significantly more favourable, both in terms of a more enthusiastic recognition of benefits and even from a costs/benefits point of view. In fact, nine out of ten piloting SPs reported either some or a significant positive contribution of STORK 2.0 integration to the overall Business Value of their service, and seven out of nine responding SPs found that the benefits justified the costs in integrating the services. Part of the positive economy of the STORK 2.0 approach is due to significant re-use of components of an integrated system and in the general experience gained which would significantly reduce the integration costs of future services.

In general, integrating an existing eGovernment service took more effort than anticipated, even when project-related costs and overheads are not considered, and the costs over all the partners was quite variable, in large part due to the greater complexity of the AUB procedure over the basic authentication and to the extent of the modifications required to allow the eGovernment service to handle foreign eID information for users and companies. All in all, though, both development costs and operating expenses were not deemed unreasonable.

Although increases in users and cross-border markets were limited, due to the limited extent of piloting, the most important Business Value benefits, those most strongly indicating the likelihood of adoption and sustainability of STORK 2.0 services, were highly positive. Among these were the cost and time savings[1], the improved quality of service, the overall positive costs/benefits analysis and the improved economy of STORK 2.0 solutions in the medium term. These, together with the willingness of SPs to maintain pilot services after the project and their identification of future service opportunities were strong indicators of sustainability and adoption.

We include some “unedited comments” from SPs:

> *NL: Connection of the eGovernment portal to STORK 2.0 and development of a solution for identity reconciliation is a significant step up to eIDAS and therefore definitely worthwhile. However, implementation will benefit from a more mature integration package.*
>
> *LU: Benefits in terms of global interoperability - it’s a first step to eIDAS - but litle real gain in user volume.*

[1] It is difficult to estimate precise or concrete time savings given the fact that some savings are in total elapsed procedure time, others in time spent completing the procedure and still others savings of time for avoided travel. In some cases days of elapsed procedure time and visits to Business Registers are saved when credentials are produced automatically through the STORK 2.0 network. In other cases minutes and hours are saved when procedures are handled online, with already existing, national eID credentials, and when powers credentials are produced and validated instantaneously.

EE: Promoting cross-border services and reducing investors´ costs gives to STORK 2.0 significant positive value. Trustworthy services will help to increase usage of cross-border services even more in the future.

4.2 Contribution of the pilot to STORK 2.0 benefits

The following paragraphs present those pilot benefits that most directly contribute at the project-level as measured according to the Common Technical Criteria - Functionality, Interoperability, Security, Maintainability, Scalability/Flexibility, Reliability/Maturity, Portability and Business Value – along with the additional criterion, Adoption

4.2.1 Functionality and Interoperability of the STORK 2.0 infrastructure

Metric F.1 - Implementation of Use Cases.

The implementation and piloting of the different use cases was partially, but significantly successful: the two most important use cases involving basic authentication (AU or AuthN) and authentication on behalf of a legal person (AUB) were successfully tested: AU in all ten piloting SPs (AT, EE, GR, IS, IT, LT, LU, NL, SI and SK) and AUB in eight MS (AT, EE, GR, IS, IT, LT, SI and SK) and six SPs (AT, EE, GR, IT, LT and SK). The third use case, involved the creation of delegated powers as part of the SP service, was implemented in some SPs but could not be piloted because the underlying Powers Validation function was not fully tested and deployed in core STORK 2.0 production infrastructure.

The overall evaluation of the metric although partial, must still indicate significant achievement with respect to the previous STORK project, with respect to objectives and with respect to the requirements of the eIDAS Regulation.

Metric F.2 - Implementation of Use Case variations.

Here, too, the pilot met with partial success: some variations of the AUB procedure (simplified user interface at the B-IDP) were implemented and deployed, some variations were implemented and tested in both common software and at SPs, but not deployed for lack of time (persistent logon, or SSO), and some variations were not implemented (3-MS authentication scenario; fully chained mandates).

A mitigating factor is that the un-deployed functionality is significantly beyond the requirements of eIDAS Regulation.

Variations 3, 4 and 5 of main CFUC#1 (simplified user interface, persistent logon (SSO) and 3-MS scenario) were each successfully implemented in at least one SP/MS.

Metric I.1 - Verification of cross-border services.

Considering the achieved interoperability status illustrated in Table 3 and Table 4 of Section 2.4 there were (at least) 32 different combinations of MS-MS cross-border transactions verified with respect to the 28 that were planned.

Therefore the metric was successfully achieved.

Metric I.2 - QAA mix – successful authentication with different combinations of QAA values.

An important PEPS function is to guarantee that communication between the end-user and the Service Provider (SP) is established with sufficient certainty as to the identity of the end-user and adequate security of the communication and information exchanged. The SP specifies the desired level of Quality Authentication Assurance (QAA) in the initial

Authentication Request, and the PEPS interacts with the IDP to determine whether the request can be satisfied or not. Both internal testing and inspection of the actual piloting period logs verified that three different QAA levels had been successfully requested and respected (QAA=1, 3 and 4) so the target success criterion of two different values was met and exceeded.

Metric I.3 - AQAA mix – successful authentication with different combinations of AQAA values.

One of the strengths of the STORK 2.0 approach is the flexibility of verification of legal person or company credentials offered in the AUB procedure. One aspect of flexibility is the possibility for the SP to request and receive the Attribute Quality Authentication Assurance level (AQAA) for attributes describing the company (Legal Person attributes) and the end-users powers to represent the company (mandate attributes). The SP can then evaluate whether the level of trust in the received information is sufficient to grant the user access to the SP application. Different Services or different operations may require different assurance levels so a goal was set to verify at least two different AQAA values in different AUB procedures.

Based on partner testing reported at the project wiki and on the inspection of PEPS logs it was seen that in piloted AUB operations three different levels of AQAA were transmitted (corresponding to the AQAA levels 1, 3 and 4). Thus the goal was achieved.

Metric BV.10 - Benefits for MS interoperability layer, IDP/V-IDP, B-IDP (Business Register).

The major direct contribution to the MS interoperability layer made by the eGov4Business pilot consisted in the assistance provided to the integration of the national B-IDP, Business Register or Mercantile register or Mandate Provider. In some cases the SP was the Business Register, in others it was a nearby collaborating agency, but in all cases, the main functional and data specifications for integrating the B-IDP were developed as part of the eGov4Business specifications. Eight of the ten piloting countries successfully integrated their B-IDPs and were able to verify the cross-border AUB procedure.

The success criterion for metric BV.10 called for 66% of all eGov4Business MS to have their B-IDP integrated, thus since 8 is only 62% of 13 the target is only partially reached, but the goal can be considered as substantially achieved.

4.2.2 Security, Maintainability, Scalability/Flexibility, Reliability/Maturity

Metric S.3 - SP rating of security of STORK 2.0 infrastructure

When SPs were asked to rate the security of the STORK 2.0 infrastructure not one gave it a negative rating, so the metric is achieved.

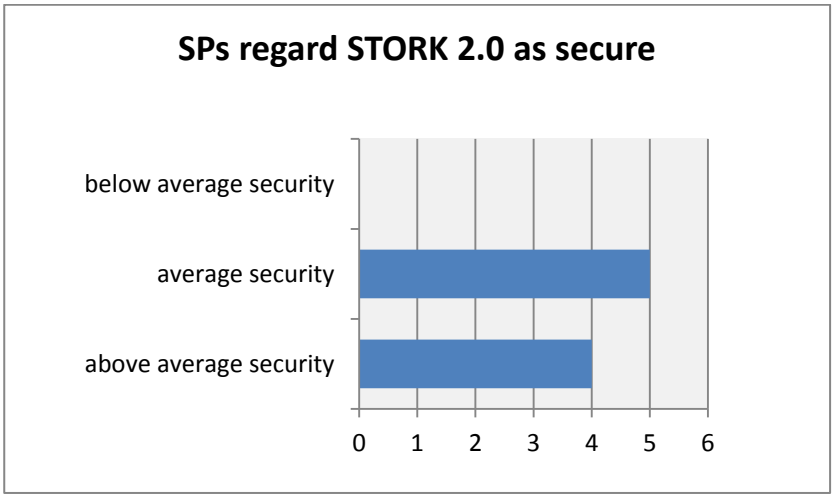

Figure 21: SPs rating of the security of STORK 2.0 infrastructure (metric S.3, SP Questionnaire Q24)

Metric M.4 – Smooth migration to new SW versions of STORK 2.0 with testing of new functionalities and regression testing of old

Those SPs that had been piloting for a sufficient amount of time to handle software releases estimated the amount of the time needed to migrate the SP software to comply with new versions of STORK 2.0 software, including time for tests to check that previous SP services kept on working along with the newly available features.

Half of the eight respondents estimated the time between 1 and 2 person-months, the other half at more than 2 p-m. Thus, no SP achieved the target of < 1 person-month of effort, and the metric was not achieved. This criterion must be re-evaluated in the future to determine whether it is too strict.

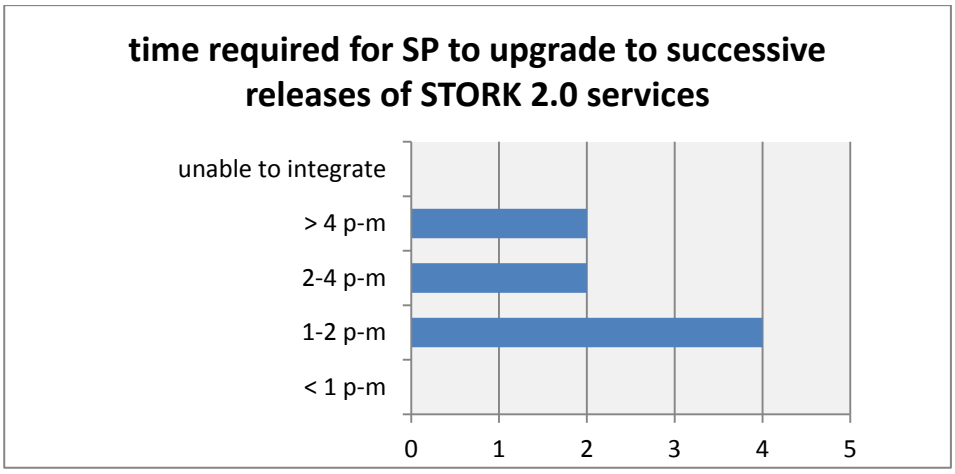

Figure 22: Half of the piloting SPs successfully performed STORK 2.0 service release upgrades in less than 2 months (metric M.4, SP Questionnaire Q28)

The main reason given by several partners for requiring more time than anticipated for upgrades, was the need to repeat extensive testing coordinated with other MS.

A secondary part of the metric required partners to evaluate qualitatively the functional improvements implemented with successive software releases, in particular whether new release features brought significant improvements to the service.

In this case, 8 out of 10 SPs felt that improvements were present and 5 of these rated the improvements as significant.

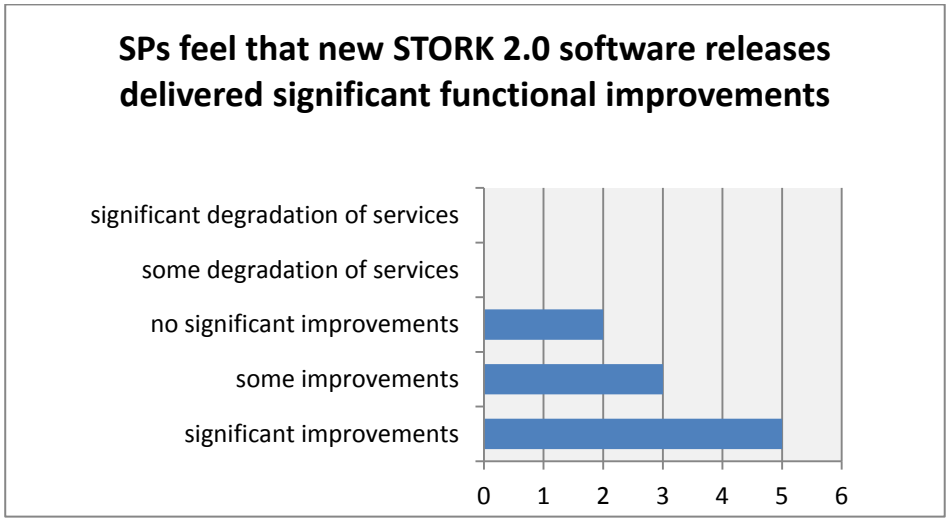

Figure 23: SP evaluation of functional improvements of successive software releases (metric M.4, SP Questionnaire Q26)

Because of the unexpected number of subsequent releases and software patches several partners felt that the costs for updates were excessive, and they preferred to wait for more stable releases, but in general partners were appreciative of the new functionalities. In particular, more than one partner noted that functionalities regarding legal entities are highly relevant to enable full SP deployment possibilities.

Metric SF.2 - Increase in number of available SP services from Go Live.

As seen in Figure 3 of Section 2.3, an increasing number of services has been put in production and the desired result is achieved. In fact, to take full advantage of the Piloting period several SPs were able to release services incrementally, groups of features or one use case at a time.

Metric RM.4 – Impact of STORK 2.0 integration on reliability and level of service.

SPs were asked to evaluate the impact STORK 2.0 integration had on the reliability and the level of service. The target of no negative impact indicated was reached. As might have been expected, most SPs indicated no net impact, since for many, replacing the authentication mechanism was not even a possible source of improved service level or reliability.

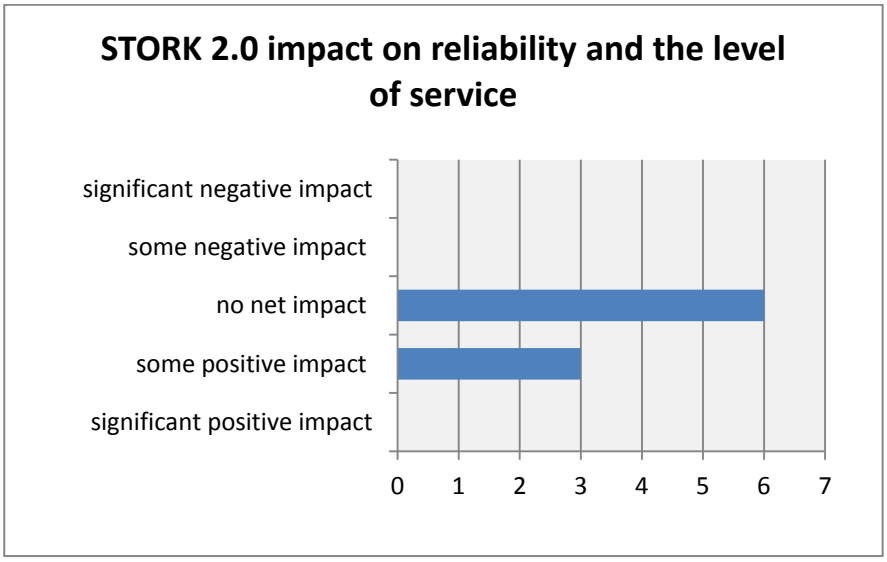

Figure 24: SP evaluation of impact of STORK 2.0 integration on reliability and level of service (metric RM.4, SP Questionnaire Q30)

4.2.3 Business Value, Portability and Adoption

Metric BV.15 - Willingness to pay for the new service.

When asked if they would be willing to pay for STORK 2.0 services no SP declared itself willing. Most were undecided, but the overall feeling of SPs certainly reflected the policy of the eIDAS Regulation to require that cross-border authentication be free of charge when carried out in the context of a public service.

With hindsight, and considering the policy of the eIDAS Regulation, this metric makes little sense and the fact that it has not been achieved is of little relevance.

The success criterion for metric BV.15 was therefore not met.

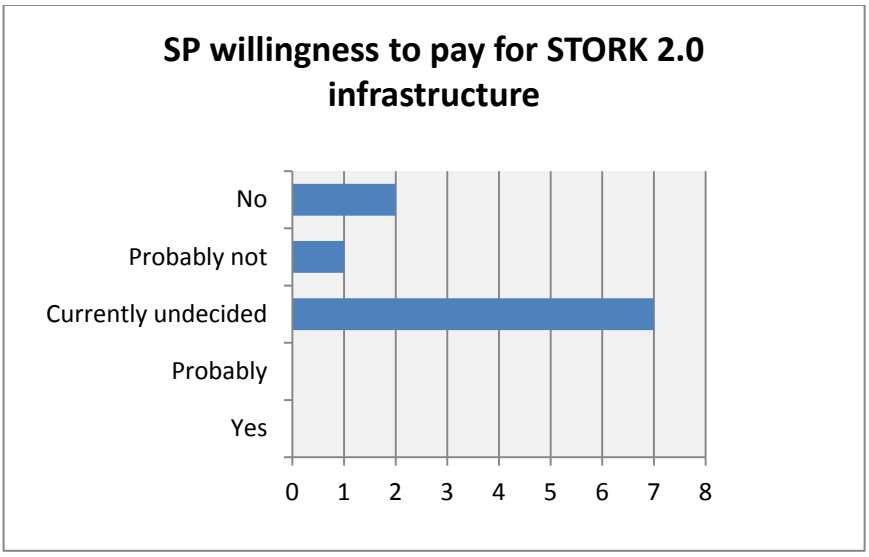

Figure 25: SP willingness to pay for STORK 2.0 infrastructure (metric BV.15, SP Questionnaire Q14)

Metric BV.16 - N. of SPs intending to continue pilot service after the project.

One of the more comforting metrics regarding the interest of SPs in guaranteeing sustainability for STORK 2.0 services was the willingness shown when asked if they would keep the STORK 2.0 enabled services up and running even after the pilot period and after the end of the project. Between definite and probable Yes answers, a total of 8 out of 10 SPs indicated their positive intentions. At the end of the project, this number grew to 10 SPs and also the 8 B-IDP partners confirmed same willingness.

This value exceeded the target of 66% of SPs and the metric success criterion was achieved.

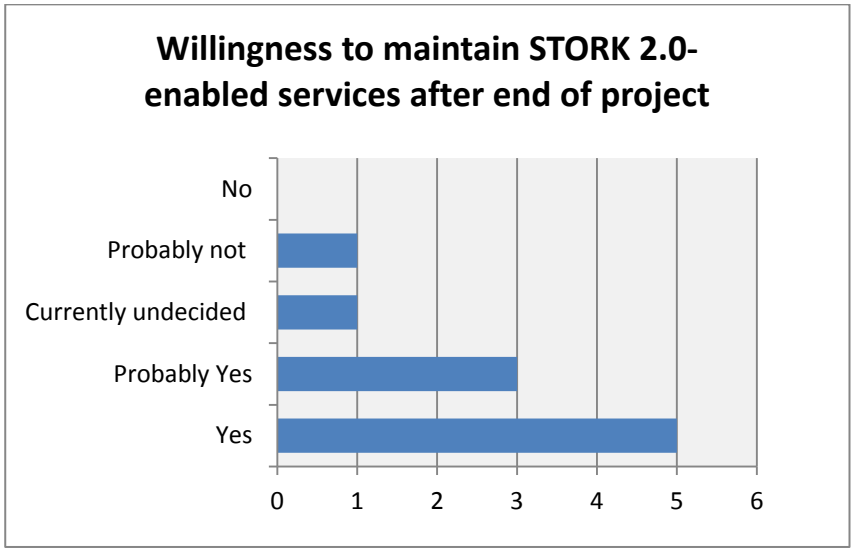

Figure 26: SP willingness to maintain STORK 2.0-enabled services after end of project (metric BV.16, SP Questionnaire Q13)

Metric P.2 - Platform portability from SP perspective –n. of diff. platforms (like Java/PHP)

Supporting the implementation of STORK 2.0 in a wide variety of Service Provider settings will facilitate and accelerate the diffusion of STORK services. It was required that the piloting should verify STORK 2.0 integration in at least two different SP server platforms (metric P.2).

In fact, as verified by the responses to Q35 of the SP Questionnaire, the following different SP environments and technologies were used to integrate eGovernment services with the national STORK 2.0 infrastructures (and thus the metric is achieved):

- Python; PostgreSQL;
- Ubuntu LTS Server, Java v.1.7, Tomcat v.7
- Java EE, jBoss, CAS Jasig framework with bundled Spring workflow library, OpenSAML Library
- Opercaine Cenos 6
- Java 1.7, Tomcat, Postgresql, Apache 2.4
- Java 6, Jway Form server
- Linux, Oracle identity and access management, Liferay, JAVA
- Java v.1.7, Tomcat v.7, REST

- Websphere Portal, Java-Struts, Spring frameworks

Metric A.3 – Sustainability.

The complex concept of Sustainability was measured as a composite of the following different Business Value metrics: BV.08, BV.09, BV.14, BV.16, BV.17, BV.18.

Since each of these metrics achieved its target level of success, the metric A.3 is considered as achieved.

4.3 Pilot-specific benefits assessment

The next paragraphs assess those pilot benefits which were more specific to the eGov4Business pilot. In particular, we consider some overall evaluations of benefits and costs by both SPs and end-users, as well as some specific benefits such as savings in time, administrative simplification, improvements in the Service, in its market reach and in the evaluation of the SP in the eyes of stakeholders, end-users and even the EC.

4.3.1 Overall costs/benefits analysis and the "STORK 2.0 value proposition" – Service Providers' point of view

Metric BV.09 - Overall costs/benefits analysis for integration of STORK 2.0 services in existing eGovernment platform.

Service Providers were asked to assess the overall costs/benefits of the STORK 2.0 value proposition, in particular, if the benefits outweigh the incurred costs – direct monetary costs and effort. Positive responses greatly outweighed negatives, in fact only two non-positive responses were given – one negative and one neutral – and each was primarily motivated by legal or organisational issues that were regarded as temporary in the respective MS.

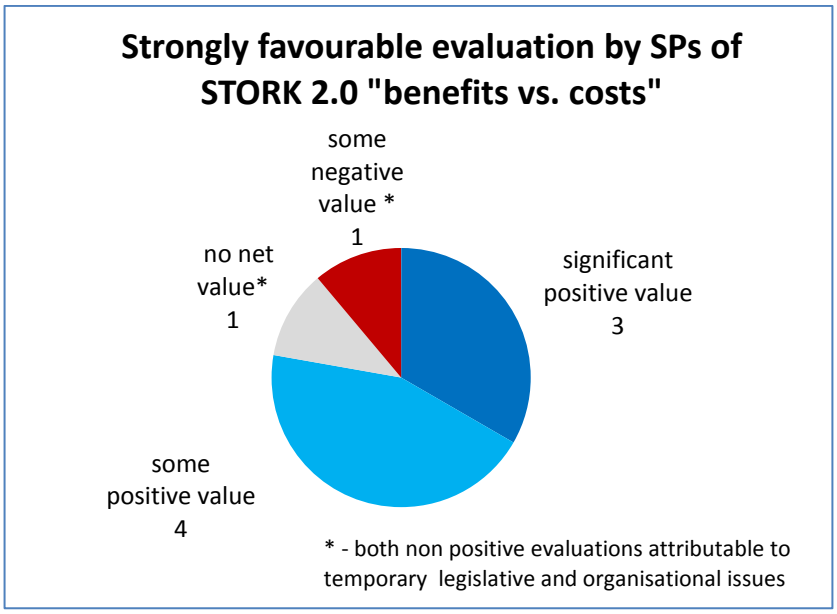

Figure 27: Costs/benefits evaluation by SPs of the overall STORK 2.0 value proposition (metric BV.09, SP Questionnaire Q21)

Metric BV.04 - Concrete benefits for Service Providers.

This metric verifies the existence of a significant number of common, concrete benefits for SPs. It is a composite evaluation of the following different individual concrete benefits, addressed in the SP Questionnaire questions Q5 – Q11:

- The SP's qualitative evaluation of the contribution of STORK 2.0 to the Business Value of the eGovernment pilot service (SP Questionnaire Q5)
- The SP's qualitative evaluation of the impact on the stakeholders' view of the pilot service (SP Questionnaire Q6)

- The SP's qualitative evaluation of the impact of STORK 2.0 on the quality of service (SP Questionnaire Q7)
- The STORK 2.0 impact on compliance with EC policies (SP Questionnaire Q8)
- The role of STORK 2.0 in opening the pilot service to cross-border end-users for the first time (SP Questionnaire Q9)
- The impact of STORK 2.0 on reducing the time of administrative procedures for the end-user and for the SP (SP Questionnaire Q10)
- The contribution of STORK 2.0 in reducing costs of administrative procedures (SP Questionnaire Q11)

The success criterion chosen for the combination of values was that at least one of the benefits should have been cited by 90% of SPs and three other benefits should have received positive evaluations by 60%.

In fact, we will see, in the paragraphs that follow and in Section 4.4, that after examining all the metrics related to the above list of SP questions that the success criterion has been fully achieved and exceeded because

- 100% of SPs indicated positive impact on improved EC compliance (see section 4.3.5),
- 90% of SPs indicate STORK 2.0 helped increase Business Value of the pilot service, improve the stakeholders' view of the service and reduce the time for the administrative eGovernment service (see Figure 28 and Figure 29, below and section 4.3.6),
- 70% of SPs declared that STORK 2.0 had contributed to improve service quality and to expand the cross-border market (see sections 4.3.3 and 4.3.8),
- 60% of SPs judged that STORK 2.0 had helped reduce administrative costs (see section 4.4.3)

Nine out of ten piloting SPs felt that STORK 2.0 integration added positive Business Value to their eGovernment service. The one neutral voice added the comment that the lack of impact was due to the fact that the SP implemented some key features late in the piloting period. Similarly other SPs felt that the mildly positive response could become significantly positive in the future as the service became more widely known and used.

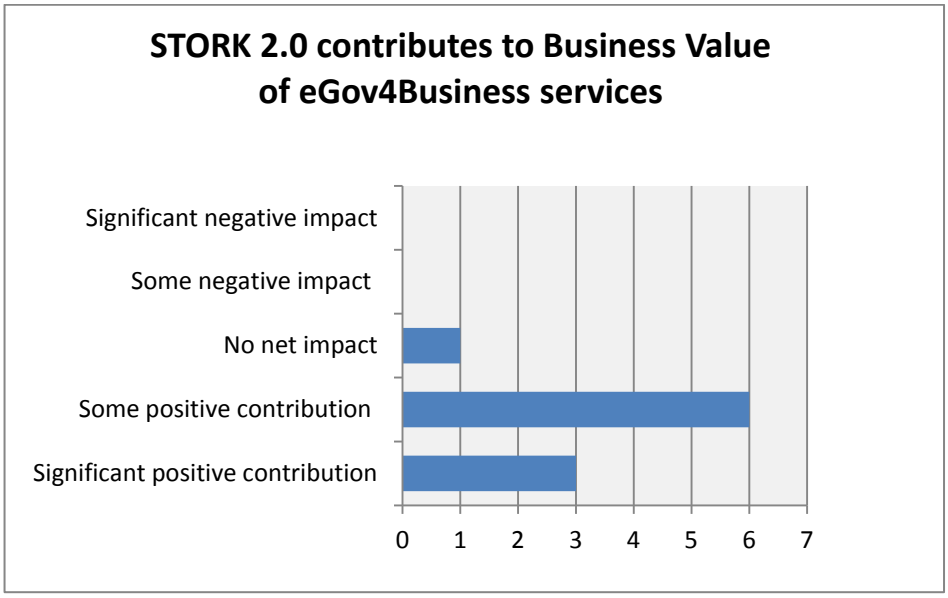

Figure 28: Impact of STORK 2.0 on Business Value of SP services (metric BV.04, SP Quest Q5)

Similarly, nine out of ten piloting SPs felt, slightly less strongly, that STORK 2.0 integration had a positive impact on the stakeholders' view of the pilot service.

Once again, partners explicitly commented, "Marketing is essential and will increase stakeholders´ perception in the future."

