COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

ICT Policy Support Programme (ICT PSP)

Towards pan-European recognition of electronic IDs (eIDs)

ICT PSP call identifier: ICT-PSP/2007/1
ICT PSP Theme/objective identifier: 1.2

Project acronym: STORK

Project full title: Secure Identity Across Borders Linked
Grant agreement no.: 224993

STORK Overview for new MS

Actual submission date : **14th November 2011**

Author(s) : **John Heppe, Tim Schneider, Herbert Leitold, Renato Portela**

Abstract:
This document presents an overview of STORK for new Member States which consider or have decided to connect to the STORK platform. Its objective is presenting a quick view of what STORK is and how it works, thus those countries may avoid reading the complete documentation.
Thus it presents a brief history, the structure of the platform and collaboration and communication mechanisms.
Finally it includes the cookbook with the recipes to establish yourself as a STORK connected MS and a recommendation for reading most important documents.

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

© Copyright by the STORK-eID Consortium

Table of contents

List of abbreviations

<Abbreviation>	<Explanation>
MS	Member State
MW	MiddleWare
STORK	Secure idenTity acrOss boRders linKed
PEPS	Pan European Proxy Server
QAA	Quality Authentication Assurance
SP	Service Provider
V-IDP	Virtual Identity Provider

Executive summary

This document presents an overview of STORK for new Member States which consider or have