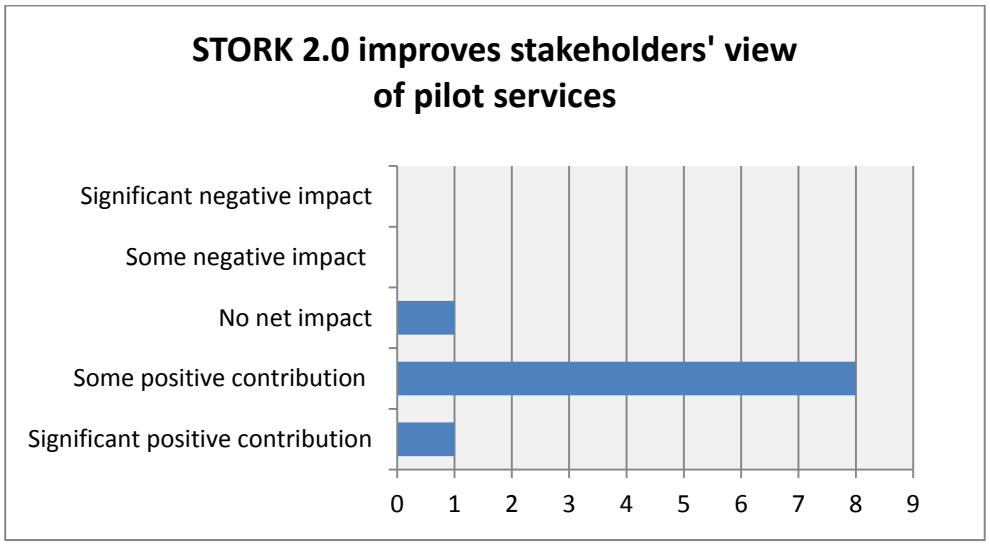

Figure 29: Impact of STORK 2.0 on Stakeholders' perception of services (metric BV.04, SP Questionnaire Q6)

4.3.2 Overall evaluation of the STORK 2.0-enabled services – the end-users' point of view

As was the case with Service Providers, in addition to being asked to express their opinions on specific issues and benefits of STORK 2.0-enabled eGovernment services, they were also asked several questions of a more general or mixed character.

Metric BV.01 - Documented benefits for end users.

End-users were asked to confirm or deny the fact that there were any of a series of benefits in the STORK 2.0 integration (new procedure perceived as easier, more convenient, time saving and/or reliable). Positive responses, at 52%, outweighed negative ones 2:1, but there were a large number of undecided respondents, which led to not reaching the threshold defined in the success criterion of 85% positive responses.

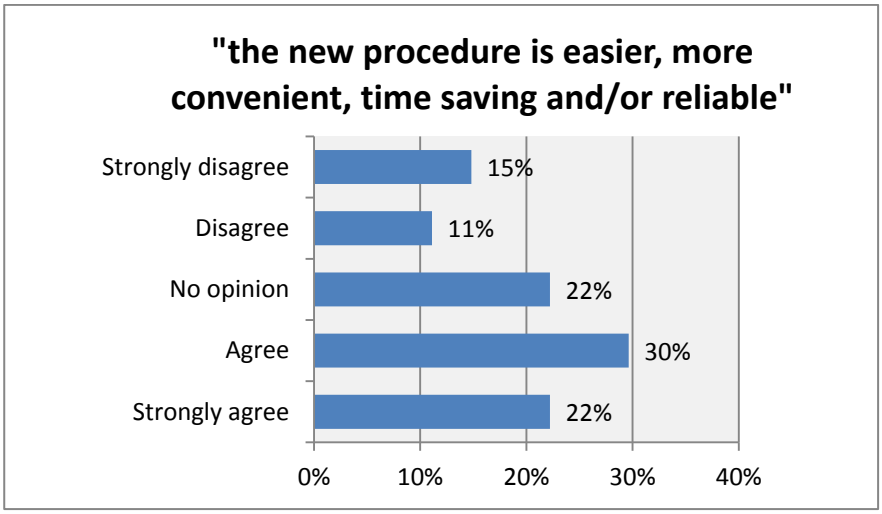

Figure 30: Positive impact of STORK2 on SPs' perception of overall Quality of Service (metric BV.01, End-user Feedback Form Q12)

Although not "critical" this gap is fairly worrisome; 26% of unhappy end-users is not a situation to leave unattended. The major reasons for this gap could be found in specific issues with the user interface and STORK 2.0 procedure flows as well as in general issues regarding the immaturity of eID usage, in particular in cross-border settings.

When asked to choose the greatest benefit derived from being able to access foreign eGovernment services using native identity credentials end-users had clearer ideas. Saving time was favoured by 47% of respondents and Simplification of administrative procedures was chosen by 34%. Cost savings and Security were at a distant 11% and 8% respectively, a clear indication that end-users prefer (or more directly perceive) convenience to cost and security.

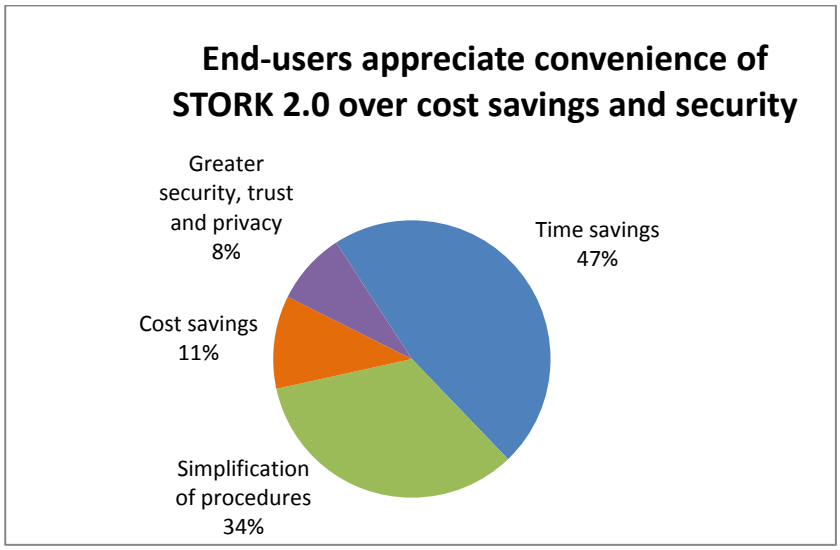

Figure 31: End users preferences for benefits provided by STORK 2.0 integration (metric BV.01, Feedback Form Q8)

Metric A.1 - Impact on end-users; expectations for benefits.

Another overall measure of end-user satisfaction was measured in end-users readiness to recommend STORK-enabled services to other businesspersons.

The success criterion of 66% was substantially reached.

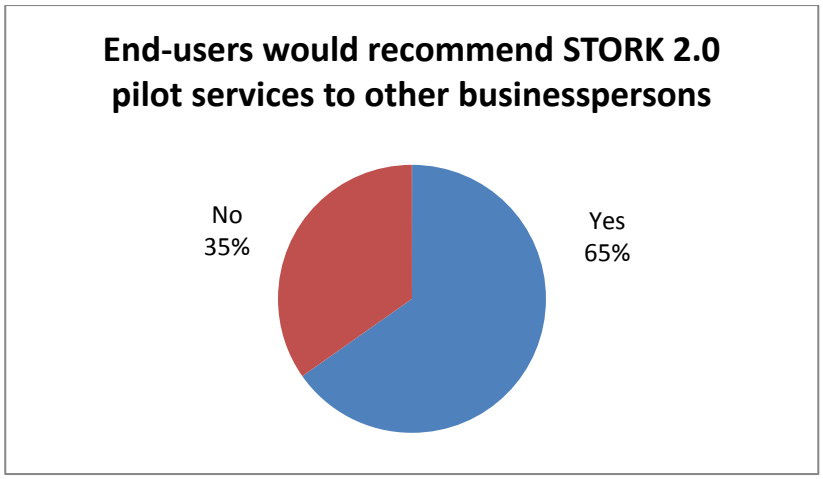

Figure 32: End users readiness to recommend STORK 2.0 enabled services to others (metric A.1, Feedback Form Q17)

4.3.3 Improvements in the Quality of SP services

Metric BV.07 - Improvements in (perceived) quality of service. Value

The first indicator of quality of service is an end-user's rating of ease of use and "user experience". 56% of the responding end-users found the system Satisfactory or Very satisfactory and another 24% found the system Adequate, which gives an average of 68% positive responses, achieving the target of over 66% positive responses.

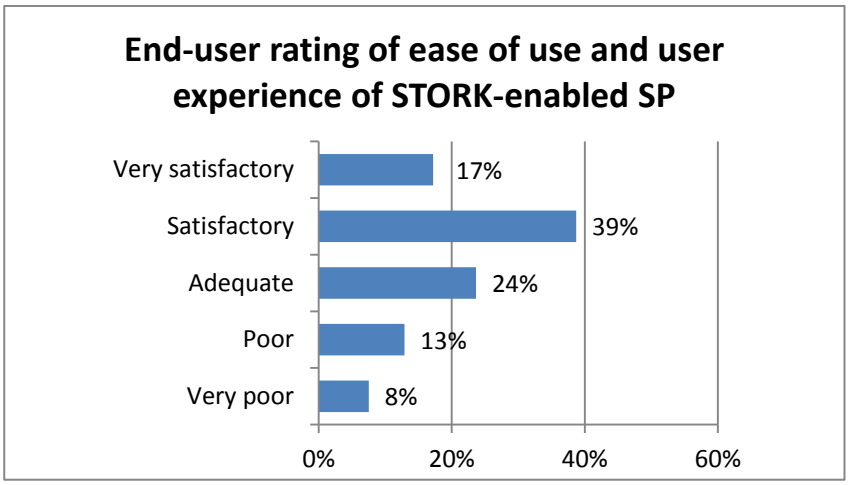

Figure 33: End-user rating of ease of use and user experience of STORK-enabled SP (metric BV.07, End-user Feedback form Q6)

End-users were also asked to evaluate how their opinion of the eGovernment SP had changed after using the new STORK 2.0-enabled procedures. Responses were similar to other evaluations with a slightly greater tendency away from the extremes and towards the middle and slightly improved categories.

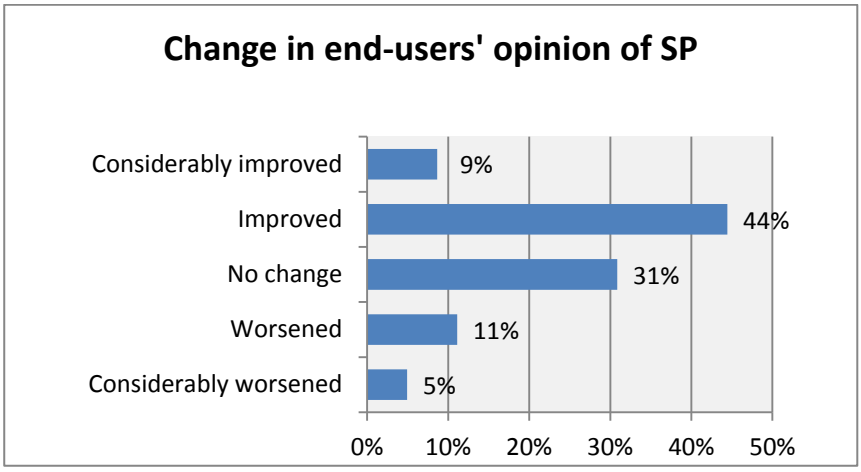

Figure 34: How STORK 2.0 integration affected the end-users' opinion of the SP (metric BV.07, End-user Feedback form Q9)

This tendency towards the upper-middle rating was even more pronounced when SPs were asked to give their own opinions of the impact of STORK 2.0 integration on the overall Quality of their services.

In this case, only the intermediate ratings were chosen: 7 out of 10 SPs indicating "Some positive contribution" to overall service quality from STORK 2.0 integration and the remaining three SPs evaluating STORK as having "No net impact" on service quality. In particular, no SP attributed to STORK a negative impact on service quality.

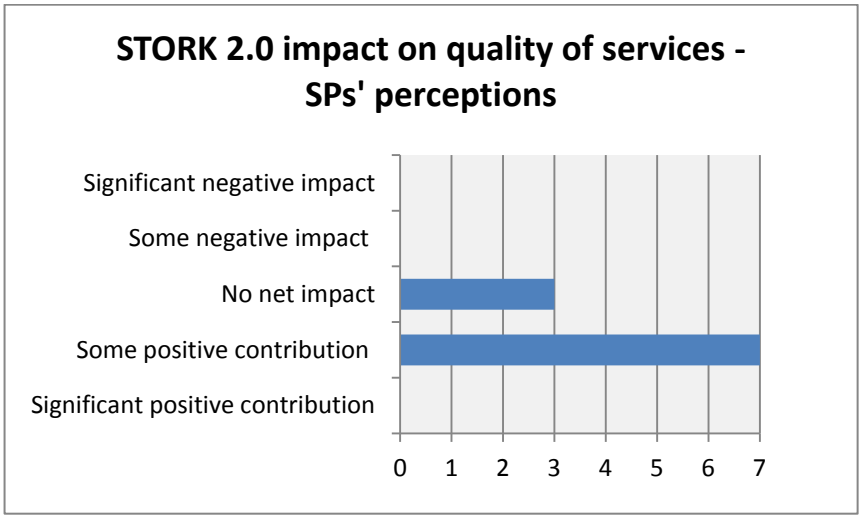

Figure 35: Positive impact of STORK2 on SPs' perception of Quality of Service (metric BV.07, SP Questionnaire Q7)

The success criterion for this metric required that the average of all the positive ratings for the three individual factors should be greater than 66%; this has been substantially achieved.

4.3.4 Definition of a shared mandate attribute structure and usage

The eGov4Business pilot contributed heavily in the definition, specification, implementation and validation of all things related to company powers and the procedure of authentication of a person acting on behalf of a legal person. This includes the technical activities of defining the structure of the mandate attribute and the development of some special software

procedures, contributed to the common code, for handling the corresponding SAML token, as well actions addressing the organizational, semantic and legal issues involved in achieving cross-border interoperability. In particular, several details in the model and implementation of the AQAA scheme were also influenced by input from the eGov4Business pilot. All these contributions enriched STORK 2.0 results and were useful in showing the way for future developments.

Metric I.4 - Various mandate types used (semantic/legal perspective).

A person acting on behalf of a company can possess different types of powers of representation from full, general powers to more specific and limited powers. The typeOfPower attribute of the STORK 2.0 mandate token expresses, in a simplified, but agreed-upon form, a brief taxonomy of role-oriented company powers. Since there is no EU-wide legal basis for these values – no standard description or ontology exists - each national infrastructure had to create a suitable mapping from the national system of powers to the STORK 2.0 model.

The most important values correspond to full powers and no powers, but an additional value, "Other" proved useful for indicating cases of probable full powers which required human verification (for example, to confirm the fact that free-text fields did not reduce or otherwise limit the powers indicated through machine processable parameters.

Pilot testing, as documented in SP transaction logs and in the end-user feedback forms indicated that the three values "General powers", "None" and "Other" provided a reasonable first step towards cross-border interoperability. All three values were effectively used, satisfying the success criterion of the metric I.4, which required at least two different TypeOfPowers values to be successfully piloted.

We note that the implementation of the eIDAS Regulation does not make explicit use of a model of different representation powers: the juxtaposition of two persons is used to indicate that one person represents (with presumably full powers) the other. In fact, clause 2 of Art. 11 of [16] reads, "A minimum data set for a natural person representing a legal person shall contain the combination of the attributes … for natural persons and legal persons when used in a cross-border context".

More "exotic" types of mandates were discussed, such as joint mandates and chained mandates, but they were modeled and implemented only in their most simple form. For example, the problem of transmitting a full chain of mandates – one person representing another who represents a third, and so on - with all the details on the intermediate mandates was declared as useful in a final system, but beyond the possibilities and necessities of the current pilot. Such information may be necessary, however, to guarantee validity and legal value of representation powers under certain conditions.

4.3.5 Compliance with EC regulations; Early piloting of eIDAS-like or eIDAS compatible eID solution

As indicated in section 2.2.2, an important goal for Piloting SPs was to increase or facilitate their compliance with different EC Regulations and Directives, including sector-specific norms in areas such as Agriculture, Labour, Environment as well as transversal measures like the Services Directive and the eIDAS Regulation. Very often synergy was created internally within the SP since STORK integration enabled simultaneously the integration of the SP with a national eID (or eIDAS) infrastructure which in turn helped satisfy the cross-border access requirements of a specific sectorial norm.

Metric BV.08 - STORK 2.0 contribution to EC policy aspects (Serv. Dir., eIDAS)

When specifically asked whether STORK2.0 was helpful in enabling better compliance with EU policies SP responses were unanimously positive, differing only in degree of enthusiasm.

The success criterion is therefore achieved.

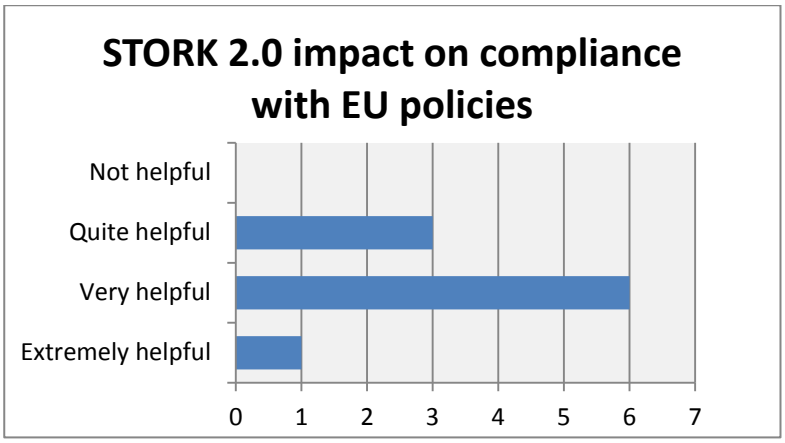

Figure 36: STORK 2.0 is "very helpful" in achieving EU policy compliance (metric BV.08, SP Questionnaire Q8

Metric F.3 - Successful authentication procedures, individual and "on behalf of" a company or a person

We saw in Section 3.3.1 that the metric UU.3 measuring successful transactions as indicated by the end-users in their feedback forms was satisfied. Metric F.3 looks at the same data from a more detailed level, looking at which STORK 2.0 procedure was being attempted, basic authentication or the more complex AUB. In spite of the greater complication of the AUB procedure the success rate is basically the same as for the simpler Authentication as a natural person. This may be due to the fact that a user with credential to represent a company may already be more prepared than users attempting basic authentication.

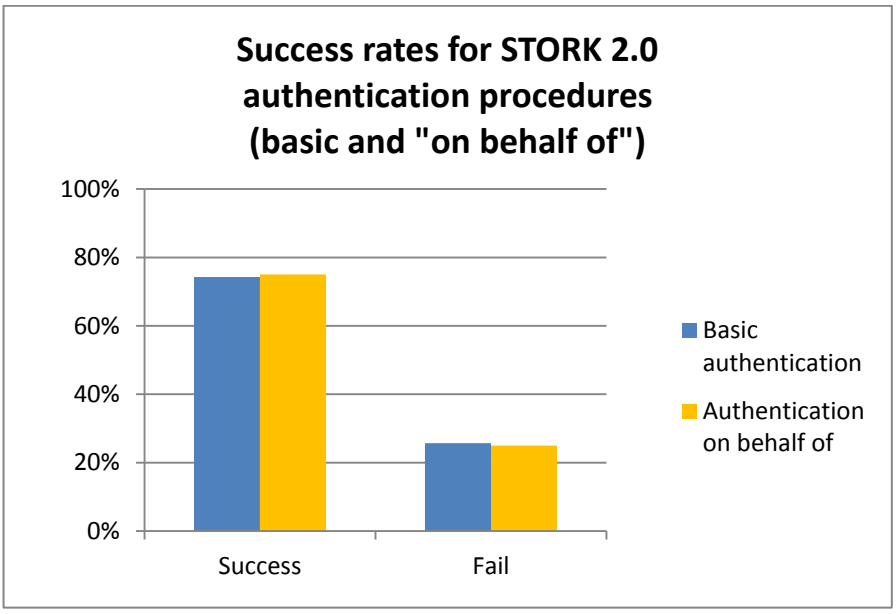

Figure 37: Four out of five authentication procedures were error-free (metric F.3, End-user Feedback form Q4 and Q5)

4.3.6 Time savings for End-users and SPs

Among the goals of the EC Services Directive are the saving of time for users and providers of administrative services. All SPs, Points of Single Contact and general eGovernment portals, were asked to estimate these two quantities for their STORK 2.0-enabled services.

Metric BV.06 - Average estimated reduction of the length of time of the administrative process.

When asked how enabling their services to use STORK 2.0 contributed to reducing the length of time of the administrative processes for end-users (taking into account the manual paper processing and validation of documents, waiting periods, physical presence etc.) 9 out of 10 SPs indicated some saving of time (including those cases when the procedure would not have been otherwise possible, online) and 7 SPs indicated a savings over 50%. In terms of savings of elapsed time, even taking into account the large variability of the measure "elapsed time", the indicated savings are to be measured in days and weeks of quicker service – for a businessman trying to open up an activity abroad that is a significant business advantage.

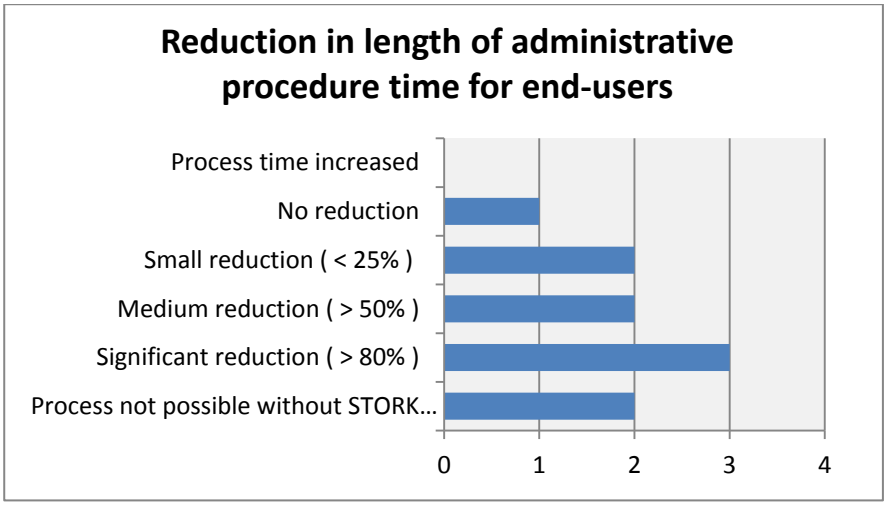

Figure 38: Time-saving for end-users of administrative procedures (metric BV.06, SP Questionnaire Q10)

In like manner, SPs estimated their own reduction in time for processing STORK 2.0-enabled eGovernment requests. Here, savings were slightly more modest indicated by 7 out of 10 SPs of which only 5 indicating a better than "Small reduction" (in time).

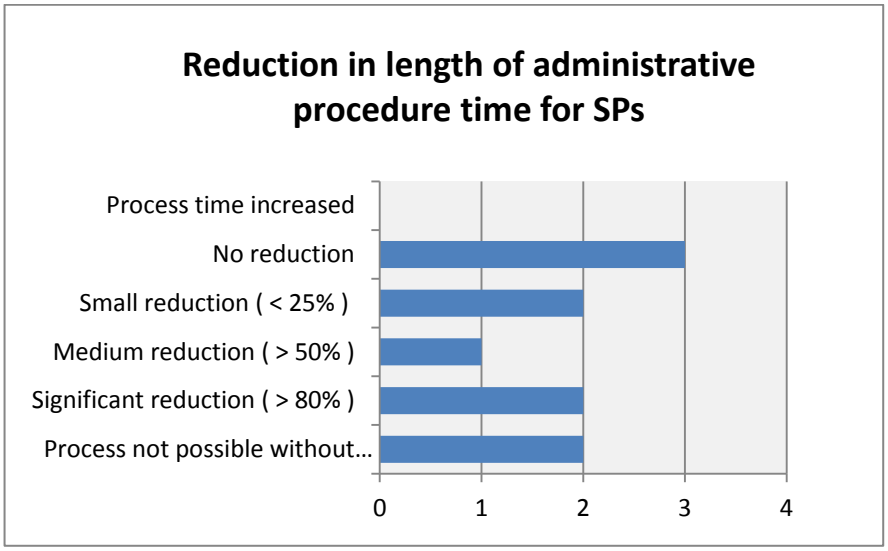

Figure 39: Time-saving for providers of administrative processes (metric BV.06, SP Questionnaire Q10)

The metric considers the average of these savings of the SPs, or 80% savings of which 60% are better than small savings, and the success criterion can be considered achieved.

4.3.7 Simplification of administrative procedures for users

Metric BV.03 - Documented simplification of administrative procedures for end users.

Over a third of end-users responding to feedback forms (Q8) indicated "Simplification of procedures" as main benefit (See Figure 31). In fact, 28 of the 71 respondents indicated Simplification as their primary benefit almost three times the pre-established success criterion level of 10 positive responses.

In fact, simplification was achieved in several moments of the eGovernment services, from the registration of new users using personal eID information supplied by the IDP to the authorisation to act on behalf of a company using Legal Person eID information and the mandate attribute. Some processes could be dealt with online, in real time for the first time, accelerating the overall process by days and weeks, and reducing the actual procedure time by a matter of hours, thanks to the automatic retrieval of credentials.

4.3.8 Potential widening of market and increase in customer base

Metric BV.13 - Services enabled by STORK 2.0 that would otherwise not have been available online across borders.

Seven out of ten eGov4Business SPs declared that STORK 2.0 has made it possible for foreign businesspersons to access services that otherwise would not have been available online. We note that negative answers indicate the presence of a prior, SP-specific system for registration and authentication of foreign end-users.

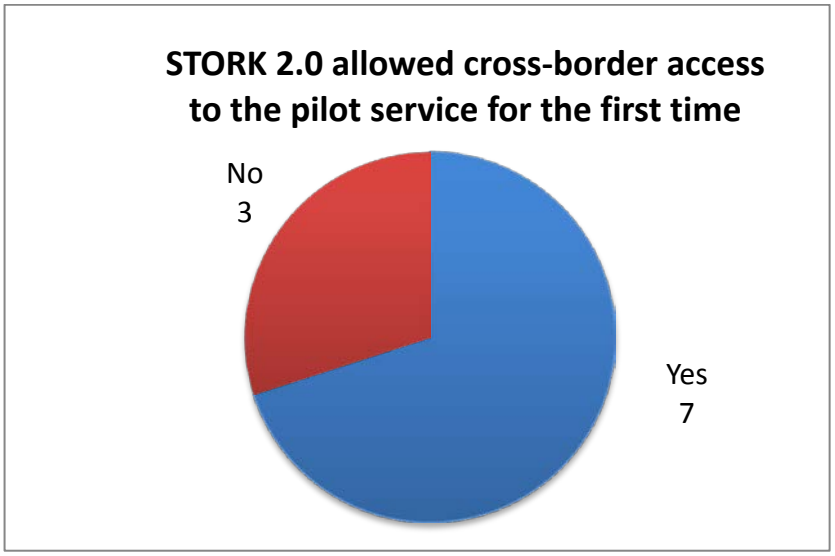

Figure 40: STORK 2.0 created new cross-border access for 7 out of 10 pilot services (metric BV.13, SP Questionnaire Q9)

The promising prospects of re-using STORK 2.0 integration to open new services, besides those already piloted in STORK 2.0, to European markets has already been exploited in LT and is being actively evaluated and planned in IT and EE. Moreover, agencies, ministries and eGovernment portals in close contact with pilot partners are also likely candidates for a "contagion" effect to appear. In fact, a Belgian Fisheries service has already integrated STORK for its Dutch users. See, for example, Figure 53 in Section 6.1.

4.4 Pilot-specific costs assessment

To better understand the costs and effort necessary to integrate a service with the STORK 2.0 network we consider the following macro categories of costs:

- Capital expenses:
    - Cost of development and adaptation of SP to STORK 2.0
    - Cost of integration with national STORK infrastructure
    - Additional one-time capital expenses
- Technical maintenance and operational costs

Additionally, to complement the overall costs/benefits comparison we also consider

- Cost of replacing the STORK 2.0 system with a different system for cross-border eID

4.4.1 Capital costs

Metric BV.17 - Costs of adapting SP service to cross-border, STORK 2.0 users.

The following chart shows the relative sizes of costs expected to be incurred in adapting and integrating an existing SP service to STORK 2.0.

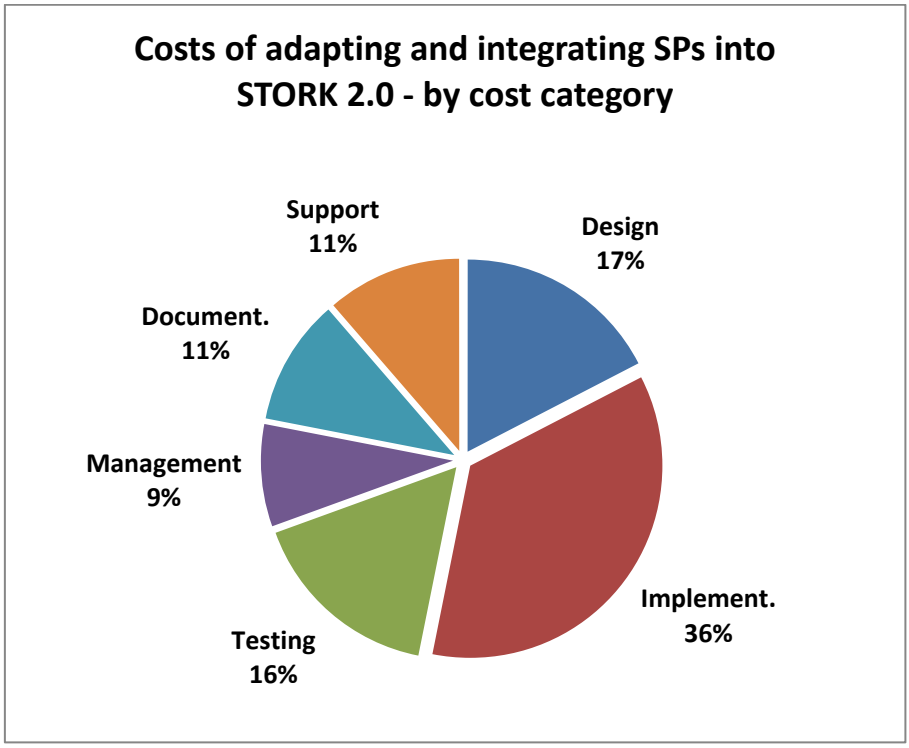

Figure 41: Costs of adapting and integrating SPs (metric BV.17, SP Questionnaire Q17)

Dividing these costs per (anonymous) partner confirms the relative breakdown, but highlights the high variability of overall expenses.

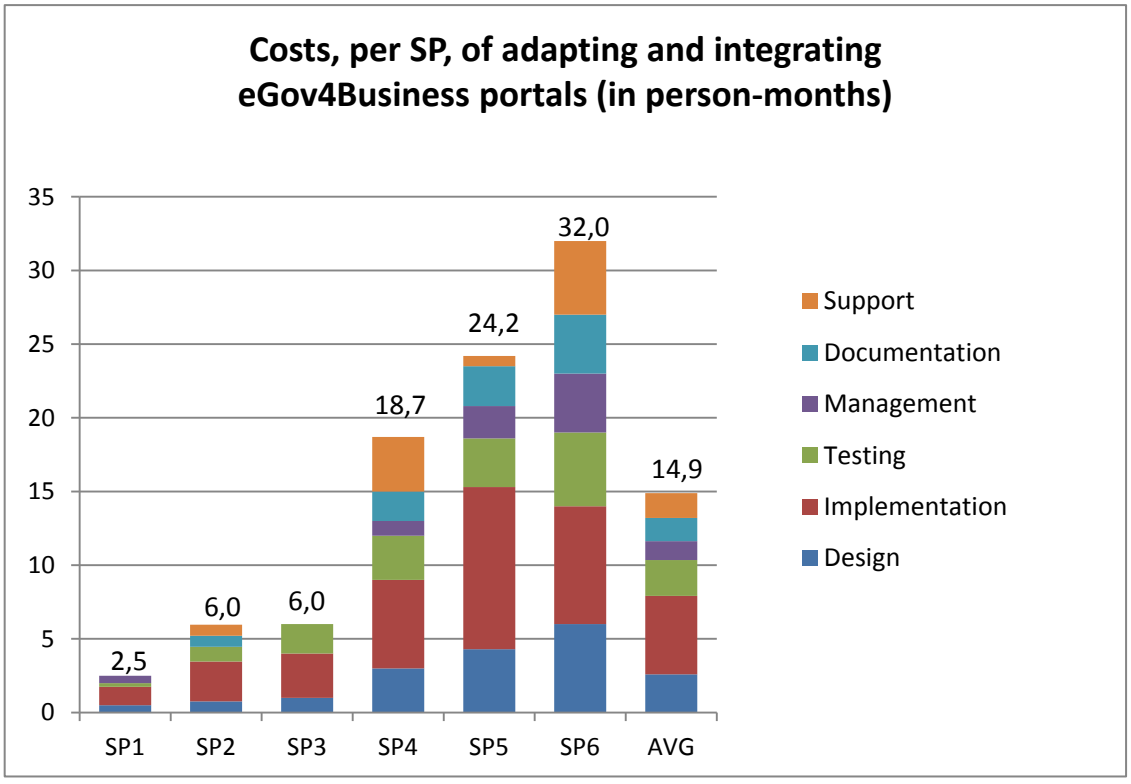

Figure 42: Costs per (anonymous) SP of adapting and integrating SPs (metric BV.17, SP Questionnaire Q17)

The large variation in costs is due to several factors:

- The different combinations of the STORK 2.0 functionalities implemented in the various SPs (see Figure 1),
- The number and complexity of the eGovernment services integrated
- The degree to which these eGovernment services were ready to accept eID information from other MS and the prior compatibility with STORK approach of the SP service authentication architecture (e.g., a high modularity of authentication services and identity management functions).

Detailed information on the costs illustrated in Figure 42 is provided in the following table.

Costs for adapting and integrating eGov4Business services/portals to STORK 2.0 (in person-months).

Partner names are kept confidential.

Partner SP	P1	P2	P3	P4	P5	P6	Avg.
Design	0,5	0,8	1,0	3,0	4,3	6,0	**2,6**
Implementation	1,3	2,7	3,0	6,0	11,0	8,0	**5,3**
Testing	0,3	1,0	2,0	3,0	3,3	4,0	**2,4**
Management	0,5	0,0	0,0	1,0	2,2	5,0	**1,3**
Documentation	0,0	0,8	0,0	2,0	2,7	4,0	**1,6**
Support	0,0	0,8	0,0	3,7	0,7	5,0	**1,7**
Totals	**2,5**	**6,0**	**6,0**	**18,7**	**24,2**	**32,0**	**14,9**

Table 6 : Main categories of Capital cost

Besides the implementation costs given above, some partners incurred additional, one-time capital expenses for expenses such as Administrative or legal fees, Acquisition of hardware, Hosting services, Additional technical training for developers, Support team training, Other development costs. Overall these can be viewed as follows:

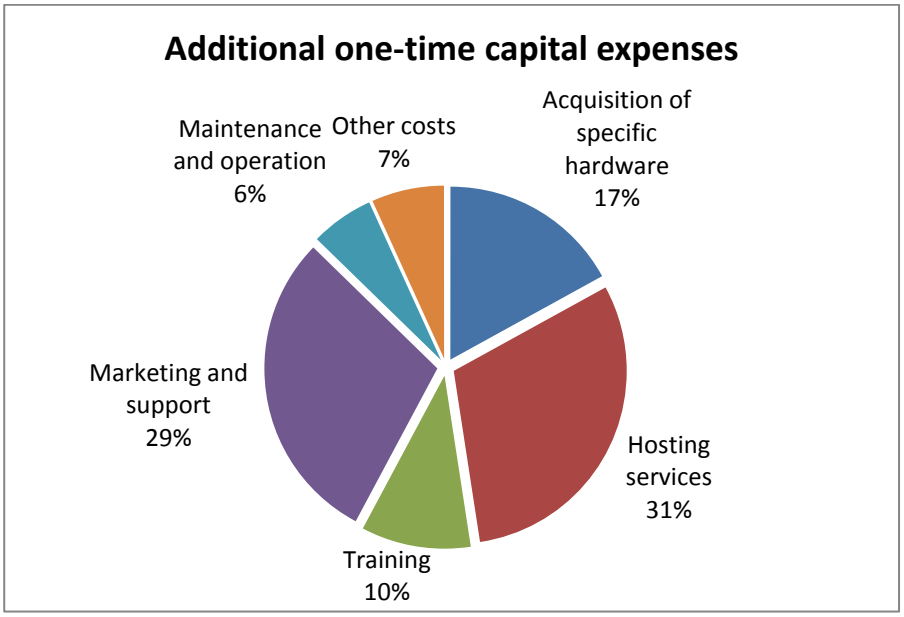

Figure 43: Additional one-time capital expenses (metric BV.17, SP Questionnaire Q18)

Detailed information on the costs illustrated in Figure 43 is provided in the following table.

Additional one-time capital expenditures							
Partner SP	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**Avg.**
Acquisition of specific hardware	0,0	0,0	0,0	2,0	0,0	3,0	**0,8**
Hosting services	0,0	0,0	1,0	2,0	0,0	6,0	**1,5**
Training	0,0	0,0	0,0	1,5	0,0	1,5	**0,5**
Marketing and support	0,6	0,7	1,0	2,6	0,8	3,0	**1,4**
Maintenance and operation	0,1	0,2	0,0	0,5	0,0	0,9	**0,3**
Other costs	0,0	0,0	2,0	0,0	0,0	0,0	**0,3**
Totals	**0,7**	**1,0**	**4,0**	**8,6**	**0,8**	**14,4**	**4,9**

Table 7 : Main categories of Additional one-time capital expenditures

A further breakdown on the costs illustrated in Table 5 and Table 6 is given in Appendix III

To supplement the qualitative evaluation of costs/benefits, and for comparison with the costs reported above SPs were asked to compare the costs incurred in adapting the eGovernment service to STORK 2.0 with the cost of developing an in-house solution to the registration of foreign users. It was seen that the STORK solution was considered economical, especially when re-use was possible in more than one SP service context. In part this is due to the

possibility of designing the software in re-usable modules, for example for communication with PEPS, for marshalling and unmarshalling of data between SAML and Java formats, etc.

The success criterion of 66% favourable replies was achieved as 70% of SPs agree that the cost of adapting another service to STORK 2.0 would be less than one-third the cost of developing a new solution.

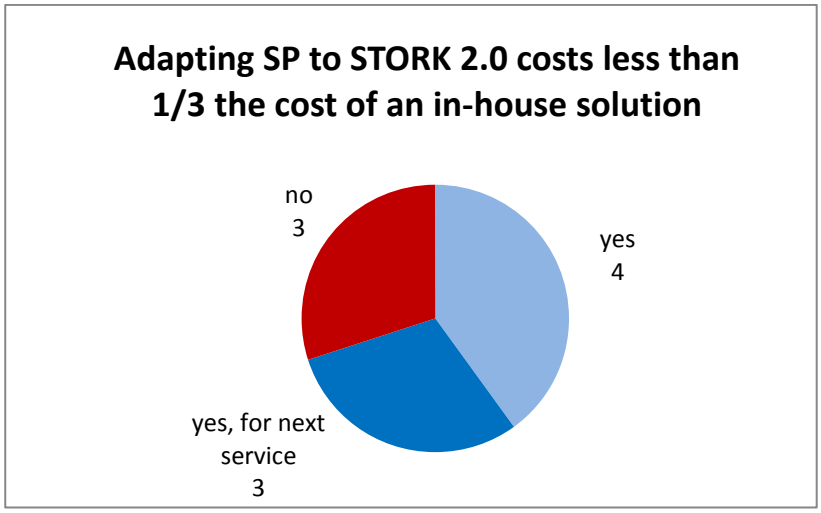

Figure 44: Cost of adapting SP to STORK 2.0 vs. cost of in-house solution (metric BV.17, SP Questionnaire Q43)

Metric SF.4 - Effort to integrate the SP with PEPS

To get a clearer picture of the minimum costs required of any new actor to connect to the STORK 2.0 network, SPs estimated the effort required to integrate their system with the PEPS excluding all effort for adaptation of internal business logic of the SP system. With 6 out of 10 pilot SPs reporting less than 2 months effort the success criterion (66% of SPs < 2 months) is substantially achieved.

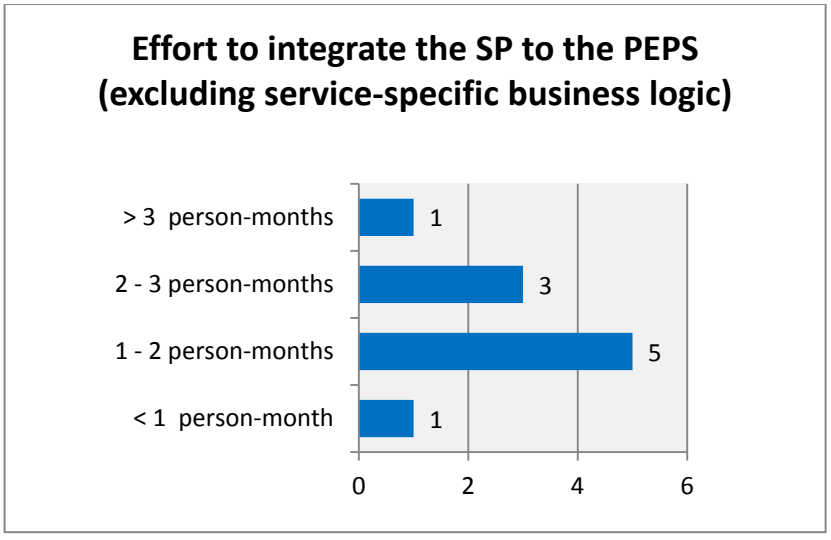

Figure 45: Costs of integrating SPs to MS infrastructure (metric SF.4, SP Questionnaire 42)

4.4.2 Operational costs

Metric BV.18 - Cost of support, training and documentation.

Piloting SPs were asked whether the cost of service support (including training and documentation) was in line with their usual SP practices; responses were basically positive or non-negative.

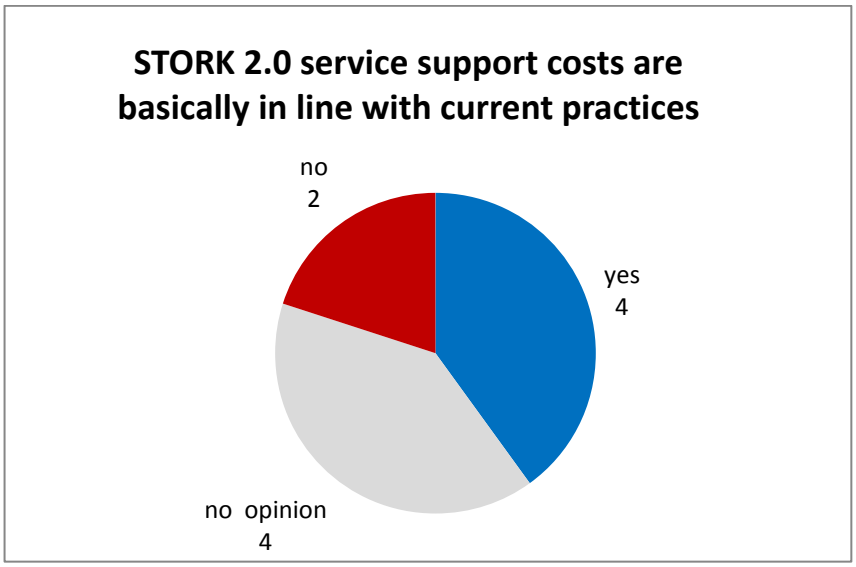

Figure 46: Support costs for STORK-enabled pilot service are in line with SP practices (metric BV.18, SP Questionnaire Q44)

Metric M.2 - Evaluate the cost of maintaining the involved services and systems

The table below presents an estimate of the recurring operational costs expressed in person-months as incurred during the execution of the pilot. Costs represent monthly averages, taken over all (responding) partners, of the maintenance and operation costs for the services (only the costs derived from keeping the services connected to STORK 2.0). Partners have estimated only those costs that a new STORK 2.0 adopter would face – that is, project costs and other development-related costs have been excluded.

The metric requirement of over 66% of positive feedback from piloting SPs was satisfied (see, also, Figure 27 (metric BV.09, SP Questionnaire Q21))

Maintenance category	***Cost during first month (p-m)***	***Sustained average cost for the remaining months (p-m)***	***Tendency of costs***
Specific developments during operation (Optional)	-	-	-
Patching common STORK software updates	0,23	0,15	Stable
System auditing and monitoring	0,07	0,08	Stable
System infrastructure operational expenditure (logs management,	0,25	0,08	Stable

backups, network related costs, etc.)			
Total:	**0,54**	**0,32**	**Stable**

Table 8 : Technical maintenance and operational costs for SPs (metric M2, SP Questionnaire Q20)

Metric M.3 – Evaluate the cost of replacing the system.

SPs evaluated whether the cost of maintaining STORK 2.0 is greater or less than the cost of developing a new system to provide the necessary cross-border authentication functionality. 8 out of 10 SPs said the cost was less; 2 had no opinion, and thus the metric is achieved. One of the SPs with "no opinion" thought that the costs and deployment times of some of STORK's ancillary services, such as digital signature features, weighed negatively in the evaluation.

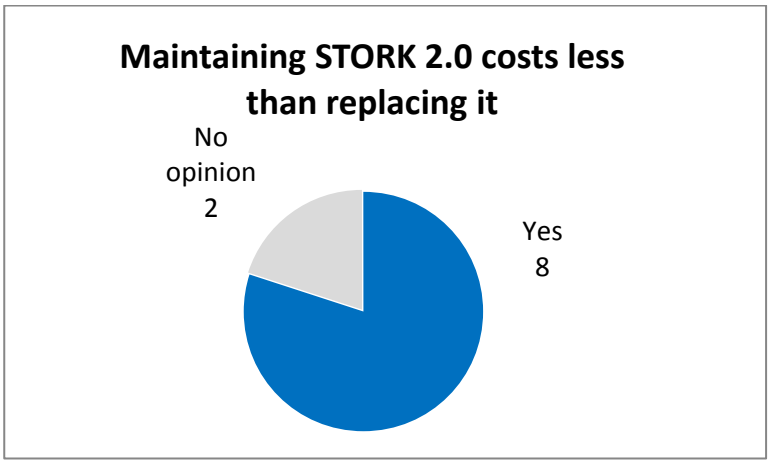

Figure 47: Costs of maintaining or replacing STORK 2.0 integration (metric M.3, SP Questionnaire Q41)

4.4.3 Cost savings

Metric BV.05 - Documentable cost reductions for SPs.

We recall from Figure 44, above, that 7 out of 10 SPs estimate that they would have spent over three times the cost of STORK adaptation had they developed a system for the authentication of foreign users in-house. Combining this with the capital costs for implementation indicated in Table 6 : Main categories of Capital cost and Table 7of section 4.4.1 yields an average, estimated initial costs savings of up to 40 person-months (on an estimated total effort of 60 p-m).

Looking beyond this to service provision SPs estimated whether and how much STORK 2.0 contributed to reducing the cost of the administrative processes. The success criterion of 66% of SPs reporting savings was substantially achieved.

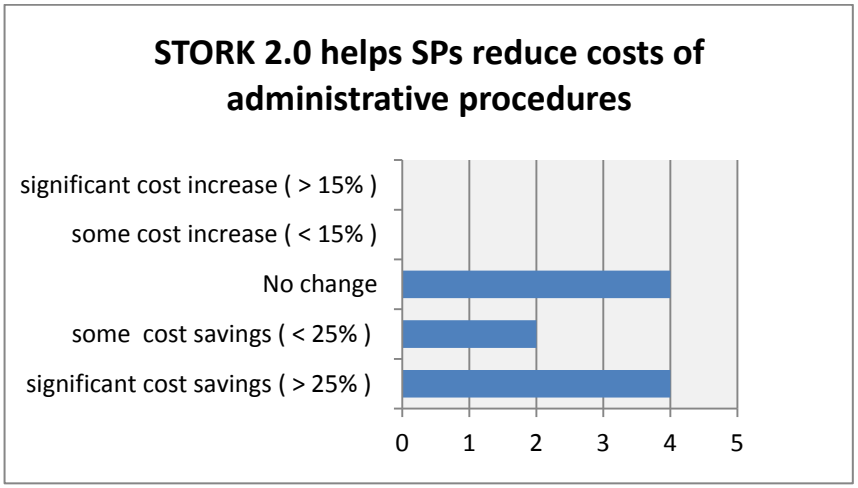

Figure 48: STORK 2.0 saves costs for majority of SPs; raises costs for none (metrics BV.05)

Metric BV.02 - Documented cost reductions for end users.

The end-user of a STORK 2.0-enabled eGovernment service should also enjoy cost savings resulting from re-use of his/her national eID mechanisms (for example, there's no need to acquire foreign credentials) and from the online access to cross-border procedures (less need for travel abroad).

Out of 83 responses to the question, "What is the greatest benefit derived from being able to access foreign eGovernment services using your own native identity credentials" there were 9 replies of "Cost savings" the success criterion of 10 positive replies was substantially Achieved. Moreover, considering the fact that 43 replies were in favor of "Time saving" it is more than certain that some of the Time savings also translates to Cost savings ([35])

4.5 Strategy followed to maximise pilot benefits

4.5.1 Benefits and resultant impact

The eGov4Business Pilot succeeded in producing a number of specific benefits for each of its different stakeholders. The main goal of all activities was to simplify access to eGovernment services so that foreign businesspersons could register and logon to pilot services with no more difficulty than domestic users. This was accomplished through the implementation and deployment of the STORK 2.0 interoperability infrastructure. The purpose of real-life piloting was to demonstrate that the cross-border authentication furnished did, in fact, produce all the specific, concrete end-user benefits that were expected:

- easier access to information and procedures across borders through quicker and easier logon process,
- reduced time for EU-wide business administration procedures,
- reduction of paper in cross-border administrative procedures,
- lower travel costs abroad and for national documentation (e.g., business credentials),
- more direct contact between businesspersons and foreign public administrations and at the same time more efficient use of local intermediaries and representatives,
- greater security in the access to eGovernment portals (with respect to portal-specific logon mechanisms) and access to a potentially larger number of services thanks to the greater security

At the same time, piloting served to refine the goals and priorities of the other stakeholders (SPs, MS actors, other Public Administrations) in order to maximize their own benefits and ensure the sustainability of the maturing services and organisation:

- improved security and efficiency of PSC portals and eGov for business portals,
- acceleration of public administrations compliance to eIDAS regulation, the Services Directive and other measures aiming to reinforce the European economy and promote the Digital Agenda,
- promote the integration of Business Identity Providers, B-IDPs - national Business Registers, Commerce and Mercantile Registers – as Attribute Providers of Legal Person identity information and mandate (powers of representation) information;
- gain the commitment of the B-IDPs as permanent members of the STORK 2.0 national infrastructures, in synergy with the EC Directive on Business Register Interconnection and the eIDAS implementation,
- promote greater harmonization and re-use of national eID schemes and European solutions (CEF)
- exploit the portals multiplier effects to achieve an increased user base of companies served by the portal and a wider usage of the underlying eID technology
- a better understanding of the costs vs. benefits of services
- clearer ideas about the organisational needs and governance mechanisms necessary to achieve sustainability for a national eID infrastructure with cross-border capabilities.

At various moments before and during piloting, evaluations were made by the EC Reviewers and by the internal Pilot Evaluation Team (Workpackage 6) which led to specific recommendations for how to best focus project energies on obtaining greatest benefits with the available time and resources.

Specific recommendations to the eGov4Business Pilot led to

- greater engagement of the B-IDPS,
- better measurement of benefits and achievements
- more focus on the engagement of portals in their national infrastructures and more effective actions for the engagement of users
- greater documentation of interoperability issues that will be further developed in future initiatives like e-SENS, ISA^2, CEF and national developments – issues such as language transliteration needs and solutions, evolutions of the mandate and powers of representation model and functions, refinements based on real-world applications, of the Attributes Quality Authentication Assurance scheme, liability mechanisms for operations and governance

In evaluating achievements, a fundamental step is showing how the STORK 2.0 solutions did enable real cross-border eID interoperability across many different eGovernment service platforms in different countries. Of particular importance is the innovative Authentication on behalf of a company procedure, AUB, involving the gathering of company eID information including powers of representation credentials in real-time from the appropriate national Authorities (B-IDPs) integrated into the STORK 2.0 network.

The next important objective was to leverage the visibility of the eGovernment services to extend STORK 2.0 network to new Service providers and eGovernment portals in other

Ministries and agencies. To achieve this second step it was necessary to confirm and consolidate the significant, positive added value of the STORK 2.0 approach in the opinions of both SPs and end-users. This confirmation does, indeed, come from the overall positive results of the business value metrics as well as the positive and constructively critical end-user feedback that was submitted. Additionally, one of the most telling results is the large number of SPs – ten - that are planning to keep their STORK 2.0-enabled services up and running after the project and that are interested in effectively realising a convergence between the eIDAS infrastructure and the STORK 2.0 solutions.

A further measure of the successful facilitation of the wider take-up of STORK 2.0 solutions was evidenced by the integration of Business Registers in 8 out of the10 piloting countries, even if most of the Business Register were not project partners. Implementation and testing, for the first time in Europe, of the "Authentication on Behalf of" (AUB) gave MS a unique opportunity to accelerate the development of cross-border capabilities for their national eID schemes anticipating and even exceeding eIDAS regulation specifications.

Finally, the success of the SP pilot service in the Netherlands attracted a new STORK 2.0 SP from Belgium, the Flemish Fisheries Authority. Analogously, successful piloting in EE, IT, LT and other MS convinced national authorities to connect additional services with the STORK authentication service.

4.5.2 Expectations gap management

The gap analysis aims at assessing the major gaps between the eGov4Business pilot objectives and goals and the achieved results as measured by the 54 metrics defined through the Benefits Logic Pilot evaluation approach. The main sources of input for the metrics were the SPs themselves and the pilot users, both real end-users and focus group participants.

All of the most important, basic project goals were achieved. Some (overly) ambitious goals were only partially achieve, for example, some of the variations on the AUB process flow required to simplify administrative procedures, representation of company powers and of suitable structures for mandate chains and joint powers. It is true, however, that these partially achieved goals represent the most advanced features, important but not critical in the short-term.

The major gaps revealed by the evaluations concern the following issues (we note that the related metrics are listed to help verify the degree of partial achievement, and that the goals of many of these metrics were, in fact, achieved):

1. Partial implementation, with respect to plans, of STORK 2.0 functionalities and eGov4Business service use cases (metrics F.1 and F.2)
2. Lower than expected usage of SP services during the piloting period (metrics SF.1, BV.11, BV.12, UU.3)
3. Only moderately positive end-user evaluations of STORK 2.0 usefulness, usability, security, control over personal data (metrics F.4, UU.1, DP1, DP.2)
4. The presence of several different types of obstacles to cross-border interoperability. (I.5)

Regarding the first point there are a few mitigating factors worth mentioning. The main one is that the essential operations of basic authentication and Authentication on behalf of a company (AUB) were implemented and sufficiently pilot tested to demonstrate their value and sustainability. The use case ("delegating powers" and PV Powers Validation) and single functionalities that were not piloted (3-MS scenario, SSO, fully chained mandates) represent more advanced features which did not prevent any partner from "going live". Moreover, in the case of PV, SSO and 3-MS scenario initial common STORK 2.0 software releases were

implemented and tested and feedback provided to WP4 “Common Specifications & Building Blocks” (see, for example, the Lessons Learned in Section 5.3.1), but final releases did not get distributed and deployed in the pilot MS STORK 2.0 common interoperability infrastructures in time for piloting. These functionalities represent advances in excess of eIDAS technical specifications and thus do not greatly compromise the net value of project results in the short to medium term.

On the other hand, the fact that the implementation of mandates and the AUB operation itself exceed the eIDAS specifications creates an expectations gap in the reverse sense – there is the danger that these functions will not be completely supported by some national eIDAS nodes thus limiting the convergence between project results and the future CEF eID building block and risking to lose some degrees of cross-border interoperability that were achieved by STORK 2.0 MS. This risk is being addressed by the STORK 2.0 partners involved in e-SENS and CEF and ISA[2] initiatives (see more details on this in section 6.3).

Regarding the usage gap, it must be said that in general usage of cross-border eGovernment services for businesses has been a source of disappointment for European projects, including LSPs, for many years. There certainly is a demand for a variety of services, but the effective obstacles go beyond the technological, organisational and legal. The business culture itself is still so heavily based on traditional procedures, real-world presence and face-to-face contact. The habits of using cross-border online services and the underlying eID infrastructures are not yet fully established. Add to this the fact that the majority of eGovernment services represent operations that are infrequent for the individual businessperson or company such as establishing a business or branch abroad, or performing annual or seasonal filing duties with a trade register, etc.. Thus, significant usage during one piloting season or significant growth in the user base was probably beyond any reasonable expectations. The success of the NL Farmers portal, with over 250 real end-users performing over 750 transactions, did prove that where the demand was present and mature, the STORK 2.0 infrastructure was able to satisfy it; in fact the repeat usage of the STORK-enabled authentication at the Farmers portal occurred even if the previous authentication mechanism (the “old logon”) was still operating.

A gap that causes more concern than low usage was the limited achievement – in the eyes of the end-user – in the general area of “end-user experience”. Although most of the success criteria associated with the metrics focusing on usefulness, usability, security, control over personal data were satisfied or substantially achieved, the general success was always partial and less than brilliant. This is partly due to the nature of eID management, dealing with security, privacy and other issues which must be both invisible and trust-inspiring at the same time. It can also not be denied that improvements in user interface are needed in order to reduce to an absolute minimum the impact on the end-user of technical security issues and legal data privacy constraints. But these are changes that can and will be made incrementally.

The most serious and disturbing gap concerns the extent to which barriers to interoperability persist (i.e. general data privacy issues, character set issues, legal value of e-mandates and powers taxonomy, required attribute sets not always available, status of back-office/offline PV procedure with respect to privacy data privacy) and spring up too frequently in eGovernment procedures. EU efforts to harmonise laws regulating European companies and business practices must still eliminate many national differences and incongruences. Legal issues, organisational and semantic issues – the business-world equivalent of “culture shock” experienced when moving from one country to another – create situations of incomprehension which are serious obstacles to company mobility and which represent interoperability gaps between MS and their eGovernment services.

These problems will benefit from the lessons learned in STORK 2.0 (see, for example, Section 5.3), lessons which are being transferred and carried over into other European and national initiatives, but the permanent solutions of these problems are not expected in the short term.

5 Pilot learning

5.1 Overview and major findings

The eGov4Business Pilot involved much more pioneering and adapting of the originally planned solutions than was anticipated at the start of the project, however this effort came with the positive benefit of a corresponding large amount of additional learning that took place during the implementation and running of the pilot services. One of the causes of the additional learning was the unexpected issues that were raised in cross-border interoperability on different interoperability dimensions: technical, semantic, organisational, legal and political. These issues, in turn, were largely generated by the unexpected complexities that arose in modelling and implementing the procedures and the data for the authentication processes involving a person representing another Legal Person, in the case of this pilot, usually a company. The data involves personal identifiers of the represented and representative persons – each furnished by a different Attribute Provider, the IDP and the B-IDP. Additionally, STORK 2.0 handled explicit information regarding the powers of representation of one person on behalf of the other. This was the mandate token or attribute, usually furnished by the B-IDP, but in some cases furnished by a specific authority. Moreover, STORK 2.0 modelling also included the complete procedures for the retrieval of this data from all the providers, even in the case when they were not all located in the same MS.

A further source of significant difficulties in interoperability was the basic design hypothesis that all procedures and data transfers would be accomplished in a single user session, real-time and online with key authentication data being machine processable so that the authentication processes and decisions could be completed automatically according to the individual “access logic” built into the SP system.

Thus, solutions for the eGov4Business Pilot were “designed for the future”, however implementations had to deal with a large number of limitations known and unknown, foreseen and unforeseen due to the reality of the available information, the needs of the SP services and the portals in which they are published, and the needs of the different organisations and Public Authorities involved in the phases of access, authentication and fulfilment of the eGovernment services, not to mention the European, national and local laws and practices which also condition a service.

This pilot has generated significant knowledge in the following areas:

- Modelling of mandates of one person to represent another; of the different types of powers of representation that may be usefully described ,and of the different ways that these powers are represented and used in eGovernment services. The different types of powers and the company liabilities associated with them are coded in national law and would require a detailed ontology to model and implement at the European level (see [9]). A rather simple model was implemented in STORK 2.0 and the eGov4Business pilot deployed an even more simplified version of that (since anything more complicated would have created the need for government-authorised mapping of taxonomies or ontologies). Also, chains of mandates and joint mandates represent structural variations with additional semantic and technical complexity.
- Integrating eGovernment portals into the STORK 2.0 eID infrastructure considering the high level of security and data privacy guarantees established by the project. In particular, the systems of Quality Authentication Assurance and Attribute Quality Authentication

Assurance (QAA and AQAA) with their implementation guidelines are an important project resource that has been validated with B-IDPs and SPs.

- The broad testing in 13 different MS with 13 different SP services and environments afforded a unique opportunity for pushing the boundaries of interoperability of cross-border public services. The unprecedented degree of cross-border interoperability between administrative registers that was achieved in the eGov4Business piloting raised new issues in cross-border interoperability: there are many ways that official data in one country might not be immediately useful or even comprehensible, much less machine-processable in other countries. Semantic problems dealing with company attributes, local legal issues, language and character set issues were all encountered and addressed during piloting. Figure 49, below, shows the number of piloting SPs which encountered interoperability issues of the various types.
- And finally, the pilot is contributing strongly to STORK 2.0 sustainability by strengthening national infrastructures – in particular with regards to the integration of B-IDPs – and by continuing future work on STORK 2.0 results at the national level and internationally with CEF, ISA2, e-SENS, ECRF and BRIS (see [20]-[33]).

Metric I.5 - Absence of Legal and semantic obstacles.

Piloting Service Providers encountered a wide range of unexpected obstacles to their smooth interoperability. Problems with data models, metadata, legal constraints and organisational roadblocks were encountered in almost as many variations as MS were represented. While technical and semantic complexity were important areas where challenges were encountered, organizational and governance aspects were at the same level and legal, liability and policy obstacles were ranked as being of even higher importance, in line with expectations, i.e. solutions for technical and semantic issues are in the end easier to find than for legal and policy aspects.

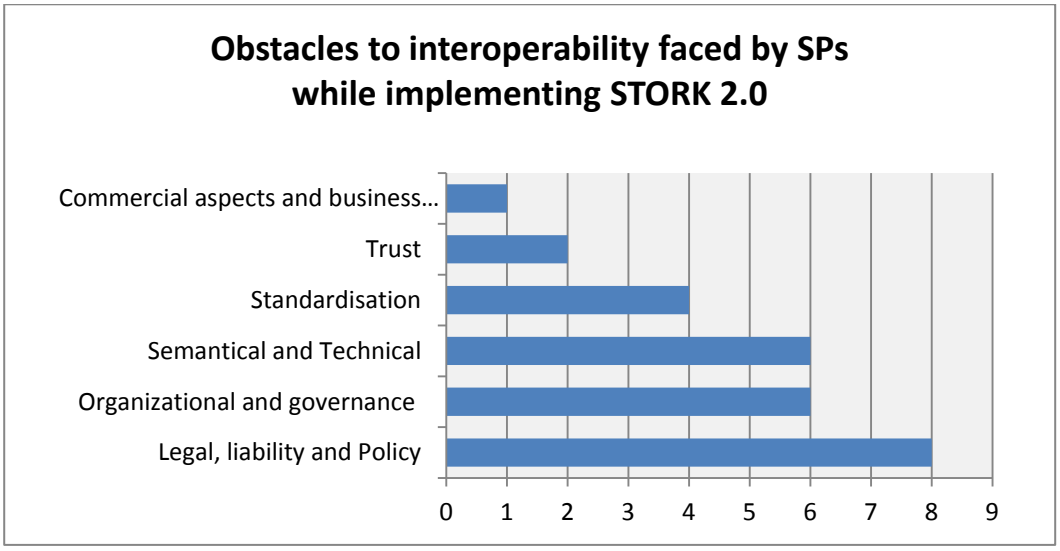

Figure 49 : The different kinds of obstacles faced by SPs while implementing STORK 2.0 (metric I.5)

This chapter is dedicated to the presentation of the most significant lessons learned. Table 20 in APPENDIX II Lessons learned table lists all the lessons reported here according to pre-established numbering scheme.

The following figure reports the distribution of these lessons in categories.

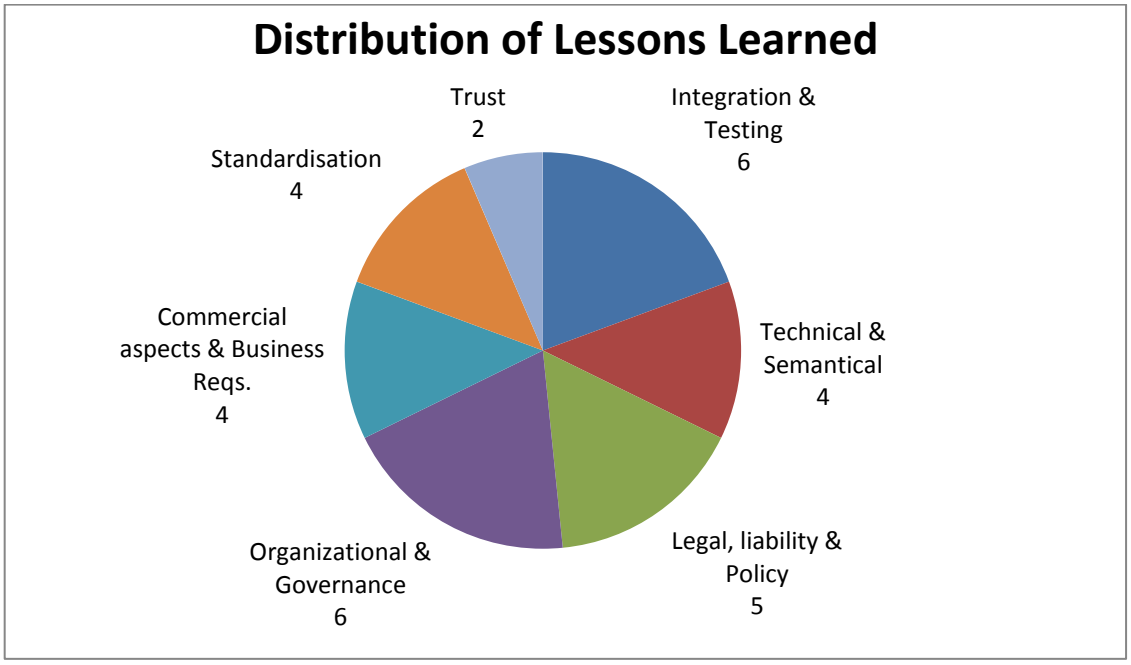

Figure 50 : Distribution of Pilot Lessons learned in macro areas

5.2 Approach to knowledge-building

Never was the adage "the devil is in the details" more true than for European interoperability.

Many projects, initiatives and even recommendations and directives have seen their efforts get snagged in the details of local laws, procedures, customs and even online services implemented by national and local competent authorities.

The objective of the approach to knowledge-building in STORK 2.0 is to facilitate future implementation and adoption of project results, and more generally to consolidate and spread a "culture of interoperability" in the area of cross-border eID management and authentication services which underlie all levels of public services.

In STORK 2.0 in general, and in the implementation and deployment of the eGov4Business pilot in particular, several techniques in knowledge building were used to gather, document and exchange relevant information about eID management and other project issues: face-to-face workshops, phone meetings, wiki pages, questionnaires, service demos, the software repository and bug-reporting. In particular, a rich knowledge base of documents, notes, discussions, was gathered in the wiki besides the "standard technical documentation" consisting of requirements specifications and analysis, technical specifications and design, implementation artefacts, testing plans and results and other documents. A Mandate Special Interest Group was informally created to study and present certain issues relating to powers representation and mandate structures. But much of the learning took place while "doing", in particular together with other partners in efforts such as: integrating SAML tokens with SP authentication mechanisms, harmonizing QAA and AQAA levels with SP security and data integrity needs, harmonizing "powers information" across a network of trusted data providers and data handlers and collaborating in cross-border interoperability testing.

Learning was consolidated in a collaborative way in the Pilot, with other pilots and with other workpackages. Cross-workpackage discussions – online and in conference calls, joint studies

and face-to-face workshops were particularly fertile occasions for sharing and advancing learning. Contributions were solicited from different stakeholders: service owners, developers, end-users and members of industry possibly interested in using or exploiting project results. .

It also goes without saying that end-user feedback was a major source of knowledge and critical advice which translated into more lessons learned. Feedback was given directly in focus group testing and training sessions as well as through the web-based feedback forms hosted at the Piloting micro-site. This feedback form was revised during the running phase to better capture important information and to be easier to fill out.

Lessons learned are presented in the next subsections according to the common logical framework established for all STORK 2.0 pilots, which broadly classifies these lessons as "Implementation lessons learned" and "Lessons learned for eID as a service", each with different common subcategories which allow to clearly organize the pilot's consolidated knowledge that can be used widely in the form of "an attractive, recognizable format that appeals to the eID and Digital Single market community", according to WP6 mid-term recommendations. Learning categories, address common aspects like for whom the lesson is being learned, source of the lesson, usefulness for adoption, impact on sustainability, etc. Lessons are clearly numbered to facilitate easy reference to them and contain proposed solutions, when applicable.

STORK 2.0 is now contributing to different European and national initiatives, CEF, ISA^2, e-SENS LSP and national eIDAS implementations. The presence of several current partners in all of these initiatives guarantees continuity of the STORK legacy.

5.3 Implementation lessons learned

The following paragraphs contain the main Lessons Learned from the eGov4Business piloting – those nuggets of experience which represent solutions to particular problems encountered or simply advice concerning pitfalls or some other particular aspect of implementation and deployment of a federated, cross-border eID interoperability platform. The lessons respond, in part, to the past recommendations of the Internal Pilot evaluation team (WP6) to consolidate issues and give concrete visibility and communication to the topics discussed at meetings, phone conferences, in emails or using the project wiki.

Some topics are of general interest, others more specific to eGov4Business services; topics span all aspects of implementation and service interoperability, from software development to eGovernment organisational and legal issues, to commercial sustainability matters.

5.3.1 Integration and testing lessons learned

This section describes the lessons learned related to the technical adaptation of existing eGovernment services to accept and handle cross-border eIdentity information about people and companies and the powers of representation that a person or company may have with respect to another person or company.

The following items characterize for whom and from whom the lessons are learned, the impact on adopters and other groups, the impact on sustainability and how they have been obtained:

- These lessons will be useful to technical teams of future adopters of STORK 2.0 who act as SP and B-IDP; they will also be useful for initiatives reusing or extending STORK techniques such as e-SENS or the developers of the eIDAS-Node/ CEF eID building block.

- The lessons have been gleaned from the experience of SPs and their third-party developers as well as the partners of the technical and legal workpackages of the STORK 2.0 project
- The information will help new adopters to save time and effort when faced with similar obstacles
- Similarly, members of the STORK 2.0 technical team would benefit from reviewing the lessons for future developments of STORK or similar federated eID interoperability services
- The lessons deal with the smooth running of the STORK infrastructure and are therefore quite relevant to sustainability
- This information has been derived from the frequent interactions between the technical teams of all eGov4Business SP partners, the pilot leader, other STORK 2.0 pilots and the Pilot coordinators as well as the technical workpackage.

Lesson 1.1 Integration and handling of AQAA by SPs and APs (B-IDPs)

The handling of AQAA by some SPs raised the concerns in the terms of readiness and preparation level of SPs to deal with AQAA on the attribute level. The SPs particularly had issues to understand the role and meaning of AQAA, its difference compared to QAA, as well as how it should be handled in particular cases and implications of this handling.

Although a set of practical AQAA guidelines (a specific "AQAA cookbook" or "dummy's Guide") for SPs was provided as part of the Addendum to D3.2 QAA Status Report, the limited practical experience demonstrated the necessity to invest more effort in facilitating Service Providers to understand and apply AQAA (see Section 4.2 of [9]).

Attribute Providers also had difficulty determining how to implement the AQAA scheme. In the case of the eGov4Business Pilot, the principal attribute providers were Business Registers or mandate authorities. Even though these are official Registers the quality of the information in the register is not perfectly homogeneous as implicitly assumed by the AQAA model. Data quality may vary according to the age of the information as this reflects the data handling techniques and practices with which the information was gathered and maintained. Moreover, legislative changes can also affect the legal value of the information and therefore the way it is gathered and handled. Given this situation, it is not always a simple process for a Business Register to establish AQAA values.

Clearly in the central AUB service for authenticating a person on behalf of a company, the AQAA-labelled Legal Person identity attributes and mandate attributes supplied by one government agency – the Business register or B-IDP – to another eGovernment service portal represents an official communication of information with a precise legal value. However, in the absence of Service Level Agreements and a more explicit charter for the STORK 2.0 network or "circle of trust" this legal value is difficult to determine and the determination of liability, in case of fraud or of Legal person Identity theft is not clearly established. See Section 5.3.5 for additional considerations.

Lesson 1.2 Propagation of changes in configurations

During the operation, periodic short-time interruptions of the services were observed. One of the causes of interruptions can be traced back to the change of configurations in the connected nodes, and most notably the updates or expiry of SAML signing certificates across the PEPSes, SPs and V-IDPs.

Although the STORK 2.0 design includes the means to coordinate configurations, using the *Version Control* subsystem, in practice this system was not deployed and supported effectively by PEPS organisations and SPs and for sufficient time to evaluate its benefits in preventing above mentioned problems.

In order to improve this situation it would be necessary to first understand in more depth the reasons behind the slow uptake by partners of version control functionality, whether because of time or budget constraints or other reasons.

Lesson 1.3 Aligning and improving software development, release and configuration practices; exchange of digital certificates

Ensuring availability and reliability of the infrastructure and supporting processes is of crucial concern for project adoption. In the terms of future developments, the processes that include the maintenance, updates and support of common infrastructure should be further harmonized to support the industry practices and expectations of industry partners when collaborating and integrating with MS infrastructure.

Although the actual approach suited the needs and expectations on the level of LSP projects considering the overall project goals and objectives as well as its execution environment, the expectations of some industry partners (SP) on the metrics related to availability, maintenance and support (see Section 3.4, Paragraph 4.2.2 and Paragraph 5.3.1, respectively) were only partially aligned with what is performed in practice.

More particularly, in the scope of workshop discussions some partners provided feedback useful to improve the overall availability of the infrastructure, the differentiation between production and preproduction environments and the support workflow and responsiveness. These communications revealed a misalignment between perception and expectation of industrial partners (e.g. SPs), on the one side, and the practical realization done the side of MS infrastructure. In this sense, the future work should particularly focus on filling the gap by further advancing the metrics and tools that would facilitate the understanding and provide clearer communication and integration means to partners.

On the other hand, the infrastructure providers should strive to facilitate further adoption of industry practices in software development and maintenance with the purpose of increasing stability, transparency and overall quality of the processes. A very specific instance of this regarded the exchange of server digital certificates between trusted nodes of the network. The certificate exchanges, while the Version Control functionality was not yet in place, were often communicated among partners through the STORK 2.0 mailing lists. This kind of communication is not really the best solution for real world production quality that requires high availability of the services.

Lesson 1.4 Support and documentation channels for SPs

The updates (including some changes) to documentation, the code fixes and updates and the subsequent frequent updates of the STORK 2.0 systems imposed an additional overhead on SPs during the implementation phase of the pilot. Although the core STORK 2.0 technical interoperability development group (WP4 Core) had its bug and tracking systems, as well as wiki and development repository, these have been primarily meant for the development of the common code and inter-MS collaboration. SPs also required access to the common STORK 2.0 code for re-use of modules such as the SAML Handler, for example, but in practice development and bug reporting environments were used more by common code developers. Considering that email communication is less structured, transparent and effective, the resolution of particular issues often took more time and resources as necessary. Stronger participation from SPs, using the available tools and methodologies for common code

developers and MS operators would therefore provide more effective and efficient integration and enable an additional feedback loop.

Metric M.1 - Evaluation of code maintainability and quality of technical documentation.

SPs were asked to assess the maintainability of STORK 2.0 common code and the quality of technical documentation. The metric is achieved as 80% of answers were positive (66% required).

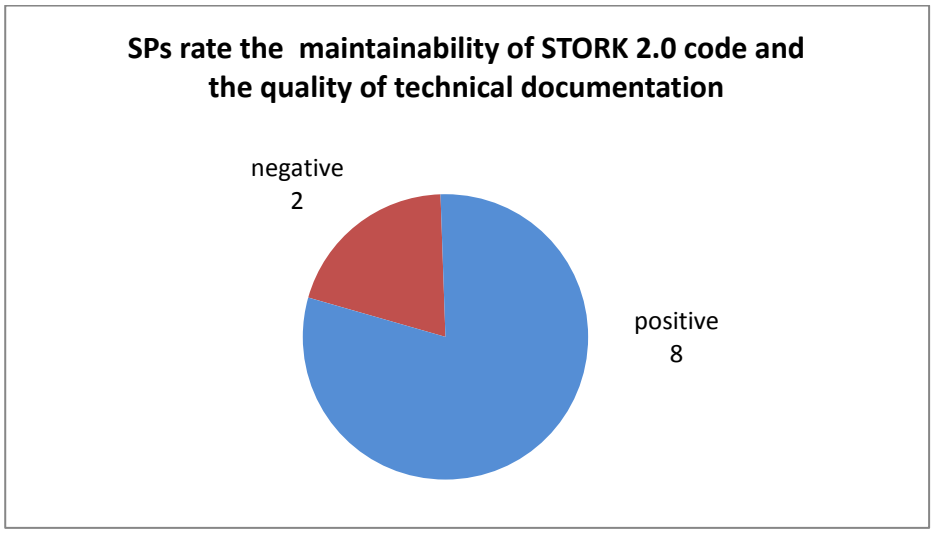

Figure 51: SPs rating of the maintainability of STORK 2.0 common code and the quality of technical documentation (metric M.1, SP Questionnaire Q40)

Metric RM.5 - Implementation level of support, incident and SLA related procedures

SPs were also asked to rate the support received from their MS infrastructure and the common building blocks development support team. The overall rating was quite positive. (60% percent of positive answers, as threshold was 66% the metric is substantially achieved).

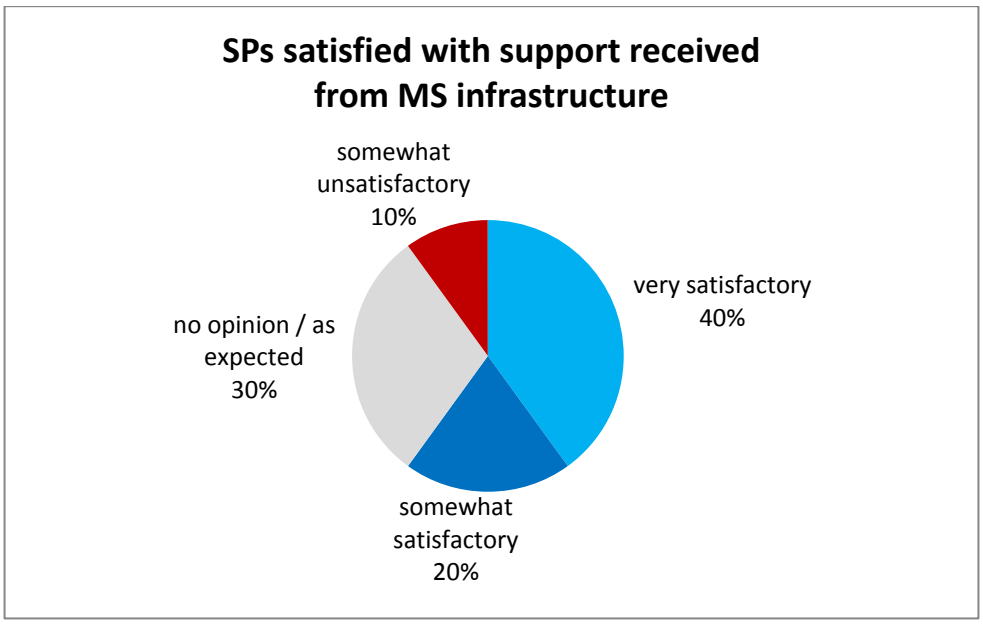

Figure 52 : The different kinds of obstacles faced by SPs while implementing STORK 2.0 (metric RM.5, SP Questionnaire Q33)

Lesson 1.5 Monitoring infrastructure

The view of STORK 2.0 infrastructure (both pre- and production ones) shows many interconnected nodes from various regions, characterized by diverse range of properties. It would be good if these properties included information on geographic location and networking capabilities, various firewall and security configurations, different versions of common software and dependence on MS and infrastructure specific processes.

At the start of the project monitoring system was implemented with the purpose to provide an overview on common infrastructure involved in the project. The practice exhibited during the development and integration flows demonstrated the need to go one step further in monitoring and testing of common connectivity. The examples of possible events with potential negative effects include frequent updates of the software, the existence at times of various partially incompatible versions of the nodes, firewall and system updates, as well as periodic certificate expiries and renewals that had to be propagated network wide. This complexity would benefit greatly from advantages provided by Version Control functionality.

The future work therefore should address the particular aspects of connectivity and interoperability monitoring that goes one step further. In order to support this action, the activities such as performing periodic test logins and attribute transfers across the infrastructure, confirming the trust relations between nodes or interoperability testing of different software versions on the protocol level could be automated, delivered as functionality and defined as common process. More attention to the AUB process and verification by each MS of the correct functioning of "MS-specific details" should also be given.

Lesson 1.6 Management of test credentials

Getting valid test credentials, in particular with the many combinations of business credentials and mandates that are present in the real world, is a more complex activity than anticipated which requires careful preparation, organisation, monitoring and a careful and intense collaboration from all MS.

This section refers to some sporadic issues with test credentials of some MS. The availability of test credentials was usually adequate, but at times problems arose: some MS delivered credentials late or in incomplete form; some test credentials were missing comprehensive support documentation or the passwords needed to open encrypted files for access and use of the credentials. Additionally, some test credentials expired during the project, causing additional blocking in preproduction and imposing an additional overhead for the support process of obtaining a new ones.

Finally, the usage of test credentials was not straightforward in some cases. Some of them required the installation of additional software, which was not always present in English. In other cases the authentication systems of MS did not provide operating or error feedback in English, requiring more effort to be invested in the testing phase than would be ordinarily expected.

5.3.2 Technical and semantic lessons learned

This section describes the lessons learned which relate to the data modelling of the identity information and credentials which are exchanged between the SP and the STORK 2.0 network. In particular technical and semantic interoperability issues typical of the Business Register world are considered in their relation to the STORK 2.0 processes.

The following items characterize for whom and from whom the lessons are learned, the impact on adopters and other groups, the impact on sustainability and how they have been obtained:

- These lessons will be useful to technical teams of future adopters of STORK 2.0 who act as SP and B-IDP; they will also be useful for initiatives reusing or extending STORK techniques such as e-SENS or the developers of the eIDAS-Node/ CEF eID building block.
- The lessons have been gleaned from the experience of SPs and their third-party developers as well as the partners of the technical and legal workpackages of the STORK 2.0 project
- The information will help call to the attention of new adopters some issues which might not have been immediately present and also to allow them to save time and effort when faced with similar obstacles
- Similarly, members of the STORK2.0 technical team would benefit from reviewing the lessons for future developments of STORK or similar federated eID interoperability services
- The lessons deal with some semantic interoperability features of the STORK infrastructure and are therefore relevant to sustainability
- This information has been derived from the frequent interactions between the technical teams of all eGov4Business SP partners, the pilot leader, other STORK 2.0 pilots and the Pilot coordinators as well as the technical and legal workpackages.

Lesson 2.1 Reusing existing definitions, views and vocabularies in mandates

The approach followed, based on delivering information on legal entities and natural persons for the purpose of AUB, defined several attributes that would facilitate this process. However, instead of outlining new concepts, one of possible directions would be to consider reusing existing definitions or schemas. These definitions can include ones proposed and supported on the EU level, such as Core Vocabularies [36] that currently approach the concepts of *person*, *organization*, *location* or *public services*. The other possibility would be to leverage existing industry and standardization approaches such as collaborative project W3C Schema Community Group [37] that define the framework for entities such as *person*, *place*, *organization*, *action* and their further subordinates.

The reliance on widely supported and adopted approaches enhances the interoperability the solution and lowers the overhead caused by the process of inventing and production testing of schemas. Additionally, there is possibility to adapt existing schemas to conform to the requirements recognized from the project flow. The state of the art of standard vocabularies was checked against STORK 2.0 needs at the start of the project, and was seen to be insufficient, but the situation must be continuously monitored and STORK 2.0 must actively promote the evolution of recognised standards to cover its own needs. A case in point is the need to further develop the work on mandates and powers, and in fact, STORK 2.0 partners have proposed that ISA^2 embrace this need.

Lesson 2.2 Addressing semantic and legal gaps between descriptions

There are some of the identified attributes that provide the descriptions belonging to the same category, but which are handled across MS in different ways. One example of this is *translatableType* attribute that describes the company type in cross-border context. Although there are some internationally recognized company types, such as *limited liability* (EN: Ltd, SI: d.o.o., AT: GmbH), its legal description and regulation is not defined on the same way in each

country. For example, belonging to the common type of limited liability, *d.o.o.* in Slovenia might not exhibit the same properties such as *GmbH* in Austria when handled in cross-border context. One such property might be minimal allowed capital of the company, which varies across the countries and might be relevant for some business processes.

This raises the requirement of SPs and all collaborating, integrated agencies and intermediaries of AUB process (for example, such as Company and Supplementary Register in Austria, which performs on-line registration of foreign legal entity and mandate relation) to understand subtle underlying differences between the types belonging to the same class that are relevant for the entity's operational, legal or functional requirements. The reality is, however, that SPs in one country might be particularly adjusted to the semantic category and requirements that are common and regulated by law in their own country, but the inclusion of foreign company information under the same category might introduce unforeseen discrepancies.

Further collaboration is needed between the ISA[2] and the community of Business Registers.

Lesson 2.3 Mapping missing or incomplete descriptions

One of the findings gathered in running the pilot is the gap in provided and required descriptions of entities delivered by one MS and consumed in other MS. We have noticed that business registries in different countries might not provide all information necessary to fulfil legal and operational requirements of the infrastructure or SP in other country.

For instance, the separate cases arose where attributes *canonicalRegisteredAddress* and *placeOfBirth* were not be delivered in complete form by the businessperson's country of origin, but were nevertheless required by an SP (or an integrated, collaborating agency) of another MS in order to fulfil the AUB process. Similarly, the business registry of one country might not provide an attribute such as *translatableType* (or company *type* in source form) at all – although it may be required by the SP and other authorities in the target MS to complete the AUB process.

One of the possible workarounds is to derive the attribute from existing information on the source PEPS. In the case of company *type* and *translatableType*, this information can be derived from the name of the company, considering that there is a legally prescribed procedure which requires that complete company name entry in business registry includes its type in one of the allowed forms. The question in this case is however whether this information can be translated and provided on-the-fly, by Business Register or PEPS, and whether the resulting assertion holds in practice, i.e. conforms to legal requirements, responsibilities and expectations from receiving party (either MS infrastructure or SP).

Lesson 2.4 AQAA syntax

The AQAA has been introduced as an extension of the STORK1 QAA model, allowing the quality levels to be assigned to attribute assertions, comparable in intent and set-up to the original QAA. Currently, AQAA, like QAA, is delivered as an attribute, although it does not describe the entity of the transaction but the quality and level of the attributes contained in an assertion (and of issuing APs).

In the case of the complex attributes, according to the current specification, AQAA is delivered on the first level, describing the whole complex attribute that contains different values. Implicitly, this approach means that this top-level AQAA describes the all sub-attributes of the complex attribute.

Considering simple attributes (like *name* or *age*), AQAA is not provided but derived implicitly from the assertion QAA.

One of the approaches that could be considered to address these points would be to analyse whether the repositioning of AQAA as an extension of an attribute (like the current extension "*availability*") would be beneficial for the stakeholders.

5.3.3 Legal and liability lessons learned

Cross-border interoperability projects often face legal issues, making it essential to map all possible obstacles before and during implementation of technical solutions. It does not matter how good or necessary the new idea is, if existing legislation does not support it, implementation may become impossible. Section 2.2 of [5] identified key legal obstacles and challenges which were further studied in [8] which also took into account the just published eIDAS Regulation [15].

As seen in Figure 49 : The different kinds of obstacles faced by SPs while implementing STORK 2.0 (metric I.5), Legal, liability and policy issues were the most frequently encountered type of obstacle faced by SPs while implementing STORK 2.0 infrastructure. Based on information given by SPs, legal issues arose both on EU and national levels. Some of these issues corresponded to those listed in the previously mentioned reports, but the eGov4Business Pilot SP´s also addressed much more specific and detailed problems. The aim of this chapter is to describe these legal issues to inform and give guidance to future SP´s and member states in similar situations. The information is quite relevant for the sustainability of an organisation like STORK 2.0.

Lesson 3.1 Issues related to QAA and AQAA; multiple identifiers and identity reconciliation

To successfully implement the AUB procedure it is essential to establish the link between the represented person and the representative. A most effective way is to create this link as a "statutory mandate" part of the registration of the represented legal person; e.g., to enter the unique national identification number and other identity information of the "authorised representative" into the business register, or B-IDP. This enables the validation of the existence of the link during the authentication process, as required by AUB. Unfortunately, some national data protection regulations prohibit the free use of a person's unique identifier. In other cases, persons have different identifiers for communicating with different government agencies; in other countries, only hashed identifiers can be in used; and so on. If the unique identifier used for STORK 2.0 personal authentication at the IDP and at the SP portal differs from that entered into business register, the natural person cannot be automatically linked to the legal person.

If linking is based on some other attribute like name, date of birth or address, it may not be 100% reliable. But in practice, it was seen that in most cases an alternative identifier – more secure than just name, birth date or address - was present in both the Business Register and the IDP so that certain identification was able to be made by the B-IDP.

In other cases, an operation like "identity reconciliation" was implemented as a specific operation at the SP.

This operation has potential implications on the AQAA of attributes provided by the AP.

Moreover, providers of personal information or otherwise reserved information and attributes may themselves pose requirements on the Assurance levels of the user identities and the technical sessions to which they release their information. For example, personal health records requiring high QAA to access must not be released in a session initiated by a low-QAA authentication. Such restrictions must be built into and permitted by the overall workflows of the authentication procedures.

The overall Lessons learned (as reported in [9]) are:

- Only if same unique identifier has been used in commercial register and during authentication, can the link between represented and representative can be trusted. Otherwise, some actor or actors must implement an “identity reconciliation” procedure to safely unite eIDs across administrative sectors.
- For validating QAA of issued attributes, the AQAA Cookbook was introduced to provide practical guidance to attribute providers and service providers. It was seen that the variety of national legal and organisational situations required successive adaptations of the original, simplified model. The iterative process of refining the QAA and AQAA models is still going on, at the close of the project. Work will be carried into future evolutions of the eIDAS implementation in future studies and projects.

Lesson 3.2 Translation of mandates, use of standard values and legal value of STORK 2.0 SAML tokens

During piloting, member states faced three kind of issues related to translation.

Firstly, commercial and administrative registers, including business registers, usually provide information only in the national language. Although STORK 2.0 did adopt certain partial solutions for some information common across borders such as legal form and powers of representation, much legally significant information, for example, about restrictions and limitations of representative powers, is usually entered manually as free text. This makes it impossible to completely validate mandates automatically in a large percentage of cases.

Secondly, when using “standard values” which have even been agreed upon by the project so that the information is machine-processable, but which are not authorised by any national law, the problem exists of who is responsible for mapping these values from and to national schemes and what is their liability in case of damage-producing error. The main example of this concerned the representation rights codified in the STORK 2.0 Powers Taxonomy and transmitted in the “mandate attribute”. Each MS, according to the actors involved and the specific configuration of the national STORK 2.0 infrastructure, established its own procedure for implementing the mapping and sought its own legitimation, but doubts remain concerning the legal validity in cross-border transactions of such transformed information.

Thirdly, we can ask the very general question, "Under what conditions could the legal value and acceptance by any relying parties of data in XML code (or some other suitable machine-readable format) be universally ensured?" Is it necessary for Attribute Providers of “authoritative data” to declare the legal validity of electronic data expressis verbis? Is it sufficient that the authentic origins of the data (i.e. the fact that they were at some point in time originally issued by an authoritative source) can be determined by relying parties when necessary? Or could it be envisaged that a third party acts as an authenticating service, confirming the authenticity and reliability of the data towards all relevant relying parties even without identifying the originating authentic source? STORK 2.0 has shown the viability of these options: attributes can be issued with quantifiable trust by attribute providers (using the AQAA which allows authentic sources to be identified), or alternatively trust can be derived solely from the fact that data originates from a PEPS/V-IDPS without considering AQAA levels. Other issues such as the liability of PEPS/V-IDPs (or Member States) are however not conclusively resolved yet, as this requires policy decisions and/or legislative interventions which transcend the scope and competences of STORK 2.0.

Some lessons learned:

- Agreed high-level ontology and common mandates were suitable for piloting in order to help service providers in mandate validation process, but there is a great long-term need for a more universal European-wide standardisation of certain information such as powers of representation, company legal forms, company activity status and the different forms of insolvency or limited activity common solution. Some of these issues are being addressed, but only very partially, by EU initiatives such as BRIS [18] or eJustice [32]. See also [9].
- When implementing new administrative processes, one must deal with the likely possibility that in some cases not all information will be machine-readable. Human verification or confirmation, such as the translation of mandate restrictions and other free text fields written in foreign languages may be a necessary step in the procedure. STORK 2.0 processes were "designed for the future", but the present reality posed restrictions and barriers to interoperability that system implementation was forced to deal with.
- The previous consideration unfortunately holds for a much wider class of problems besides language and data standardisation. It underlies the slow and uneven progress towards implementing the EC Services Directive [17], Business Register Interconnection [18] and other specific areas of EU policy and direct EC intervention.

Lesson 3.3 Issues related to transliteration - Non-Latin characters

As noted above, according to Member States' regulations, in most of the cases for communication and registration national languages are used. Since no one usually translates or transliterates names and addresses, for example, the following legal issue related to acceptance of non-Latin characters was raised:

- Who is entitled and responsible for transliteration of names? Can an infrastructure body such as the STORK 2.0 PEPS perform it, and if so, which PEPS, that is the PEPS in which MS?
- How to ensure sustainability of provided services, e.g. if registration is done using both Greek and Latin characters, how can the information be searched and modified afterwards? How can the end-user know what kind of alphabet to use?
- Even if some information is automatically translatable, there persist many situations when free text is used.

The eIDAS expert group was informed of this issue, and a partial response has been written into the Implementing Acts [16] which contain the following clause:

> Data shall be transmitted based on original characters and, where appropriate, also transliterated into Latin characters.

We note, however, that the interpretation of just which situations are appropriate and the identification of the body that should perform the transliteration are left unspecified.

Lessons learned:

- It is usually possible to solve those issues from technical side, but from the legal point of view, there is no commonly accepted solution at the present time.
- During the project, Greece implemented a solution which enabled the Greek MS infrastructure (PEPS & APs) to provide original Greek and transliterated Latin values of the representative´s identifier, given name, surname, legal name and address.

Lesson 3.4 Confirmed minimum sets of attributes

As seen in the discussion of Lesson 2.3, during the pilot testing phase, it became clear that major differences in legal requirements relating to mandatory attributes for SPs and B-IDPs would have greater than anticipated impact on the achievable interoperability of services. Even end-users, through the feedback forms published at SPs and at the STORK 2.0 "micro-site", raised the same issue since in some cases they were not able to access an e-service because information required by the SP was not made available through the user's own MS STORK 2.0 infrastructure. For example, in case of simple authentication, Dutch C-PEPS was only able to provide information about the identifier, but some SPs required additional information about name, surname, address, QAA etc.

In other cases, information generally evaluated (in prior work both by the eGov4Business pilot partners and by STORK 2.0 partners concerned with establishing the infrastructure requirements and capabilities) was seen to be required under certain circumstances – for example, person's place of birth, VAT number or other identifiers of companies and company officials, and others.

Lessons learned:

- In case identity or attribute provider couldn´t provide attributes requested by service provider, piloting continued between those partners whose set of attributes matched. It became clear that agreeing on a commonly approved list of mandatory attributes is necessary, but that back-up measures are required to maintain flexibility and service levels.
- One of implementation acts of eIDAS [16] sets out requirements concerning the minimum set of attributes for both natural and legal person, but explicit information about the link between legal and natural person together with mandate content is not present (as was discussed in Paragraph 4.3.4).
- Enriching the minimum sets of attributes is necessary, but with certain rules to gain flexibility and avoid unpleasant restrictions on cross-border interoperability.

Lesson 3.5 Powers validation functionality and prior user consent

One of the basic principle in STORK 2.0 project is the direct engagement of end-user in the processes involved in Identity Management. This principle preserves data protection and means that the end-user controls and consents to all cross-border attribute transactions and without his/her specific, prior consent, transactions will fail.

Based on their feedback, end-users consider this principle as having been achieved, but SP´s in some MS need to go further. In some cases, portals register the business credentials (specific company information and their powers to represent the company) of their registered users and check the validity of the registered information when the end-user requests access to the service or asks to perform operations requiring the credentials. This check is performed "back-office", machine-to-machine and real-time without user interface for the convenience of the end-user. In other service work scenarios, back-office operations performed days or weeks after the end-user was in session (i.e., authenticated via STORK 2.0) may also require checks to insure the up-to-the-minute validity of credentials verified in a previous session. The Powers Validation (PV) operation was designed for these and other cases. Another intermediate example occurs when validating the powers of a mandate from one person to another. Even if the mandate itself is valid it may be necessary to confirm the validity of the powers of the represented person or persons in the case of a chained mandate. This requires

the validation of powers of a person different from the end-user and not a party to the present online session.

Such cases would require special prior consent to have been granted from the interested parties to allow the validation operations to take place outside their online presence, but within certain restricted conditions and for specific purposes.

5.3.4 Lessons learned through interaction with other initiatives

It is important to respect adoption of internal policies and strategies while creating new policies at EU level and vice versa. As seen in Paragraph 4.3.5 (Metric BV.08) STORK 2.0 helps organizations comply with EU policies (Services Directive, eIDAS Regulation, etc.) and helps effective implementation of such policies and wider adoption by many parties (multiplying their impact) as well as feeding input to new policy-making work.

As already mentioned, Pilot Partners in their role as eGovernment for Business service providers and also as operators near to national business registers are working with national and international organizations like ECRF (European Commerce Register Forum) and EBR (European Business Register) on topics dealing with business identity attributes. Synergies with EC initiatives like BRIS (Business Register Interconnection System) and other projects dealing with cross-border Business Registers are also being exploited.

Lessons learned deal with the different approaches to solutions of (difficult) problems in cross-border semantic interoperability in Public Administration schemes and procedures. Issues such as unique identifiers and harmonised Business Attributes are recurrent.

Tight collaboration with CEF, e-IDAS and e-SENS for the last years has significantly contributed to exchange knowhow and experience in order to take into consideration lessons learned during the project and helping to avoid same mistakes or to repeat already achieved success.

The eGov4Business Pilot has also participated at a number of joint e-SENS meetings to exchange experiences and to pass on to the next generation of building blocks the experiences of STORK 2.0.

There is a strong partners presence in the eIDAS expert group where the exchange on eID in public networks is fundamental for the continuity of project and national initiatives.

On the national level most of the partners represent government Ministries or technical agencies that sit on or guide the national workgroups which regulate and implement the MS Public information infrastructures. This allows them to both influence the decisions at the national level in favour of the STORK 2.0 model and results, as well as feeding back to STORK 2.0 difficulties encountered in local/national implementations of eID as a service.

5.3.5 Organizational & governance lessons learned

The lessons described in this chapter will help to contribute to the improvement of the maturity and sustainability of STORK2.0 cross-border services by defining standards for quality, performance and governance, and give recommendations to future partners on how to ensure smooth adoption of STORK services.

Most of the experience originates from feedback given by pilot partners and external stakeholders, but also from feedback given by end-users.

The lessons are useful to new adopters of STORK 2.0 – SPs and B-IDPs – and could help them avoid some pitfalls in organising a trusted service. The information is quite relevant to the sustainability of services.

Lesson 5.1 Engagement of correct stakeholders is everything

Based on the feedback given by pilot partners, an important point for ensuring success and future sustainability of STORK 2.0 is interagency co-operation between all actors of eGovernment service network: technical portal developers, security service (eg, authentication) providers, content providers (Competent Authorities of different sorts and sectors). This was particularly felt in the eGov4Business Pilot since around each of the eGovernment services there was usually a group of agencies and ministries involved in one aspect or other of service provision. In some cases low cooperation between agencies blocked the publication of STORK 2.0-enabled services. In other countries, the Business Register did not agree to connect to the network (for economic or for technological reasons) and some other solution for company information had to be found. Additionally, many of the online services themselves involve integration of different agencies – Trade registers, Tax authorities, etc. – and the lack of a single attribute required by one agency but not supplied by STORK 2.0 with appropriate AQAA level could determine interoperability success or failure.

Interagency co-operation lessons learned are as follows:

- Early in the project a mapping of all relevant stakeholders to different steps in the procedures is needed and getting their approval, sponsorship and in some cases their strong commitment in advance will help to prevent blocking or delaying situations such as those described above. It is important to realise that this mapping should be checked and updated periodically so as not to miss some aspects which may have been overlooked at the start of the project.
- Explaining the importance of the project and making sure that all doubts about legal, trust, security, data protection etc. are addressed.
- New partners will need guidance on how to join the network, what are the requirements and procedures.

These lessons are particularly relevant since many piloting SPs already see opportunities to extend the STORK 2.0 network to other Public Administrations in their Member States.

Metric BV.14 - Opportunities for integrating additional services and portals.

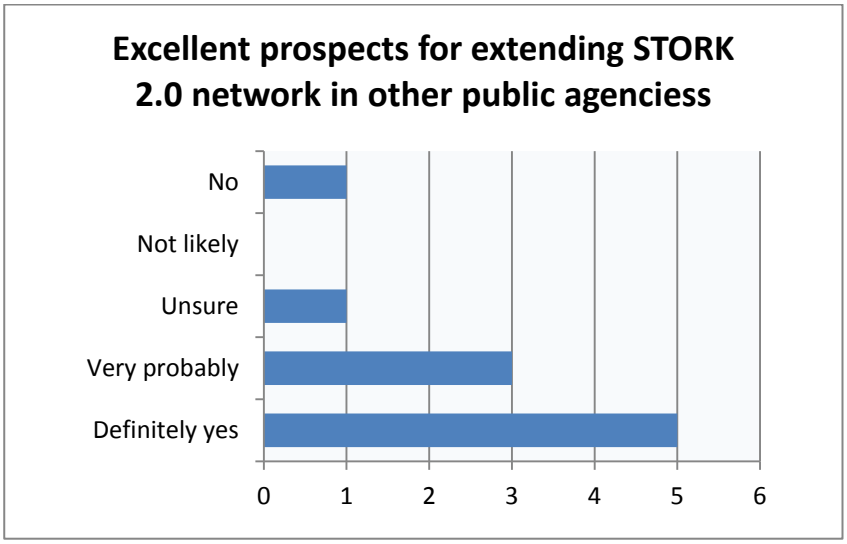

Figure 53: Opportunities for integrating additional Public eGovernment services to Stork 2.0 (metric BV.14, SP Questionnaire Q23)

Lesson 5.2 Time saving and simplification of procedures are considered to be the greatest benefits

Based on the feedback given by end-users (see Metric BV.01 - Documented benefits for end users. and Figure 31) time saving and simplification of procedures are considered to be the most valuable benefits of STORK 2.0 over cost saving and security. Seamless eID management will someday become an essential commodity in cross-border eGovernment, and the demand although still immature, is currently ahead of the supply.

Lessons learned:

- In the opinion of users and service providers alike, saving time and effort in cross-border eService outweigh pure savings in costs.
- Together with changing paper-based procedures into electronic processes, optimization and simplification of procedures – administrative procedures, in particular - need greater focus. This will pose ever greater emphasis on collaboration between agencies and elimination of semantic and organisational barriers.

Lesson 5.3 Long term solution ensuring circle of trust is needed

A clear legal and organizational framework supporting interaction between different stakeholders needs to be in place in order to gain maximum benefit from a project like STORK 2.0. In order to achieve the project results, 14 Member States out of 18 signed a non-legally binding MoU (Memorandum of Understanding), describing the rights and obligations of the STORK 2.0 infrastructure (see chapter 3 of the [8] for details).

Some lessons learned during implementation of STORK2.0 were:

- A semi-formal MoU is not a long-term solution for establishing a European-wide circle of trust. Until the eIDAS Regulation [15] will be fully entered in force in 2018, new Member States may face legal obstacles while joining infrastructures such as STORK 2.0.
- Specific obstacles encountered during project included:
    - A MoU does not offer sufficient value since it is not legally binding;
    - The existing project legal framework is not sufficient. Although the existing legal framework may seem an adequate solution, it does not express the necessary joint commitment and liabilities of all STORK 2.0 participants (see also [8]).

Lesson 5.4 Need for common service level agreement rules

From the governance, sustainability and legal point of view, issues related to service levels are not yet resolved (see [8]). There is no common regulation or agreements stating rules for uptime, downtime, availability etc. of STORK 2.0 infrastructure. In addition to that, each IDP or Attribute Provider may have established its own rules regarding their services and these rules may be in conflict with expectations and needs of other stakeholders.

A particular problem in the eGov4Business Pilot concerned the legal value and the liability involved in the provision of mandate attributes dealing with company representation powers. The danger of “legal person identity theft” is a real one, and as indicated in *Lesson 3.2* Translation of mandates, use of standard values and legal value of STORK 2.0 SAML tokens. The legal basis and the security of the mandate information are fundamental assets of the STORK 2.0 network.

Lessons learned during the project, are as follows:

- On the operating level “industry-strength”, Service Level Agreement (SLA) is essential to guarantee the continuous access and performance levels required of such an international infrastructure. It would help to have attribute providers and service providers bound by certain terms and conditions governing their connection and correct use of the infrastructure and services.
- Neither eIDAS Regulation [15] nor its implementing acts [16] establish specific rules for assuring flawless data exchange and operation of services, and where errors occur, more detailed and clearly established rules for determining liability are needed (beyond generic provisions recognising MS authority).

Lesson 5.5 Definition of appropriate governance model for STORK 2.0

As highlighted by several partner groups and by the STORK 2.0 eID as a Service Work Package, an appropriate governance model needs to be defined in order to secure the STORK 2.0 heritage after the close of the project. An important lesson learned from the pilot is the need for development of STORK 2.0 towards a mature and sustainable cross-border service, especially by defining standards for quality, performance and governance. Future convergence of the STORK approach and the national eIDAS implementations will be an important and positive element of STORK 2.0 adoption and sustainability. This will require adaptation of national legislation, governance structures and regulation frameworks, referring to the eIDAS Regulation. A roadmap for this has been created with short and medium term solutions, and this is discussed in Chapter 6, below.

Lesson 5.6 eID is an enabler for cross-border eGovernment, but usage patterns are slow to change.

The usage of the STORK 2.0 pilot services was completely conditioned by the normal usage patterns of the underlying services offered to cross-border users. In the case of the Public Services for Business pilot (“eGov4Business”) these services deal with business obligations at eGovernment registers and at one-stop-shop portals for businesses such as the Points of Single Contact (PSC) established by the EC Services Directive [17]. Some other portals, the NL Farming portal and the Italian WEEE Registry for Waste of Electronic and Electrical Equipment, for example, allow businesspersons to perform their periodic, annual or seasonal duties online, saving a the trip to the front-office. However, usage of individual services by individual end-users remains infrequent, tied to the demands and deadlines of normal bureaucratic operations. Facilitating access to services will broaden the market of the eGovernment services, but it is not reasonable to expect it to multiply the service usage.

5.4 Lessons learned for eID as a Service

5.4.1 Commercial aspects and business requirements lessons learned

This section covers the lessons learned in considering eID interoperability as a service offering to national customers in order to support the development of a sound business model.

The lessons learned:

- are intended for SPs and B-IDPs as potential adopters;
- are learned from the eGov4Business pilot partners, interaction with the MS infrastructures and, of course, from the final users;
- are useful for the specific STORK 2.0 workpackage “eID as a Service” mainly as input to their own business modelling and decision-making;

- can be essential factors for the adoption, as they address commercial aspects and business requirements;
- have an important impact on sustainability, as they report expectation and needs from the adopters, expressed during the piloting phase.

Information was collected confronting Partners and using sources for evidence such as SP questionnaire provided by the eGov4Business pilot partners; final users' Feedback Forms; eGov4Business periodical reports.

It must be said that due to the, in some cases, more limited piloting period most Service Providers are still in the process of defining their future service developments or improving the existing ones, and thus have not yet fully elaborated a well-defined commercial model; some preliminary indications regarding unwillingness to pay for services have already been seen in Figure 25 of Paragraph 4.2.3 where the effect of the free of charge position of eIDAS in relation to cross-border authentication to public services was seen . The same goes for B-IDPs whose integration in the national eID infrastructures are still being planned and implemented in most MS.

It is a fact that the eIDAS Regulation will require that a minimum set of government services be provided for free, but it does allow public agencies to offer "added value services" which will require the sorting out of appropriate pricing models, taking into account that new services which start as rather expensive often gradually become commodities or even public utilities. The STORK 2.0 infrastructure aims to be consolidated through short-term sustainability actions in order to become or be integrated in the CEF "eID building block" solution for all other digital government and digital marketplace initiatives.

Lesson 6.1 Cross-border services made possible through STORK2.0 integration

Some of the eGov4Business pilot services could not be offered economically to foreign customers without STORK 2.0 cross-border eID. One reason for this, for some services, was the difficulty in reconciling the high cost of the required security with the low volume of usage of the services. Developing ad hoc or in house services was prohibitive.

As seen in Figure 40 in Paragraph 4.3.8, above, the majority of responding SPs indicated that STORK 2.0 Authentication allowed their services to be offered to foreign professionals or companies for the first time, either because an equivalent level of trust couldn't be otherwise guaranteed, or because it would be too expensive to manage a sure identification of the foreign subject. Services that yesterday were offered only to national businesspersons and companies, because of the positive cost-benefit ratio, can now be extended to EU neighbours at marginal additional costs.

Lesson 6.2 Added STORK-enabled functionalities improve SP services

As seen in Chapter 4, STORK 2.0 integration helps SPs improve their services by making access easier, document exchange and contact with the SP simpler and reducing overall service time and even travel costs, thus raising the overall quality of service and improving the SP image in the eyes of end-users. SPs also expressed the same feelings about the improvements in their service quality and image.

Although security is essential to an eGovernment service, SPs must always bear in mind – and should stress in their marketing communications - those benefits which end-users value most, convenience, simplification and time savings (see Figure 31: End users preferences for benefits provided by STORK 2.0 integration (metric BV.01, Feedback Form Q8)).

Lesson 6.3 Time for SP migration to STORK2.0 needs to be reduced and the operation simplified if possible

Considerable efforts were spent by SPs to make their Services compatible with STORK 2.0 infrastructure.

eGov4Business Service Providers estimated the amount of time (effort in person-months) it would take to deploy their services assuming the infrastructure was stable and not subject to all the changes and improvements seen in the STORK 2.0 project lifetime. This information helps future adopters assess their own service integration efforts against the major benefits of having cross-border interoperability.

Figure 45 in Paragraph 4.4.1 shows that 60% of SPs estimate a deployment time of less than 2 months and 90% of piloting SPs estimate deployment within 3 months. This meant that a priority issue for final (and future) development activities is the creation of an improved STORK 2.0 integration package which could significantly reduce the costs of implementation for SPs. Excessively high integration costs could deter potential adopters.

Lesson 6.4 Fees and models for payment

When questioned about possible payment models for STORK 2.0 cross-border eID interoperability services, SPs were both undecided and unwilling to express themselves. Flat fees, pay-as-you-go (cost per transaction) or mixed models received equally lukewarm responses. The general consensus was that it rests a political decision and that additional study is required to determine whether – and to what level of service – eID should be a free public infrastructure.

Some specific comments provided by SP partners:

- We cannot provide this answer, it would be only speculation and personal opinion.
- There is no special methodology in place to make an exact estimation. But taking into account eIDAS Regulation, cross-border e-authentication should be free of charge for public administration.
- No opinion on this matter yet.
- Some SP services require payments (about 20% of all services), but we do not foresee taxing eID authentication services between PEPS.
- This has to be considered further and is a political decision.
- This question cannot be answered right now, since it depends on political decision related to data exchange, but in general STORK services should be free of charge (at least between government agencies).

5.4.2 Standardisation lessons learned

This section will include lessons related to the use and enforcement of standards on the development of STORK 2.0.

The lessons learned:

- are learned from the eGov4Business pilot partners and their experience during services integration;
- are intended for the maintenance of the STORK 2.0 results;
- should simplify future software maintenance and development
- can accelerate and promote adoption;
- have an important impact on sustainability.

Information was collected confronting Partners, interacting with other initiatives (e.g. e-SENS, eIDAS) and by means of end-user feedback forms answers.

Lesson 7.1 Need for a homogeneous GUI

At national level, the local parts of PEPSes have not always been developed in an homogeneous way having in mind a same approach in terms of clarity of the user interface, functionality, the ease of use.

The consequence can be, in some cases, that of giving the final user the perception of not having a clear idea of the path he is following during the authentication procedure. A common approach is also needed for the use of key terms; too frequently key-words are related to technical jargon (e.g. the use of the word "attribute" in PEPS user interfaces, which has a specific meaning in an XML structure context, but should be replaced by a more common term such as "information" in user dialogues).

Moreover the lack of more homogeneous standardization at GUI level, beyond existing guidelines and best practices provided, doesn't help the final user feeling that he is in control of his own data, as the passages from SP to the different actors in the STORK national infrastructures (foreign PEPS, national PEPS, Attribute Providers) can disorient the end-user.

Metrics regarding ease of use (see Metric UU.1 - End-users' perception of usability. in Paragraph 3.3.1) and data privacy and security (Metrics DP1 and DP2 in Paragraph 3.3.2) received acceptable but not exceptional ratings from end-users. STORK 2.0 aimed for higher ratings, typical of mature, market ready services.

Lesson 7.2 Further efforts needed to standardise the STORK 2.0 Mandate

Mandates carry critical information about a person's power to represent or act on behalf of another person, legal or natural. The lack of a standard among MSs, when dealing with both form and content of mandates, created legal implications and liability issues which seriously affected the terms of the Piloting. Temporary solutions must be made more robust and permanent to avoid negative impact on adoption, but solutions will not be easy or quick.

Pilot partners and their MS representatives are actively engaged in consultations with the ISA^2 Program for continuing work on representation powers and mandates, to best ensure semantic interoperability and harmonization in this area. Pilot partners are also working with national and international organisations like ECRF and EBR on this same theme. Synergies with EC initiatives like BRIS (Business Register Interconnection System) are also being exploited.

If mandate structures become more standardized then it is reasonable to expect improved services from the PEPS regarding their automatic processing. Their current status lies somewhere between fundamental eID information and specialized domain attributes. (see for example D5.3.4 chap.5.4.1 [4]). A more complete handling by the PEPS, for example of all intermediate elements comprised in chained mandates, could simplify processing for SPs and provide useful added value to the STORK 2.0 infrastructure.

Lesson 7.3 Greater use of standards in developments

The adoption of the SAML standard adds significant value to the pilot implementation.

The SAML architecture is the simplest way to guarantee a secure and strong implementation of message interchange in a "point to point" scenario. STORK 2.0 designed a federated environment based on single point of contact in each Country (PEPS or middleware) avoiding the need for a direct communication between the SP and the foreign IDP.

That said, the project implemented the SAML 2.0 standard concerning the token syntax definition only. The PEPS handling of complex attributes (e.g. mandates) was not fully developed so that more effort is needed on the part of SPs to handle them, at times by means of agreed workaround solutions. Concerning nodes (PEPS, IDP, AP), metadata "look for" functions and "node to node" service functions, typical of SAML 2.0 objects, were not implemented.

STORK 2.0 should consider making greater use of data modelling and processing standards – even those already adopted, like SAML 2.0 – for future improvements and benefits.

Lesson 7.4 Further developments of the STORK 2.0 QAA/AQAA model vs. convergence with eIDAS model

From the point of view of the eGov4Business SPs and B-IDPs (Business Registers), the overriding factor regarding standardisation, concerns the compatibility with the national eID mechanisms implementing the eIDAS regulation. More generally the QAA/AQAA scheme is similar to the eIDAS model and both have taken ISO 29115 into account.

Although some improvements to the STORK 2.0 model have already been suggested and implemented, the main appeal of the STORK 2.0 solutions derives from their compatibility with EU and national approaches therefore that must be maintained at all costs.

5.4.3 Trust & normal working practices lessons learned

This section will go through the lessons learned on the field of the trust model definition. The lessons are learned:

- Mainly for the top-level stakeholders, like the EC and the MS.
- From the pilot partners and users.
- Have an impact on sustainability.

The information was based on the answers provided by Pilot partners by email exchanges, from SP questionnaire and Users Feedback Form collection of answers.

Lesson 8.1 the STORK 2.0 "circle of trust" and AQAA mechanism

A critical area affecting cross-border interoperability involves the different elements bringing trust in the STORK 2.0 network. A basic component – already cited among the Standardization Lessons Learned – is the Attribute Quality Authentication Assurance mechanism for measuring the reliability of attribute assertions. The handling of the AQAA scheme (not only by SPs but also by B-IDPs) was not as straightforward as planned (see Paragraphs 5.3.1and 5.3.3) and in some MS it was difficult to map AQAA requirements and criteria to specific national contexts. To help partners overcoming this issue, easing the task for SPs and B-IDPs of measuring respectively the required level of services and the quality of attributes, by means of the AQAA scheme, a "cookbook" (practical guide) document was developed, as Addendum to D3.2 QAA Status Report [6].

Feedback on the cookbook from Pilot partners was positive in 50% of cases in which it was reported that the cookbook helped to assess the AQAA levels for managed attributes. In order to build trust at every opportunity it would help to include similar simplified descriptions of some of the key trust mechanisms of STORK 2.0 in all STORK 2.0 documentation.

Lesson 8.2 Reliability trust and security of STORK2.0 for mission-critical services

The STORK 2.0 infrastructure, as far as reliability, trust and security are concerned, is perceived by Service Provider as adequate for Piloting purposes but still lacking some "industrial-strength" features. Responses to SP Questionnaire Q38 "What would be necessary for you as service provider to trust mission-critical services to the STORK 2.0 infrastructure?" show how SPs are concerned about this topic; some answers that is worth to mention:

- "SLA (Service Level Agreement) of STORK and mean uptime is essential since our service depends on external service provider and any delay reflects on our service as well".
- "Improvements are still needed at legal level MoU (Memorandum of Understanding), functional level (Mandate Management) , quality assurance and SLA"
- "Need of agreements between countries with assurance that PEPS would be supported in the future"
- "Proven security, MoUs, SLAs, clear governance"

End users were also asked, more in depth, through the extended Feedback Form section, to express whether they felt in control of the data transmission of their personal data during the whole online process (for the specific service accessed). The answer reached a 67% of positive results; the same range of positive result (70%) was expressed on the question concerning the User feeling on the entire procedure as "secure enough". As mentioned in the previous Paragraph, this feedback level is acceptable but not exceptional, and effort on several fronts should be made towards improvement.

It goes without saying that improvements in reliability, trust and security are needed in order to guarantee the continuous access and performance level required of such infrastructure, to prevent or minimize the risk of service failures or security flaws that would, in turn, cause a loss of confidence on the accessed services, and consequently a severe image of STORK 2.0; an even stronger MOU, endorsed by all participating MS, would be needed.

In this context, standard eGovernment SLA levels should be adopted by all actors in STORK 2.0 in order to grant a harmonized minimum level of trust for STORK 2.0 services.

6 Pilot adoption and sustainability roadmap

6.1 Overview of pilot sustainability

As seen in the previous Chapter 5 on Pilot Learning, the eGov4Business piloting experience, although limited in time and intensity, did provide ample opportunity to encounter, study and handle many of the issues that present themselves as either barriers to future development and sustainability of the STORK 2.0 network, or as accelerators of that development. By considering all of these factors in the short, medium and long term perspectives we are able to map out a strategy, or roadmap, to preserve the most valuable STORK 2.0 assets and experiences in order to maximise the return of investment, for partners and the EC, and consolidate the position of STORK 2.0 in the scenario of pan-European identity federation solutions. Partners of the eGov4Business Pilot, in general, are particularly interested in maximising the chances for sustainability of the results achieved because they are often involved in the establishment of part of the national eID infrastructure, either the PEPs node or the B-IDP business credential and mandate provider.

Sustainability on the short-term lies largely in the continuity provided by project partners, in their willingness to continue providing STORK infrastructure and SP services as well as in the fact that many of them are able to support these efforts from within other projects, notably e-SENS which is taking up STORK 2.0 results in their eID building Block [26]. In the medium-term, this eID building block will be integrated into the CEF infrastructure [20] where it should evolve into a longer-term solution.

The following graphs concretely measure the willingness of eGov4Business SPs to promote STORK 2.0 solutions by maintaining their current services[2] and by spreading the STORK integration to other services in their own and nearby domains.

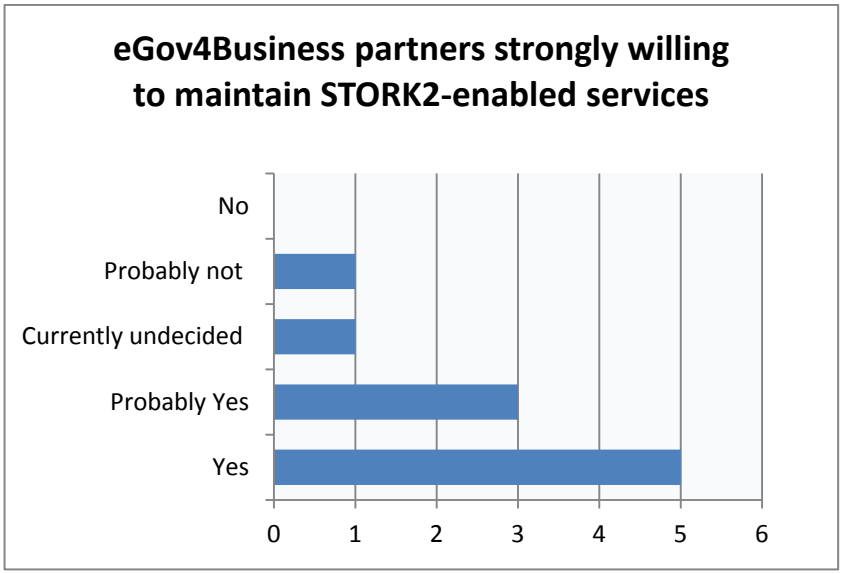

Figure 54: Willingness of eGov4Business SPs to maintain STORK 2.0 integration after the project (metric BV.16, SP Questionnaire Q13)

[2] We note that in communications to Project management at the end of the project ten (10) piloting SPs indicated their willingness to continue running their services after STORK 2.0.

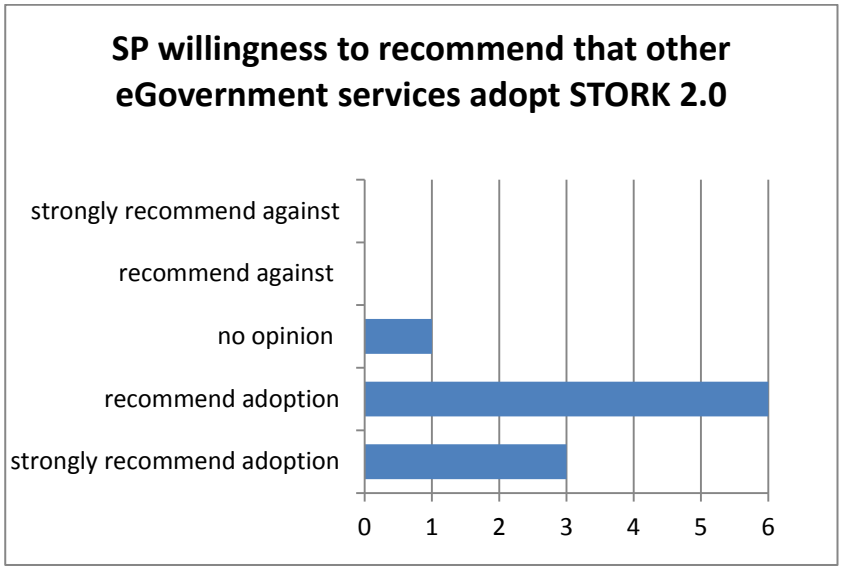

Figure 55: SPs favour STORK 2.0 adoption by other eGovernment services (metric A.1, SP Questionnaire Q36)

Sustainability of the Public Services for Business Pilot can best be considered in the two main phases which were experienced during piloting and which roughly correspond to the phases of eGovernment maturity "integrated services" and "transformed services". The first phase, in the case of the eGov4Business pilot, consists in the integration of an existing eGovernment service with STORK 2.0 authentication and credentials. The second consists in the change in procedures which becomes possible when identity, and to an even greater extent, business credentials being available and automatically processed online lead to change in the eGovernment service procedures themselves. Out of session and/or offline transmission and verification of documents may become automatic, requests to the end-user may be transformed into direct back-office connections between agencies in different countries, harmonised data facilitate automatic processing of information, once again allowing certain offline delays to be entirely avoided.

Both STORK 2.0 operations, basic authentication (AuthN or AU) and authentication on behalf of (AUB) opened up possibilities in each of the phases of eGovernment maturity, but clearly, it was the AUB procedure that encouraged much more extensive and deep integration and service transformation. Such transformations led to many of the new challenges in interoperability which were discussed in the previous Chapter(s). These were the "unchartered waters" which made STORK 2.0 piloting such a pioneering endeavour

A good overview of the opportunities and the potential for businesses created when existing eServices are enhanced, or leveraged, by cross-border eID is given in the 2012 EC "Study on Analysis of the Needs for Cross-Border Services and Assessment of the Organisational, Legal, Technical and Semantic Barriers" [13]. The quantitative analysis of this study listed the following as the services most in demand: consulting the business register, paying social contributions for employees, filing various tax declarations, submitting a tender for public procurement, etc. The study identified eID as a key enabler and the cost-benefit analysis has estimated the cost of implementing a cross-border eID mechanism on top of an existing service as from 150-200 k€. These figures are roughly compatible with the estimates of effort and savings (in person-months) given by STORK 2.0 partners (see Section 4.4.1. On the other hand, the study indicated as a recurring barrier that there "are no comprehensive building blocks that would allow SP's to easily develop comprehensive solutions" and also that "a

major challenge for many services is readiness of local infrastructures, stakeholders and legislation". With the building blocks developed by STORK 2.0 and a clearer view on deployment costs (section 4.3.2.1) together with the legal certainty through eIDAS Regulation, SPs are now less hindered by this barrier and may more readily invest in releasing the cross-border potential of their business services. We recall from Paragraph 4.3.8 that 7 out of 10 eGov4Business pilot SPs used STORK 2.0 infrastructure to reach cross-border markets for the first time. This is certainly a strong selling point for the service.

Sustainability of the main use cases is made more achievable by the production integration already implemented in major services and portals like in AT, EE, GR, IS, IT, LT, LU, NL, SI and SK. The experience can easily be exported to other services. This already has been started through introducing the use cases to the e-SENS large-scale pilot which is taking up STORK technology in three ways: first in the further development and maintenance of the STORK-based "eID building block" itself; then in the piloting activity of the "Business Lifecycle pilot"[27] which sees many partners integrating the STORK eID building block; and finally, in the newly added Pilot domain of "eAgriculture"[28]. The main purposes of this last area are to work on the expansion of the successful STORK 2.0 cross-border farmers use case and on the convergence of STORK 2.0 solutions with the implementations of the eIDAS Regulation.

However, two prerequisites for the sustainability of the STORK 2.0 infrastructure and the start-up of new use cases within e-SENS or around the STORK 2.0 pilots are:

- the guarantee of well managed and maintained software and
- the establishment of an adequate governance structure – organisations and rules – to create an environment of trust, security and legality that is essential to cross-border eGovernment services.

Regarding the first point, the STORK 2.0 project consortium, acting through their co-chairman, successfully petitioned EU DIGIT and e-SENS to provide a short term home for the STORK software, organizational infrastructure and know-how, and to actively start the management and maintenance of STORK software.

Concerning the second point, an important first step is the liability regime established in Art. 11 and Recital 18 of the eIDAS Regulation [15]. This will be sufficient for short-term developments, but will need further study to encompass the future complexity of the services and organisations involved, in particular regarding the differences between eGovernment actors and services and those in the private sector , in particular for aspects related to respective liability regimes, support levels and advanced business and pricing models (for more details on these aspects see D5.2.5 eBanking Pilot Final Report [12]).

The area where the pilot navigated unchartered waters is to be seen differently, like on AUB with mandate semantics. In bridging the few national islands where such services currently exist, STORK 2.0 has achieved significant results, evolving STORK 2.0 specifications to include attributes for legal persons and representation powers and mandates, and adapting the procedures implemented in the SW building blocks to allow cross-border transfer of this kind of information integrated in real eGovernment processes. The feasibility of the developed solution has been verified by means of the STORK 2.0 pilots, in which use cases that require cross-border access to information about representation capabilities have been successfully tested. Besides that STORK did add the concept of role based mandates and the subject has been explored in a special interest group. Issues explored are, among others, the concept of service based mandates based on common semantics, transport of 'original mandate' information supporting text and images and the transliteration of the Greek character set. For the latest challenge a solution was elaborated and implemented.

However, the project has also encountered new, important barriers that currently hinder the adoption of an EU wide solution for cross-border transfer of information on powers of representation of companies or persons, the most relevant being the lack of a common semantic framework. Representation is complex and the national solutions are often too much focused on country specific details. Therefore, although there are some similarities among countries, there is not a shared European taxonomy about representation powers and mandates, and that prevents powers/mandates information originating in one country from being directly machine-processable in another. So in particular on electronic mandates a far better knowledge of the MS situation is needed. While eIDAS addresses the basic AUB scenario, mandate semantics is complex and should be explored and piloted in new projects under the ISA^2 umbrella or in CEF or Horizon 2020. Further work is needed in particular to get a better view on MS not involved in STORK or in domains that haven't been piloted. Therefore, STORK 2.0 MS Council did request DG Informatics, entrusted by the European Commission to manage the ISA programme, to take the necessary steps to promote the adoption of actions, under the ISA programme and its successor ISA^2[23], aimed to continue the work performed in STORK 2.0 regarding the semantic interoperability and harmonisation of representation powers/mandates information about legal entities. This action was supported by all Member States.

Summarizing the overview, the ground for pilot sustainability and reach-out to further services is laid by eIDAS and the STORK 2.0 building blocks in areas covered by eIDAS. This is also supported by e-SENS. In areas where further work is needed – mainly on mandate semantics that is not touched by eIDAS – STORK 2.0 has taken action to start this work through ISA$^{2.}$. Because at least 8 service providers will continue to maintain the successfully piloted services, STORK MS-Council and co-chairs initiated the process of handing over STORK 2.0 software, know-how and organizational processes to enable e-SENS[3] and CEF to take-over the management and maintenance of STORK 2.0 software and in this way ensuring sustainability of the STORK 2.0 infrastructure until essential STORK 2.0 functionality and attributes are supported by the ultimate solution: the eIDAS node.

6.2 Pilot outcomes relevant for eIDAS & CEF

The EC has already, in the framework of ISA, maintained the STORK1 software, common specifications and QAA model [29]. The code is improved in several aspects (such as bug fixing, adaptation for various application servers etc.). This implementation of STORK is used by the ECAS service of the EC [30].

The STORK 2.0 project has shown how extended federated European-wide eID management can give a major boost to cross-border eGovernment services in Europe. Based on the original STORK1 common code, the project developed functionality for cross-border representation of legal entities, for the exchange of specific attributes and support for additional use cases specific to the eGov4Business pilot, such as powers validation and SSO (persistent logon at a single SP).

Ten of the thirteen piloting MS took the STORK 2.0 software into production, performed production tests and performed service deployment and launch. To continue this service delivery after the lifetime of STORK 2.0, maintenance of the STORK software is necessary.

[3] "e-SENS will continue to learn from the experiences of previous LSPs as well as Member States and associated countries to ensure the use of best practices and consideration of national requirements. e-SENS will consolidate, improve and extend the solutions developed in order to create general purpose components that can be extended to other domains", http://www.e-SENS.eu/about-the-project/project-background/

After all, if after the end of the STORK 2.0 project a security issue occurs, prompt intervention of a technical support team will be necessary. With STORK 2.0 partners formally no longer being responsible, someone needs to take care of such an issue, if sustainability is to be achieved.

Besides that, the e-SENS pilots also depend on a reliable infrastructure for authentication of users and for the retrieval of personal and business identity attributes.

eIDAS liability regime is relevant in this respect, particularly for scenarios like those piloted in eGov4Business with a rich set of actors. The eIDAS liability regime is linked to the notification of identification schemes by the MS and distinguishes between the liability of Member States, identity providers, and operators of authentication procedures (equivalent to a PEPS/V-IDP operator in STORK 2.0). In that sense, the approach of the eIDAS Regulation considers the distinctions between the participants in an eID ecosystem relatively well. Each of these parties are made liable for damage caused intentionally or negligently to any natural or legal person, exclusively in relation to the components of the identification process over which they can exercise substantial control. In practical terms, liability must be borne [4]:

i. by the notifying MS for the ability of an eID to be uniquely linked to a person at a specific assurance level, and for the availability of an eIDAS node (e.g. a PEPS /V-IDP in STORK 2.0 that confirms identification data);

ii. by the issuer of electronic identification means (IDP) for the attribution (i.e. the linking) of the means to a unique person;

iii. by the party operating the authentication procedure (PEPS/V-IDP/eIDAS node operating organisation) for the ability of this component to correctly confirm identification data.

All liabilities under eIDAS are to be interpreted in accordance with national liability rules, which may in practice limit specifically the liability of Member States or national public bodies; on this point, the eIDAS Regulation does not provide for perfect harmonisation. In addition, the Regulation does not cover other “parties to a transaction” where eIDs under eIDAS are used, meaning that Service Providers liability remains covered under respective national liability rules. Thus, the eIDAS Regulation represents a significant step forward compared to STORK 2.0’s non-legally binding Memorandum of Understanding.

It can therefore be concluded that as of Summer 2015, an EU-wide infrastructure exists encompassing over 60 SPs (10 in the pilot) and 21 APs (of which 9 are related to the pilot), based on the STORK 2.0 software, which meets a real European demand which is complementary to other eGovernment infrastructures and organisations such as the network of PSCs or of Business Registers and which is capable of providing cross-border interoperability to enable such networks.

Service providers, citizens and businesses rely on the survival and conservation of a secure and reliable infrastructure so that SP’s can provide cross-border services and citizens / businesses can start service delivery process after authentication with a national eID authentication token. At the same time, start of voluntary recognition of notified eID schemes under eIDAS auspices (Art.9, with a horizon for mandatory recognition of 3 years) represents a major driver for uptake of eID across the EU and further stimulates the need for strong support of cross-border eID solutions at MS and EU level (e.g. eIDAS Cooperation Network is also being launched as per Implementing Regulation (EU) 2015/1501).

[4] It does not affect those national rules on, for example, definition of damages or relevant applicable procedural rules, including the burden of proof.

Rationale and business justification:

As stated earlier, cross-border authentication supported by the STORK 2.0 infrastructure is up and running, it is moving beyond the pilot phase towards full operation under CEF/eIDAS. Ten eGov4Business SP's will maintain the service after the project. So there is a business demand for continued management of the existing STORK 2.0 infrastructure.

After all, experience shows that setting up an EU-wide infrastructure is necessary, but not sufficient to really guarantee a boost in cross-border services. Even the impact of an EC Regulation requires an ambitious set of wide-reaching actions to be fully implemented. Cross-border service delivery, underpinned by authentication with national eID tokens will only get a boost, and thus can ensure the increase of economic growth desired by the EC, when citizens and businesses (facilitated by the cross-border service) perceive its added value and when they start to use their national eID to start cross-border service delivery. This awareness-raising can be supported by use cases that will generate large numbers of users: enrolment of students, Tax services, services related to citizens in border areas, services related to pension funds.

To meet this goal there are several prerequisites after the lifetime of the STORK 2.0 project, in particular in relation to the CEF building blocks that support eIDAS, to the eIDAS interoperability framework implementing act [16] and to its related technical specifications (which refer to "eIDAS node" for what has been called "PEPS" or "V-IDP" by STORK):

- STORK 2.0 software maintenance;
- Assessment of functionalities extended by STORK 2.0 with respect to STORK1, to identify those which require immediate convergence with the eIDAS node, and the creation of a roadmap for the convergence of functionalities requiring further implementation and/or study;
- Establishment of a decision making process on the roadmap for convergence of STORK and the eIDAS node;
- Resources for the implementation of the roadmap, in particular for adding functionality to the eIDAS node;
- Setting up maintenance of the converged software and implementing maintenance
- Setting up a governance structure and adequate formalisations of liabilities of actors and service providers, including service level responsibilities and guarantees.

The eIDAS regulation defines which attributes are to be exchanged: the minimum dataset. This set is smaller than the STORK 2.0 dataset and is defined slightly differently at points. To ease the exchange of these attributes, , based on eIDAS technical specification which are in turn largely based on STORK 1, DG DIGIT develops the eIDAS node and associated eIDAS SAML profile. For STORK 2.0 countries however, it is not likely that they will replace their STORK infrastructure by the eIDAS node but rather that STORK 2.0 and eIDAS might co-exist. For example, some non-STORK countries may deploy just the eIDAS node reference implementation, while STORK 2.0 countries may prefer to continue to have their infrastructure in place as long as it remains compatible with eIDAS and as long as needed to support the service delivery processes based on STORK 2.0 attributes and functionality. Factors influencing such decisions are:

- Some countries already use the STORK 2.0 software in their production services
- It takes the member state considerable effort to migrate

- It requires time and budget of SP's, IDP's, AP's and business registers to migrate
- The eIDAS node does not support exchange of all the STORK 2.0 attributes out of the box
- The eIDAS node does not provide for all the STORK 2.0 extended functionalities or procedures, like powers validation, single sign-on and anonymity
- A need for compatibility exists with eIDAS nodes (achievable through adapters that may be developed in the context of e-SENS)

The eGov4Business Pilot considers the following STORK 2.0 functionalities as essential. Integration of these features in the eIDAS node is strongly recommended to enable the ongoing and uninterrupted exploitation of the cross-border services developed in STORK 2.0 that are now in production:

- StdIDP –standard STORK authentication (covered in eIDAS)
- AUB – authentication on behalf of
- B-IDP, Legal Person IDP & Mandate Provider (MS specific), assurance and maintenance of their connection to the interoperability infrastructure is key as is the continuity of management by such infrastructure of transportation of information coming from them (related to legal persons attributes and other information needed in electronic mandates which has been defined and used in STORK 2.0)
- Representation Powers Taxonomy (EU-wide "ontology")
- V-IDP (allowing interoperability with MW countries like Austria)
- XHTML signature functions (allowing to sign electronic forms, e.g. XAdES format)

Some other required features, but of a slightly lower priority are:

- Improved handling of Multiple Attribute Values (for company powers and mandates)
- Chained mandates (if a MS maintains chains internally, but asserts the endpoints i.e. "representative X is representing Y", then eIDAS covers this but the chain itself and mandate content are not currently in eIDAS scope)
- Improved attribute aggregation features to enable arbitrary multiple MS processes (for example the 3-MS scenario which sees the IDP, the B-IDP and the SP in three different MS)

All these issues have been brought to the attention of both the Commission (DIGIT, CEF) and the e-SENS management board. Currently (end of September / early October 2015) this has to be settled in agreements between DIGIT / CEF, e-SENS, STORK 2.0 MS and STORK 2.0 co-chairs which are all involved in the discussions.

6.3 Challenges for adoption and proposed actions to overcome them

We briefly consider here some of the main risks for pilot sustainability under the planned convergence.

First, interoperability in STORK 2.0 for specific pilot use cases depends on which functionalities and attributes are supported by respective national common infrastructure components (PEPS/V-IDP). Different MS implementations may lead to partial interoperability between MS for a given particular service requiring an unusual combination of features. To reduce this risk a maximum of transparency and feature/requirement tracking has been performed as Pilots have mapped all STORK 2.0 common functionalities and attributes to

pilot use case needs. This information has been handed over to DIGIT and to e-SENS for evaluation and as support for relevant decision-making.

Another critical short-term risk stems from the fact that the STORK 2.0 project, and together with it the maintenance of the STORK 2.0 software, ends at the end of September 2015. As a big bang migration from STORK 2.0 to the eIDAS node is not expected, this imposes a risk on software security and interoperability of cross-border authentication in countries that have deployed the STORK 2.0 software in their production services. The extent to which e-SENS will help in addressing this risk in the short term is being discussed by all interested parties.

Action lines to address all risks have been discussed by the STORK 2.0 MS Council. The results, discussed above, are the relations created and the expected orchestrated collaboration between initiatives of individual STORK 2.0 partners the EC, in particular DIGIT, ISA and CEF, and on the short term the e-SENS Large Scale Project.

The main organisational challenges for adoption and evolution of the project results have been discussed in the previous Section 6.2. Actions to meet these challenges have also been thoroughly described. The overriding premise is a convergence with eIDAS implementation on technical, organisational and governing levels. The practical necessity of identifying resources which could be allocated to the corresponding tasks has also been performed and is in the process of verification.

Individual challenges of a more technical, organisational and legal nature have been discussed as Lessons Learned in Chapter 5. They include issues such as

- Adequate support and documentation of a federated system for eID management to facilitate integration of new actors (MS, IDPs, APs, SPs)
- Governance mechanisms to define responsibility and to monitor and guarantee overall system and service SLA
- Areas of technical improvement: end-user interface, procedure optimisation, attribute data standardisation
- Further development, establishment and maintenance of trust and security mechanisms (AQAA, certificate and key management)
- Language and character set interoperability barriers
- Semantic barriers concerning company powers and other legal person attributes
- Clarifications concerning the co-existence of free and fee-based information

Under the proposed STORK 2.0/eIDAS evolution and convergence scheme these issues will be more deeply addressed by the organisations providing continued development of the CEF building blocks [21]. Several of the issues regard deep process transformation and cross-border legal issues which will require considerable further study and pioneering.

All of this is perfectly coherent with the general results and observations of the Deloitte study [19] of 2013 which identified, in general, the key challenges for sustainability of large scale pilots (LSP) results to be as follows (extracted and rephrased from study):

- **Participation of stakeholders** groupings which already exist but either require further support, are not sufficiently represented, or lack a means of participating in the management mechanisms. Provisional mechanisms may be needed until permanent solutions can be found.

- **Need for governance** which is strongly dependent on the maturity of the platforms and on their varying needs for coordination. Less mature solutions may require stronger and higher intensity governance approaches to support more rapid development and enforcement of standards and norms.
- **Market maturity**: not all core service platforms/building blocks fully qualify as market services. Services may be mature at the national level but less so at the cross-border level. It is probably not appropriate to take a market-based approach for all services. Some services will need continuing public sector support until the market is ready to play its role. Maturity will be greatly improved under the umbrella of CEF.
- **Technical maturity**: Not all building blocks have clear consensus on how interoperable communications can be organised across the EU. This implies that some platforms require more extensive efforts to guide their establishment, whereas others simply need their existing outputs to be maintained.
- **Financing mechanisms**: eID is offered as a market service in some Member States, and is entirely government-funded in others. This evidence implies a need for flexibility in the organisation of a variety of funding mechanisms and streams at the national level. At public sector SP level, the electronic identification and authentication services, need to be provided for free according to eIDAS Regulation.
- **Take-up**: The take-up of LSP solutions – whether by users/customers, public sector organisations, or private sector firms – varies quite considerably according to their status as pilots rather than as fully functional, stable solutions. Therefore, adoption cannot be taken for granted; considerable attention needs to be paid to how take-up might be facilitated, and how near that take-up is to the market.

The same study positions (personal) eID as shown in Figure 56: Relative maturity of LSP building blocks, below. The innovative STORK 2.0 extension of personal eID management to cover Legal Persons and their representation at eGovernment services would certainly lie at or closer to the "emerging" end of the spectrum.

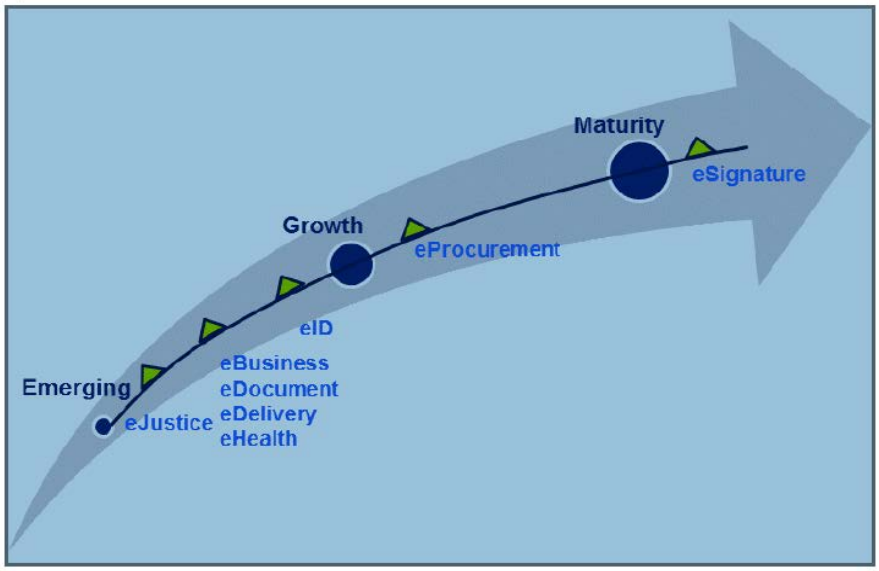

Figure 56: Relative maturity of LSP building blocks

6.4 Commercial projections for business models and roadmaps

The commercial prospects for cross-border eID-based authentication services in Public Administration service contexts such as that of the eGov4Business Pilot have been severely limited by the conditions of the eIDAS regulation. In particular we cite Art. 7 clause (h) of [15]:

> *The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body*.

Under the above restriction, it is still useful to consider a SWOT analysis approach to the Strengths, Weaknesses, Opportunities and Threats which condition the future sustainability of STORK 2.0 solutions in the domain of Public Services for Businesses. Business cases may be developed based on services offered to authenticated users, when it is legal i.e. to charge a price for such services. Business drivers and financing support to sustainability of eGovernment services could therefore be explored in relation to such possibilities, but given that the scope of STORK 2.0 is to enable electronic identification and authentication which needs to be provided for free, the analysis of business models specific to other non-free services exceeds the scope of our considerations provided here.

Strengths of STORK 2.0 federated cross-border eID infrastructure

- STORK 2.0–enabled services have been implemented and deployed in national eGovernment service portals in ten different MS. Each portal presented its own set of services and its own technical architecture requirements for applications and for security. Moreover, each MS presents its own legal and cultural particularities which create strong pressures on semantic, legal and organisational interoperability. This broad bed of pilots is a unique proving-ground which only STORK 2.0 can claim to have experienced.
- eGov4Business SPs have been piloted by hundreds of real-life end-users, many of whom provided feedback for the future evolution and improvement of the services.
- The eGov4Business pilot has provided the most extensive and significant on the field testing of authentication procedures involving a “natural person representing a legal person”; the implemented procedures go beyond eIDAS requirements in terms of process automation, attribute gathering and semantic interoperability across borders.
- Business eID Attribute providers, B-IDPs, were successfully integrated into the STORK infrastructure in 8 out of 13 eGov4Business MS participating in the pilot; in spite of interoperability issues, this represents a significant foothold in the Business Register world and a significant advance which will be developed in the future as part of the Business Register interconnection system [18].
- A commitment from partners and EC alike to advance STORK results in the context of the CEF building block consolidation effort is underway in e-SENS, in particular, in the eID workgroup[26], in the Business lifecycle pilot[27] and in the newly created eAgriculture pilot[28], created thanks to the success of the STORK eGov4Business initiative.

Weaknesses

- Not all the eGov4Business partners successfully implemented the AUB procedure, which proved more complex and costly than foreseen, and reducing confidence in those results
- Full piloting duration was achieved with a limited number of MS-combinations, and successful piloting was to some extent restricted to “traditional border communities” (NL-BE, AT-IT-SI)

- The level of eID use in eGovernment is still not high in many MS; the lack of familiarity with the underlying mechanisms slow the diffusion of STROK-enabled services

Opportunities

- Exploiting the experience of STORK 2.0 to better meet the needs of businesses and to anticipate many interoperability issues that will face cross-border eID in the near future.
- STORK 2.0 participation will facilitate participation in current development initiatives like in e-SENS or the DIGIT/DG TAXUD project and in the CEF/Horizon 2020 developments
- Opportunities for near-future collaboration with non-STORK MS like the NO-SE, AT-DK, DE-NL showcase deployments in e-SENS
- STORK 2.0 experience will accelerate the integration with national eIDAS infrastructure and this successful pilot can be used by the EC and by MS to convince service providers that a mature approach has been found

Threats

- MS and end-user focus may shrink to eIDAS core functions and away from STORK 2.0 added value like mandates data model and powers attributes and direct procedural integration with the B-IDPs (eIDAS is limited to a "document-based presentation of credentials for identification of natural and legal persons without explicit machine-processable mandate information to properly link natural person representatives to represented entities)
- Limited expert resources for the interim maintenance of STORK in e-SENS might prove to be insufficient; in particular, the focus on STORK maintenance to security patches might be insufficient as other maintenance tasks could be needed
- MS planning may emphasize the eIDAS deadline of Sept. 2018 for mandatory recognition, thus less interest in investing to continue advanced STORK 2.0 services during the 2016-2018 gap
- AUB and integration of mandates in SPs turned out to be complex and more costly than anticipated; changes in common code through e-SENS maintenance may affect SPs which might lose interest if costs to keep up are excessive.

6.5 Short to mid- term sustainability including pilot continuation intentions by pilot partners

In 2015, the STORK 2.0 network became a reality. It has the potential to reach maturity in the years to come. Especially by connecting new service providers, IDP's, AP's and business registers to the network. Connection to the network is still voluntary. But by adopting the eIDAS regulation, under certain conditions, support for foreign eID's will be mandatory for public service providers in 2018.

Short term sustainability is granted by the intention of ten SP partners to keep the services running after the end of the pilot[5]. As explained in previous paragraphs, there are some preconditions: maintenance of the STORK 2.0 software after the lifetime of the project,

[5] All piloting partners except LU, who will withdraw the service for reasons of low usage. Maintenance by e-SENS and future convergence with eIDAS implementations will have impact on future decisions. We note that the B-IDPs all intend to continue offering their service, barring eIDAS compatibility issues.

compatibility with eIDAS node and integration of STORK functionality and attributes in future releases of the eIDAS node (CEF eID Building Block).

In the mid-term, sustainability is strongly based on support by the EC through DIGIT/CEF, which will provide financial and institutional backing to the integration of STORK and the current eIDAS node, but specific decisions are to be made in the context of CEF governance model.

It is easy to foresee a period of transition in the co-existence between STORK 2.0 PEPS/V-IDPs and eIDAS nodes in which the STORK infrastructure will evolve from a temporary substitute for the national node to a generalized IDP offering cross-border reach and integrated via a specific adapter into the network of eIDAS nodes. Such an evolution will require a temporary maintenance capacity for STORK 2.0 software as well as a carefully designed convergence of data models and system features, both functional and non-functional. This process will occur under the supervision of CEF eID Operational Management Board and should define the next generation of the CEF eID Building Block package. This converged and extended node will provide a strong and firm basis for SPs to expand cross-border service delivery.

The following is a first proposal for a roadmap of convergence.

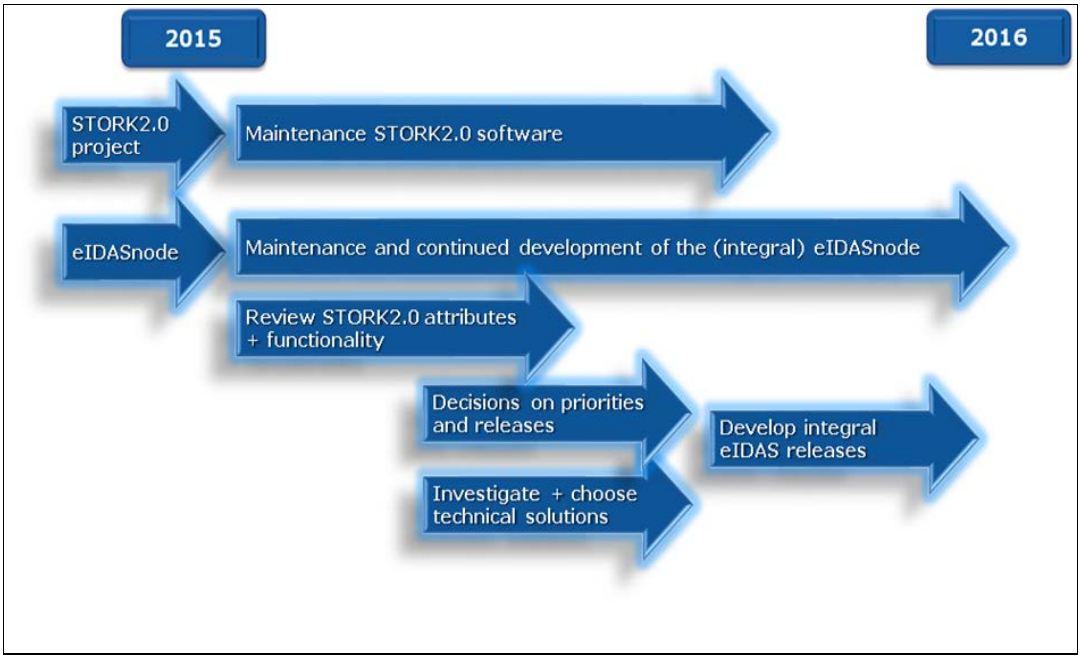

Figure 57: Roadmap for convergence between STORK 2.0 and eIDAS nodes

Without this solid basis confidence in the EU-wide infrastructure can suffer, because like all technological breakthroughs with political and organisational implications, developments in the field of cross-border authentication aren't future-proof.

To expand the cross-border services and increase the number of users dramatically it's important to look for appealing new public services for businesses, services which affect more businesses more frequently such as those involved in the migrant labour market besides the mobility of services covered by PSCs. In general, usage of services that are currently little used will not suddenly increase because of the facilitated access with national eID token to authenticate. Such enabling features are useful and necessary, but are not in themselves sufficient to stimulate wide-scale change in service usage or process configuration.

6.6 Long term adoption agenda and sustainability opportunities

STORK 2.0 project was initiated with the aim, among others, of developing an operational framework and infrastructure encompassing eID for secure electronic authentication of legal persons, including facilities for the management of representation powers and mandates.

In that sense, the project has achieved significant results, evolving STORK specifications to include attributes for legal persons, their powers to represent companies, mandate SAML tokens to capture more complete information about these powers, and adapting the SW building blocks to allow cross-border transfer of this kind of information. The feasibility of the developed solution has been verified by means of the STORK 2.0 pilots, in which use cases that require cross-border access to information about representation capabilities have been successfully tested.

However, the project has also found important barriers that currently hinder the adoption of an EU wide solution for cross-border transfer of representation information, being one of the most relevant the lack of a common semantic framework. Representation is complex and the national solutions are often too much focused on country specific details. Therefore, although there are some similarities among countries, there is not a shared European taxonomy about representation powers and mandates, preventing powers information and mandates originated from one country from being directly machine processable in other country. The STORK 2.0 solutions suffer from additional simplifications in terms of the representation of chains of mandates or joint mandates, the validation of which present particular needs expressing themselves in several different subcases.

Additionally, the need for service providers of having powers/mandates information together with the data regarding the represented and representing persons, in order to properly assess the scope of the transactions that the representing person is allowed to perform on behalf of the represented one, has been steadily highlighted in the discussions of the eIDAS Expert Group. As the current specifications for the eIDAS node are limited in the way service, service steps and mandate information can be handled, this needs to be carried forward by MS themselves e.g. through the actions taken by the STORK MS Council to propose further work on mandates to eIDAS and by STORK MS in e-SENS to develop STORK-eIDAS adaptors that allow maintaining the existing mandate structure with the domain-specific attribute mechanism in the upcoming eIDAS node through CEF.

Taking into account the fact that the goal of the European Commission ISA programme is the promotion of the interoperability of electronic public services, and that it includes specific actions on the topic of semantic interoperability like the ISA core vocabularies [31], STORK 2.0 MS Council believes that there is an opportunity for continuing the work done in STORK 2.0 regarding representation powers/mandates under the scope of the ISA programme and, in that way, to keep progressing towards the single digital market and a European-wide semantic harmonisation. In that sense, an evolution of the ISA Core Vocabularies to extend the Core Person and Core Business vocabularies with a common taxonomy for representation powers/mandates linked to legal entities may be one of the potential initiatives to be taken over by the European Commission.

7 Pilots dissemination and marketing phased strategy

7.1 Dissemination and marketing pilot strategy

Marketing and dissemination strategy in the final period of the project was largely a continuation of the activities of the past periods. Actions were aimed at two main target groups: potential pilot end-users and stakeholders involved in the evaluation of STORK 2.0 by potential future adopters, acting mainly as SPs but also as B-IDPs, the business identity and mandate credentials providers.

Known end-users have mainly been informed about STORK 2.0 piloting through material published at the SP sites themselves, but they have also been contacted directly by email (in AT, NL, IT) or at industry events or specific meetings with trade organisations or other Public Administrations such as those running the national PSCs created by the EC Services Directive (in AT, BE, EE, IS, GR, LT, LU, NL, SI, SK). Individual SPs also publicised pilot activities and services through brochures, house newsletters, websites and social media.

Of course, general project dissemination has also helped lead businesspersons to the pilot services, both through presence at international events and also continuously from the pilot micro-site ([13]) which presents the home pages of all the piloting SPs with information about the pilot service, the target market and any prerequisites needed to access the service.

Figure 58: The STORK 2.0 eGov4Business pilot micro-site

7.2 Dissemination activities carried out and their resulting impacts

This section briefly reports the dissemination activities carried out by partners in the final period of the project.

AT-ARGE:

- Presentation of STORK and STORK 2.0 to master students in an IT Security lecture at Graz University of Technology, 28 May 2015

GR-HMI:

- June-workshop in collaboration with Ministry of Commerce-ΕΣΗΔΗΣ for public servants (20 persons) both ministries, main point the use of STORK authentication in the platform of Promitheus and the possibilities it offers. An overview of STORK2.0 and other STORK2.0 pilots was given.
- September online series of online lessons-Seminar in collaboration with Stork 2.0 partners University of Aegean. The course's participants (30 persons) was undergraduate and graduate students, graduates Polytechnic departments, IT departments, and departments with ICT management and Public Administration, and Greek public servants involved in public administration and local government using ICT and Public Administration.
- Continuous support of STORK2.0 via social media channels and disseminating where an opportunity was found (e.g., in other LSPs, in national meetings and use cases). Generally, Stork2.0 –HMI partners act as "ambassadors" of disseminating STORK2.0
- Plans for sustainability when available , at this point there are two immediate opportunities:
    - An open workshop with Stork 2.0 partners University of Aegean, the workshop will focus on eIDAS and Stork2.0 and its connection to national level. Possible date in November.
    - There is the possibility of a presentation of STORK2.0 and pilot in eDemocracy conference (http://www.edemocracy2015.eu/) in December.

IS-SKRA:

- National IT Conference Reykjavík, presentation on cross-border authentication

IT-IC:

- Presentation to Unioncamere and the Cabinet Department of European Affairs

LT-IS/MOI:

- Seminar at the Vilnius Gediminas Technical University, 12/05/2015
- Joint workshop of MoI and Information Society, Vilnius 19/08/2015
- Meeting with representatives of Moldova delegation, Ministry of the Interior, LT Government Chancellery, Vilnius 10/09/2015

LU-TUDOR /CTIE:

- Presentation/representation of Stork's LU pilot via participation in e-SENS
- Discussion with IT companies, presentation of the project, link with Share-PSI.eu (brings together diverse stakeholders in the European public sector)

NL-MEAI:

- eIDnext conference: eIDAS: state of play, implementation (STORK)
- NCDO - Government-wide impact eIDAS and STORK

SI-MIPA:

- Workshop for public administration - Presentation of eIDAS regulation and Slovenia's involvement in STORK 2.0 project
- Chamber of Commerce and Industry of Slovenia - Presentation of Slovenian one stop shop for companies
- Presentation of the STORK 2.0 project at Researchers' night 2015, Ljubljana (booth and leaflet dissemination).
- SmartDoc 2014 - eIDAS and building blocks for e-authentication and trust services
- 4th Danube e-Region Conference – DeRC 2014: Cross-border e-Solutions & eServices Prototypes Development - STORK session (presentation of all pilots)
- Workshop with Croatian Public Administration - STORK presentation
- e-Governance initiatives, policies and practices in the European Union – presentation for the Indian delegation of e-Government in Slovenia

SK-MoF:

- Nomination of the Slovakian implementation of STORK 2.0 for the "Project of the Year 2015", to be awarded on October 1, 2015 at the IT Gala in Bratislava, Slovakia The expert commission compiled a wider nomination this year that comprised more than 200 personalities and companies operating in the information technology and telecommunications. On the basis of the questionnaires the jury compiled a closer vote, the nomination of three personalities, three companies of three products and three projects (one of them STORK 2.0).

8 Conclusions

The eGov4Business Pilot closes the project with some truly important results. In spite of considerable challenges encountered during all phases, from analysis and design to final piloting and sustainability planning, all the main objectives of piloting were achieved:

- Ten existing online eGovernment Services for Businesses such as official sectorial registers, national business registers, one-stop shop Business Services Portal and Points of Single Contact (PSCs) were successfully integrated with the STORK 2.0 infrastructure to take advantage of cross-border authentication services. These services allowed businesspersons and company representatives to register at and logon to portals in other EU MS based on the exchange of personal and company identity attributes and representation credentials obtained in their home countries through the STORK 2.0 interoperability network.
- These services were made possible thanks to the integration in the national STORK 2.0 infrastructures of Business Registers, Mercantile Registers and other Mandate Attribute Providers who furnished the credentials allowing validation of company representation powers. The validation of these powers across borders, in real-time and automatically (based on the machine processable SAML format) is an extraordinary result, albeit a first step needing further development, in Business Register interoperability which required specific harmonisation of numerous technical, organisational, semantic and legal issues.
- The demonstrated benefits to all stakeholders - end-users, eGovernment Service Providers (SPs) and eID infrastructure providers - was sufficient to
    - Engage in fruitful discussions with important European-level initiatives like e-SENS and get commitment from organisations in charge of national deployments of the eID building block to guarantee the short-term continuation of STORK 2.0 services and to provide for the medium-term compatibility and convergence with the CEF eID building blocks and the eIDAS nodes,
    - Convince new service providers from different Public Administrations to integrate into the network in order to take advantage of the cross-border authentication interoperability,
    - Convince current partners to maintain their services and even to extend the STORK 2.0 authentication to new eGovernment services published at their portals,
    - Gather generally positive feedback from end-users, with important indications of how services should improve the overall end-user experience and at the same time increase the perception of security, trust and respect of data privacy.

The unexpected complexities of the new STORK 2.0 procedures for “Authentication on behalf of a company (or legal person)”, AUB, were the source of several problems and delays, but these issues also provided an excellent opportunity for evaluating and contributing lessons learned to the future evolution of the eIDAS implementation, in particular, to the Connecting Europe Facility.

Pilot USE

A primary goal of the pilot was getting as many different services operational in as many different MS as possible in order to maximize interoperability and spread achieved benefits to as many stakeholders as possible. Ten of the thirteen piloting partners in as many MS did succeed in releasing their services live, in production environments, for real piloting of basic

authentication services. Six of these partners also implemented the significantly more complex AUB involving the gathering of company eID and representation credentials from Attribute Providers across national borders.

The effective use of the integrated services was limited in part due to the perennially low level of activity in cross-border eGovernment for businesses, and also due to the delays in deployment of national infrastructures and Pilot services.

Pilot VALUE

The pilot demonstrated significant benefits and value to foreign end-users of existing eGovernment service portals - achieving an unprecedented degree of interoperability with national and international eID infrastructures and with Attribute Providers across borders.

The pilot contributed to defining, implementing and validating the essential aspects of the representation and processing of company powers for acting on behalf of a legal person, comprising technical activities regarding the definition of mandate structure, procedures for corresponding SAML token handling and validation and actions regarding organizational, semantic and legal issues related to cross-border interoperability.

The eGov4Business pilot services produced verified benefits (as indicated by SPs) in rationalizing infrastructure costs, opening EU markets, lowering barriers to cross-border business development, reducing procedure time for employees and businesses and improving other aspects of Administrative burden.

The pilot contributed to improving the visibility of STORK 2.0 from PSC and other national eGovernment services and from national actors like Business Registers and their European organisations like ECRF (European Commerce Register Forum).

Pilot SPs overwhelmingly assessed as positive the benefits of STORK 2.0 with respect to costs, and as a result have produced useful indicators of the costs of implementing, integrating, supporting and maintaining STORK 2.0 services in a range of public administration situations. The variability of these costs is high, due to the variety of services and service combinations that partners piloted, and also due to the prior “STORK 2.0-readiness” of the SP systems, that is, the degree to which the systems were ready – from technical and procedural points of view - to handle foreign eID information and to connect to an external authentication service.

Pilot LESSONS LEARNED

Given the pioneering nature of STORK 2.0 – unexpected or underestimated by all parties - Project learning was continuous and involved rich exchanges between technical, legal, market-oriented and piloting teams.

Important lessons learned deal with

- Organisation, maintenance, development and support of software assets
- Actions to improve the quality of the authentication services by strengthening and extending the interoperability of mandate information and company credentials, in general
- Measures for improving trust in the STORK 2.0 network; measures to develop a more mature and sustainable cross border authentication and powers validation service, especially by defining standards for quality, performance and governance.

Pilot ADOPTION & SUSTAINABILITY

The major force for sustainability of the services lies in the willingness of Pilot Partners to maintain and further develop their STORK 2.0-enabled services. The project results are of convincing and lasting value and have broken ground for the implementation of eIDAS. This has led most partners to actively engage in lobbying actions at both national and international levels to re-use, protect and extend STORK 2.0 results. These actions have so far succeeded in creating a roadmap for the short-term maintenance of services in collaboration with the e-SENS LSP, and providing confidence in the continued development of the eID building block in the context of CEF with take-up of some of the more advanced features of the STORK 2.0 solutions and further development of other innovations, like the representation of mandates, for example, in ISA^2.

Thus, the legacy of STORK 2.0 is well-prepared to find its place in the next generation of Digital Agenda actions and infrastructures.

9 References

[1] D5.3.1 Technical & Business Objectives and Specifications

[2] D5.3.2 eGov4Business GoLive Planning

[3] D5.3.3 eGov4Business Pilot Running Phase Planning

[4] D5.3.4 eGov4Business Pilot Progress Report

[5] D.3.1 Legal Needs Analysis Report

[6] D3.2 QAA Status Report

[7] D3.3 Mandate/Attribute Management Report

[8] D3.4 Consolidated Trust Report

[9] D3.6 Consolidated Legal Entities Report

[10] D4.9 Final version of Functional Design

[11] D4.11 Final version of Technical Specifications for the cross-border interface

[12] D5.2.5 eBanking Pilot Final Report

[13] STORK 2.0 pilots Public services for Business pilot "micro site", https://www.eid-stork2.eu/pilots/public_services/index.php/en/

[14] Study on Analysis of the Needs for Cross-Border Services and Assessment of the Organisational, Legal, Technical and Semantic Barriers. Tinholt et al. 2012

[15] eIDAS Regulation, Regulation (EU) N°910/2014, see ec.europa.eu/digital-agenda/en/trust-services-and-eid

[16] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015, see ec.europa.eu/digital-agenda/en/printpdf/50813

[17] EC Services Directive, 2006/123, see ec.europa.eu/growth/single-market/services/services-directive/index_en.htm

[18] EC Directive on Business Register Interconnection, 2012/17/EU

[19] The feasibility and scenarios for the long-term sustainability of the Large Scale Pilots, including 'ex-ante' evaluation, Deloitte for EC DG/CNCT

[20] CEF, Connecting Europe Facility, see ec.europa.eu/digital-agenda/en/connecting-europe-facility

[21] CEF Digital Service Infrastructures, see https://ec.europa.eu/digital-agenda/en/connecting-europe-facility#digital-service-infrastructures-dsis

[22] ISA, ec.europa.eu/isa/actions/01-trusted-information-exchange/1-5action_en.htm

[23] ISA^2 Programme and Proposal, see ec.europa.eu/isa/isa2/index_en.htm and ec.europa.eu/isa/documents/isa_2_proposal_en.pdf

[24] H2020 Horizon 2020, ec.europa.eu/programmes/horizon2020/

[25] e-SENS project website, www.e-SENS.eu

[26] e-SENS eID Building Block, see www.e-SENS.eu/technical-solutions/e-SENS-technical-solutions/e-identity/

[27] e-SENS Business Lifecycle Pilot, see www.e-SENS.eu/real-life-piloting/business-life-cycle/

[28] e-SENS eAgriculture Pilot, see www.e-SENS.eu/real-life-piloting/eagriculture/

[29] ISA Action on STORK sustainability, see ec.europa.eu/isa/actions/01-trusted-information-exchange/1-5action_en.htm

[30] ECAS-STORK Integration, see ec.europa.eu/isa/actions/01-trusted-information-exchange/1-4action_en.htm and https://www.eid-stork.eu/pilots/pilot6.htm

[31] ISA Core Vocabularies, see ec.europa.eu/isa/actions/01-trusted-information-exchange/1-1action_en.htm and https://joinup.ec.europa.eu/asset/core_vocabularies/description

[32] eJustice portal, e-justice.europa.eu

[33] ECRF - www.ecrforum.org

[34] SPOCS factsheet, www.eu-spocs.eu/pilots/images/stories/factsheet.pdf

[35] “Time is money” from “Advice to a Young Tradesman” , Benjamin Franklin, 1746

[36] Joinup - https://joinup.ec.europa.eu/asset/core_vocabularies

[37] W3C Schema Community Group - http://www.schema.org

APPENDIX I Summary metrics

The tables in this Appendix represent the completion of the measurement phase of the Benefits Logic approach to Pilot evaluation. The results will be used by the Project Evaluation Team to assess achievements and will also act as input to the Gap analysis which will further examine the causes for missed results.

Appendix I.1: Functionality metrics

Metric ref. num. – Description; Main UVL-categories	***Metric Source (SP/ AP/ Feedback Form/ Focus Group/ Logs/ Other)***	***Success criterion***	***Result (Achieved/ Partially Achieved /Not Achieved/ Not Known) (Add percentage when applicable)***
F.1 – Implementation of Use Cases. **Value** (+ Use)	**SP** Execution of the test cases and analysis of the results.	**Qualitative based** Common functional use cases (see Chapter2 of D5.3.1[1]) properly implemented in over 66% of MS.	**Partially Achieved (46% of SP use cases implemented)** Measured Result 46% = Average (AU implemented in 77% of SPs; AUB implemented in 62% of MS and 46% of SPs; CFUC#2 implemented but not released because of dependence on unpiloted PV functionality, 0%)
F.2 – Implementation of Use Case variations. **Value**	**SP** Execution of the test cases and analysis of the results.	**Qualitative based** Variations 3, 4 and 5 of main CFUC#1[6] each successfully implemented in at least one MS.	**Partially Achieved (50%)** var.3 implemented by AT and LT; var.4 implemented and tested, but not deployed or piloted; var. 5 not implemented
F.3 - Successful authentication procedures, individual and "on behalf of" a company or a person **Use** (+ Learn)	**End-user** End-user feedback forms (Q4, Q5).	**Quantitative based** Over 66% error-free authentications	**Achieved** Basic authentication achieved an 81,6% success rate; Authentication "on behalf of" achieved 82,4% success
F.4 – Perceived usefulness (by end-user). **Use** (+ Value)	**End-user** End-user feedback forms (Q10, Q12).	**Qualitative based** At least 80% non-negative replies.	**Achieved (Substantially – 77% non-negative replies)** 77% non-negative = AVG(80% respondents for "STORK eID makes good sense"; 26% for "it is useful")

Table 9 : eGov4Business Functionality metrics

[6] These are the variations involving simplified user interface, persistent logon (SSO) and 3-MS scenario.

Appendix I.2: Interoperability metrics

Metric ref. num. – Description; Main UVL-categories	***Metric Source (SP/ AP/ Feedback Form/ Focus Group/ Logs/ Other)***	***Success criterion***	***Result (Achieved/ Partially Achieved /Not Achieved/ Not Known) (Add percentage when applicable)***
I.1 – Verification of cross-border services. **Value** (+ Use)	**SP** Evaluation of SP test reporting.	**Quantitative based** Over 80% coverage of cross-border testing (Table 28 in D5.3.2 [2]).	**Achieved** 32 different cross-border connections were successfully tested with respect to the 28 that were planned
I.2 – QAA mix – successful authentication with different combinations of QAA values. **Value** (+ Use)	**SP** Evaluation of SP test reporting.	**Quantitative based** Successful use of credentials with at least two different QAA levels.	**Achieved** Three levels of QAA (1, 3 , 4) successfully implemented
I.3 – AQAA mix – – successful authentication with different combinations of AQAA values. **Value** (+ Use)	**SP** Evaluation of SP test reporting.	**Quantitative based** Successful powers verification with at least two different AQAA levels.	**Achieved** Three levels of AQAA (1, 3 , 4) successfully implemented
I.4 – Various mandate types used (semantic/legal perspective). **Value** (+ Use)	**SP** Evaluation of SP test reporting.	**Quantitative based** At least two different (non-null) powers types used for authentication.	**Achieved** Two TypeOfPowers (=0, 9) successfully pilot tested
I.5 – Absence of Legal and semantic obstacles. **Learn** (+ Use, Value)	**End-user & SP** End-user feedback forms (Q5, Q24) and SP questionnaire (Q12).	**Qualitative based** No outstanding issues reported.	**Partially Achieved** When problems arose temporary or partial solutions were found to permit piloting, and these issues lead to several lessons learned (see Section 5.3), but permanent solutions are still lacking for several outstanding issues[7]

[7] General data privacy issues, character set issues, legal value of e-mandates and powers taxonomy, required attribute sets not always available, status of back-office/offline PV procedure with respect to privacy data privacy

Table 10 : eGov4Business Interoperability metrics

Appendix I.3: Security metrics

Metric ref. num. – Description; Main UVL-categories	***Metric Source (SP/ AP/ Feedback Form/ Focus Group/ Logs/ Other)***	***Success criterion***	***Result (Achieved/ Partially Achieved /Not Achieved/ Not Known) (Add percentage when applicable)***
S.1 – Technical verification of SP security aspects. **Value**	**SP** SP Security checklist.	-	Not measured The SP security checklist was dropped because SP security is not the issue.
S.2 – User perception of security. **Use** (+ Value, Learn)	**End-user** End-user feedback forms (Q10, Q16).	**Qualitative based** Over 66% positive responses.	**Achieved** 70% feel eID enabled service is secure 64% feel cross-border eID is secure
S.3 – SP rating of security of STORK 2.0 infrastructure **Value** (+ Use, Learn)	**SP** SP questionnaire (Q24)	**Qualitative based** Less than 20% negative rating by SPs	**Achieved** No negative rating received

Table 11 : eGov4Business Security metrics

Appendix I.4: Maintainability metrics

Metric ref. num. – Description; Main UVL-categories	***Metric Source (SP/ AP/ Feedback Form/ Focus Group/ Logs/ Other)***	***Success criterion***	***Result (Achieved/ Partially Achieved /Not Achieved/ Not Known) (Add percentage when applicable)***
M.1 – Evaluation of code maintainability and quality of technical documentation **Learn** (+ Value)	**SP** SP questionnaire (Q40)	**Qualitative based** Over 66% positive evaluation.	**Achieved** 80% positive evaluation
M.2 – Evaluate the cost of maintaining the involved services and systems **Value** (+ Learn)	**SP** SP questionnaire (Q20, Q21)	**Qualitative based** Estimates received from over 66% of piloting SPs indicate benefits justify costs.	**Achieved** 80% positive overall costs/benefits evaluations
M.3 – Evaluate the cost of replacing the system. **Learn** (+ Value)	**SP** SP questionnaire (Q41)	**Qualitative based** Compare costs of maintaining STORK 2.0 with costs to replace with new system for eID interoperability	**Achieved** 80% of SPs say maintaining STORK 2.0 costs less than replacing it
M.4 – Smooth migration to new SW versions of STORK 2.0 with testing of new functionalities and regression testing of old **Value** (+ Learn)	**SP** SP questionnaire (Q26, Q28)	**Quantitative based** Less than one person-month of effort to migrate.	**Not Achieved** No SP declared < 1 p-m effort: 50% 1-2 pm and 50%>2 pm

Table 12: eGov4Business Maintainability metrics

Appendix I.5: Scalability/Flexibility

Metric ref. num. – Description; Main UVL-categories	***Metric Source (SP/ AP/ Feedback Form/ Focus Group/ Logs/ Other)***	***Success criterion***	***Result (Achieved/ Partially Achieved /Not Achieved/ Not Known) (Add percentage when applicable)***
SF.1 – Increase in number of users by the end of the project. **Use** (+ Value)	**SP** Quantitative metrics that will come from PEPS logs	**Quantitative based** 25% increase with respect to 1-2 months after Go Live.	**Achieved** Looking at user transactions attempts over the whole piloting period on a monthly basis this has been achieved. We note that user identity is not stored in the PEPS logs.
SF.2 – Increase in number of available SP services from Go Live. **Value**	**SP** Periodic updating of service metrics on pilot wiki.	**Quantitative based** 25% increase with respect to Go Live.	**Achieved** As seen in chapter 2, an increasing number of services has been put in production and the result is achieved.
SF.3 – Ease of integration for SPs. **Use** (+ Value)	**SP** SP Questionnaire (Q27)	**Quantitative based** Over 66% SPs integrate without difficulty.	**Achieved (Substantially – 60% non-negative replies)** 60% of SPs encountered no more difficulty than expected
SF.4 – Effort to integrate the SP with PEPS **Value**	**SP** SP Questionnaire (Q42)	**Quantitative based** Over 66% of SPs spent < 2 p-m	**Achieved (Substantially – 60% of SPs)** 60% of SPs spent < 2 p-m

Table 13: eGov4Business Scalability/Flexibility metrics

Appendix I.6: Reliability/Maturity

Metric ref. num. – Description; Main UVL-categories	***Metric Source (SP/ AP/ Feedback Form/ Focus Group/ Logs/ Other)***	***Success criterion***	***Result (Achieved/ Partially Achieved /Not Achieved/ Not Known) (Add percentage when applicable)***
RM.1 – Availability of STORK 2.0 common interoperability layer. **Use** (+ Value)	**SP, B-IDP** Uptime reporting from internal monitoring tool	**Quantitative based** Over 85% for 6 months continuously.	**Achieved** Average uptime > 95%
RM.2 – Availability of STORK 2.0 National interoperability layer, **Use** (+ Value)	**SP, B-IDP** Uptime reporting from internal monitoring tool	**Quantitative based** Over 85% for 6 months continuously. [8]	**Achieved** Average uptime > 95%
RM.3 – Availability of STORK-enabled SP pilot services. **Use**	**SP** Uptime reporting from SPs (Q39)	**Quantitative based** Over 85% for 6 months continuously. [9]	**Achieved** Average uptime 94%
RM.4 – Impact of STORK 2.0 integration on reliability and level of service. **Value** (+ Learn, Adopt)	**SP** SP Questionnaire (Q30)	**Qualitative based** No negative evaluation.	**Achieved** No negative evaluation reported.
RM.5 – Implementation level of support, incident and SLA related procedures. **Learn** (+ Value)	**SP** SP Questionnaire (Q33)	**Qualitative based** Over 66% positive evaluations by SPs.	**Achieved (Substantially – 60% positive evaluations)** 60% SPs give positive evaluations of MS support

Table 14: eGov4Business Reliability/ Maturity metrics

[8] Errors not related to STORK 2.0 services or integration do not count towards dis-service.

[9] Errors not related to STORK 2.0 services or integration do not count towards dis-service.

Appendix I.7: Portability

Metric ref. num. – Description; Main UVL-categories	***Metric Source (SP/ AP/ Feedback Form/ Focus Group/ Logs/ Other)***	***Success criterion***	***Result (Achieved/ Partially Achieved /Not Achieved/ Not Known) (Add percentage when applicable)***
P.1 – User verified portability on different browser platforms. **Use** (+ Value, Learn)	**End-user** End-user feedback forms (Q22)	**Quantitative based** More than three browsers	**Achieved** At least five were verified (Chrome, Firefox, MSExplorer, Opera, Safari)
P.2 – Platform portability from SP perspective –n. of diff. platforms (like Java/PHP) **Value** (+ Learn)	**SP** SP Questionnaire (Q35)	**Quantitative based** More than two platforms.	**Achieved** > three platforms

Table 15: eGov4Business Portability metrics

Appendix I.8: Business Value

Metric ref. num. – Description; Main UVL-categories	***Metric Source (SP/ AP/ Feedback Form/ Focus Group/ Logs/ Other)***	***Success criterion***	***Result (Achieved/ Partially Achieved /Not Achieved/ Not Known) (Add percentage when applicable)***
BV.01 – Documented benefits for end users. **Value** (+ Learn)	**End-user** End-user feedback forms (Q8, Q12)	**Qualitative based** Over 85% of users find benefits from STORK 2.0 eID	**Partially Achieved (52% positive replies)** 52% agree that STORK 2.0 provides benefits
BV.02 – Documented cost reductions for end users. **Value**	**End-user** End-user feedback forms (Q8)	**Quantitative based** More than 10 positive cases.	**Achieved** 9 feedback forms name cost savings and 43 name time savings as main benefits
BV.03 – Documented simplification of administrative procedures for end users. **Value**	**End-user** End-user feedback forms (Q8)	**Quantitative based** More than 10 positive cases.	**Achieved** 28 feedback form responses list simplification of procedures as main STORK 2.0 benefit
BV.04 – Concrete benefits for Service Providers. **Value** (+ Learn)	**SP** SP Questionnaire. (Q5-Q11)	**Quantitative based** At least one benefit cited by 90% of SPs; three benefits cited by 60%	**Achieved** Two benefits for 90-100% of SPs; three others for 70% [10]
BV.05 – Documentable cost reductions for SPs. **Value**	**SP** SP Questionnaire. (Q11)	**Qualitative based** Over 66% favourable estimates received from piloting SPs.	**Achieved (Substantially – 60% favourable estimates)** Six out of ten SPs cite cost reductions.
BV.06 – Average estimated reduction of the length of time. **Value**	**SP** SP Questionnaire. (Q10)	**Qualitative based** A significant savings of time SPs and end-users.	**Achieved** 70% of SPs declare savings in SP time; 90% of SPs declare savings in length of end-user time;

[10] 100% positive impact on improved EC compliance, 90% on reduced service time; 70% quality improved, expanded market, reduced admin costs

Metric ref. num. – Description; Main UVL-categories	***Metric Source (SP/ AP/ Feedback Form/ Focus Group/ Logs/ Other)***	***Success criterion***	***Result (Achieved/ Partially Achieved /Not Achieved/ Not Known) (Add percentage when applicable)***
BV.07 – Improvements in (perceived) quality of service. **Value**	**End-user & SP** End-user feedback forms (Q6, Q9) and SP Questionnaire. (Q7)	**Qualitative based** Over 66% favourable estimates received from users and piloting SPs.	**Achieved** 68% = AVG (80% of users rate the experience as adequate; 53% have better opinion of SP; 70% of SPs rate service quality improved)
BV.08 – STORK 2.0 contribution to EC policy aspects (Serv. Dir., eIDAS) **Value**	**SP** SP Questionnaire (Q8)	**Qualitative based** Over 66% positive replies.	**Achieved** STORK 2.0 improved EC compliance: 100% of SPs
BV.09 – Cost/benefits analysis of integration of STORK 2.0 services in existing eGov. Platform. **Value** (+ Learn)	**SP** SP Questionnaire. (Q21)	**Qualitative based** Over 66% favourable estimates from piloting SPs.	**Achieved** 80% positive cost/benefit value
BV.10 – Benefits for MS interoperability layer, IDP/V-IDP, B-IDP (Business Register). **Value** (+ Learn)	**SP, B-IDP** Periodic evaluation.	**Qualitative based** Over 66% positive developments (B-IDP integration) reported from piloting MS.	**Achieved (Substantially – 62% favourable replies)** 62% B-IDPs integrated in MS infrastructure for eGov4Biz pilot (see Section 2.2.2)
BV.11 – Increase in number of users by the end of the project. **Use** (+ Value)	**SP** SP Questionnaire. (Q22)	**Qualitative based** Over 66% positive estimates from piloting SPs.	**Partially Achieved (50% positive replies)** 1 SP reported significant growth in use of Pilot service; 4 SPs reported some growth
BV.12 – Successful cross-border eGov. Service transactions. [11] **Use** (+ Value, Learn)	**PEPS** Transaction logs	**Quantitative based** More than 500 successful transactions	**Achieved** Over 1000 successful transactions

[11] See also metrics F.3 and UU.3 for the end-user point of view of "successful authentications" and "successful access to SP"

Metric ref. num. – Description; Main UVL-categories	***Metric Source (SP/ AP/ Feedback Form/ Focus Group/ Logs/ Other)***	***Success criterion***	***Result (Achieved/ Partially Achieved /Not Achieved/ Not Known) (Add percentage when applicable)***
BV.13 – Services enabled by STORK 2.0 that would otherwise not have been available online across borders. **Learn** (+ Value)	**SP** SP Questionnaire (Q9)	**Quantitative based** Over 80% of SPs.	**Achieved (Substantially – 70% positive replies)** 70% of SPs indicate eGov services opened up to new EU markets
BV.14 – Opportunities for integrating additional services and portals. **Value** (+ Learn)	**SP** MS representatives feedback via SP Questionnaire (Q23)	**Qualitative based** Opportunities found in over 80% of MS.	**Achieved** 80% of SPs are positive about the extension of STORK 2.0 to nearby services
BV.15 – Willingness to pay for the new service. **Value** (+ Learn)	**SP** SP Questionnaire (Q14)	**Qualitative based** Over 66% positive attitude among SPs.	**Not Achieved** 70% undecided, 30% negative – SPs influenced by announced eIDAS policy which says cross-border eID should be free.
BV.16 – N. of SPs intending to continue pilot service after the project. **Value** (+ Learn)	**SP** SP Questionnaire (Q13)	**Qualitative based** Over 66% positive intentions	**Achieved** 50% definite positive, 30% probable positive,
BV.17 – Costs of adapting SP service to cross-border, STORK 2.0 users. **Value** (+ Learn)	**SP** SP Questionnaire (Q17-19, Q43)	**Quantitative based** Over 66% of SPs evaluate adaptation costs at < 33% of the cost of developing a new eID interop. System	**Achieved** 70% of SPs agree that the cost of adapting another service to STORK 2.0 would be less than one-third the cost of developing a new solution.
BV.18 – Cost of support, training and documentation. **Value** (+ Learn)	**SP** SP Questionnaire (Q17-19, Q44)	**Qualitative based** Over 66% SPs evaluate costs as not out of line with SP practices.	**Achieved** 80% of SPs feel that support costs for STORK 2.0 are not out of line with current SP practice

Table 16: eGov4Business Business Value metrics

Appendix I.9: Usability/Understandability

Metric ref. num. – Description; Main UVL-categories	***Metric Source (SP/ AP/ Feedback Form/ Focus Group/ Logs/ Other)***	***Success criterion***	***Result (Achieved/ Partially Achieved /Not Achieved/ Not Known) (Add percentage when applicable)***
UU.1 – End-users' perception of usability. **Use** (+ Value)	**End-user** correlated results of the End-user feedback forms (Q 6, Q7)	**Qualitative based** Over 66% positive rating by end-users	**Partially Achieved (56% positive replies)** 56% positive rating overall with • 63% positive for experienced users; • 45% positive for naïve users;
UU.2 – Microsite and feedback form available in MS languages. **Use** (+ Value)	**SP, Pilot Leader** Assessment of SPs by pilot leader.	**Quantitative based** 100% coverage of Piloting MS.	**Achieved** 100% of Partner MS
UU.3 – Successful access to SP services. **Use** (+ Value)	**End-user** End-user feedback forms (Q5)	**Qualitative based** Over 66% positive replies.	**Achieved** 76% = 62% positive replies +14% of negative replies due to users who forgot pin or came from non-participating MS

Table 17: eGov4Business Usability/ Understandability metrics

Appendix I.10: Data Protection & Privacy

Metric ref. num. – Description; Main UVL-categories	***Metric Source (SP/ AP/ Feedback Form/ Focus Group/ Logs/ Other)***	***Success criterion***	***Result (Achieved/Partially Achieved/Not Achieved/Not Known) (with percentage when applicable)***
DP.1 – Users perception of privacy protection (safer, smarter, more trustworthy). **Use** (+ Value, Learn)	**End-user** End-user feedback forms (Q10).	**Qualitative based** Over 66% positive replies.	**Achieved (Substantially – 59% positive replies)** 59% = AVG (58% positive for respects privacy; 61% positive for trustworthy; 58% positive for safe)
DP.2 – Users perception of being in control over the handling of their own personal data. **Use** (+ Value)	**End-user** End-user feedback forms (Q14, Q15).	**Qualitative based** Over 66% positive replies.	**Achieved** 77% fully informed about data 67% in control of personal data
DP.3 – Privacy policy present on SP site. **Use**	**SP** SP Questionnaire. (Q34)	**Quantitative based** 100% presence on SP sites.	**Partially Achieved (80% of SPs)** Eight out of ten GoLive SPs publish Data Privacy statements.

Table 18: eGov4Business Data Protection & Privacy metrics

Appendix I.11: Adoption

Metric ref. num. – Description; Main UVL-categories	***Metric Source (SP/ AP/ Feedback Form/ Focus Group/ Logs/ Other)***	***Success criterion***	***Result (Achieved/ Partially Achieved /Not Achieved/ Not Known) (Add percentage when applicable)***
A.1 – Impact on end-users; expectations for benefits. **Value** (Adopt)	**End-user & Focus Groups** Overall analysis of Focus group feedback and end-user Feedback forms.(Q17)	**Qualitative based** Over 66% positive overall evaluation by end-users	**Achieved (Substantially – 65% positive replies)** 65% end-users would recommend STORK-enabled services to other businesspersons
A.2 – Impact on SPs; expectations for benefits. **Learn** (+ Value, Adopt)	**SP** Overall analysis of SP questionnaire.	**Qualitative based** Over 66% positive overall evaluation by SPs.	**Achieved** Deduced from average of metrics BV.04, BV.05, BV.06, BV.09, BV.10
A.3 – Sustainability. **Value** (Adopt)	**SP** SP (MS) assessment.	**Qualitative based** Over 66% positive overal evaluation of costs/benefits	**Achieved** Deduced from average of metrics BV.08, BV.09, BV.14, BV.16, BV.17, BV.18

Table 19: eGov4Business Adoption metrics

APPENDIX II Lessons learned table

Learned		
Index	***Title***	***Section***
1.1	Lesson 1.1 Integration and handling of AQAA by SPs and APs (B-IDPs)	5.3.1
1.2	Lesson 1.2 Propagation of changes in configurations	5.3.1
1.3	Lesson 1.3 Aligning and improving software development, release and configuration practices; exchange of digital certificates	5.3.1
1.4	On the other hand, the infrastructure providers should strive to facilitate further adoption of industry practices in software development and maintenance with the purpose of increasing stability, transparency and overall quality of the processes. A very specific instance of this regarded the exchange of server digital certificates between trusted nodes of the network. The certificate exchanges, while the Version Control functionality was not yet in place, were often communicated among partners through the STORK 2.0 mailing lists. This kind of communication is not really the best solution for real world production quality that requires high availability of the services. Lesson 1.4 Support and documentation channels for SPs	5.3.1
1.5	Lesson 1.5 Monitoring infrastructure	5.3.1
1.6	Lesson 1.6 Management of test credentials	5.3.1
2.1	Lesson 2.1 Reusing existing definitions, views and vocabularies in mandates	5.3.2
2.2	Lesson 2.2 Addressing semantic and legal gaps between descriptions	5.3.2
2.3	Lesson 2.3 Mapping missing or incomplete descriptions	5.3.2
2.4	Lesson 2.4 AQAA syntax	5.3.2
3.1	Lesson 3.1 Issues related to QAA and AQAA; multiple identifiers and identity reconciliation	5.3.3
3.2	*Lesson 3.2* Translation of mandates, use of standard values and legal value of STORK 2.0 SAML tokens.	5.3.3
3.3	*Lesson 3.3* Issues related to transliteration - Non-Latin characters	5.3.3
3.4	*Lesson 3.4* Confirmed minimum sets of attributes	5.3.3
3.5	Lesson 3.5 Powers validation functionality and prior user consent	5.3.3
5.1	Lesson 5.1 Engagement of correct stakeholders is everything	5.3.5

5.2	Lesson 5.2 Time saving and simplification of procedures are considered to be the greatest benefits	5.3.5
5.3	Lesson 5.3 Long term solution ensuring circle of trust is needed	5.3.5
5.4	Lesson 5.4 Need for common service level agreement rules	5.3.5
5.5	Lesson 5.5 Definition of appropriate governance model for STORK 2.0	5.3.5
5.6	Lesson 5.6 eID is an enabler for cross-border eGovernment, but usage patterns are slow to change.	5.3.5
6.1	Lesson 6.1 Cross-border services made possible through STORK2.0 integration	5.4.1
6.2	Lesson 6.2 Added STORK-enabled functionalities improve SP services	5.4.1
6.3	Lesson 6.3 Time for SP migration to STORK2.0 needs to be reduced and the operation simplified if possible	5.4.1
6.4	Lesson 6.4 Fees and models for payment	5.4.1
7.1	Lesson 7.1 Need for a homogeneous GUI	5.4.2
7.2	Lesson 7.2 Further efforts needed to standardise the STORK 2.0 Mandate	5.4.2
7.3	Lesson 7.3 Greater use of standards in developments	5.4.2
7.4	Lesson 7.4 Further developments of the STORK 2.0 QAA/AQAA model vs. convergence with eIDAS model	5.4.2
8.1	Lesson 8.1 the STORK 2.0 “circle of trust” and AQAA mechanism	5.4.3
8.2	Lesson 8.2 Reliability trust and security of STORK2.0 for mission-critical services	5.4.3

Table 20: All Lessons Learned

APPENDIX III Cost details

Costs for adapting and integrating eGov4Business services/portals to STORK 2.0 (in person-months).

Partner names are kept confidential.

Partner SP	P1	P2	P3	P4	P5	P6	P7	P8	Avg.
Design, requirements	0,5	0,8	1,0	3,0	4,3	12,0	9,7	12,3	**5,4**
Functional adaptation of service to interact with PEPS	0,0	2,0	2,5	3,0	8,6	3,0	8,6	10,9	**4,8**
Adaption of service GUI and support features	0,8	0,2	0,5	1,0	2,4	1,0	2,6	3,3	**1,5**
Integration of commercial eID software with enterprise	0,5	0,5	0,0	2,0	0,0	4,0	3,1	4,0	**1,8**
Testing	0,3	1,0	2,0	3,0	3,3	4,0	6,1	7,7	**3,4**
Management	0,5	0,0	0,0	1,0	2,2	10,0	6,1	7,8	**3,5**
Documentation	0,0	0,8	0,0	2,0	2,7	4,0	4,2	5,4	**2,4**
Language support, translation	0,0	0,3	0,0	0,7	0,0	2,0	1,3	1,7	**0,7**
Admin. or legal interoperability costs	0,0	0,5	0,0	3,0	0,7	3,0	3,2	4,1	**1,8**
Totals	**2,5**	**6,0**	**6,0**	**18,7**	**24,2**	**43,0**	**45,0**	**57,1**	**25,3**

Table 21: Capital costs - details

Additional one-time capital expenditures									
Partner SP	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**Average**
Acquisition of specific hardware	0,0	0,0	0,0	2,0	0,0	3,0	-	14,3	**2,8**
Hosting services	0,0	0,0	1,0	2,0	0,0	6,0	-	25,7	**5,0**
Additional technical training	0,0	0,0	0,0	1,0	0,0	1,0	-	5,7	**1,1**
Other capital expenditures	0,0	0,0	2,0	0,0	0,0	0,0	-	5,7	**1,1**
Additional training of support staff	0,0	0,0	0,0	0,5	0,0	0,5	-	-	**0,2**
Help pages development	0,0	0,1	0,0	0,5	0,1	0,5	-	-	**0,2**
Documentation writing	0,1	0,1	0,5	1,0	0,1	1,0	-	-	**0,5**
Support service adaptation	0,0	0,1	0,5	0,5	0,1	0,5	-	-	**0,3**
Increment in support inquiries.	0,0	0,0	0,0	1,0	-	1,0	-	-	**0,3**
User engagement and involvement	0,3	0,2	0,0	3,0	0,3	0,0	-	-	**0,6**
Marketing and dissemination	0,3	0,2	0,0	2,0	0,3	0,0	-	-	**0,5**
Maintenance and operation	0,1	0,2	0,0	5,0	-	9,0	-	-	**2,4**
Totals	**0,7**	**1,0**	**4,0**	**18,5**	**0,8**	**22,5**	**0,0**	**51,4**	**14,8**

Table 22: Additional one-time capital expenditures- details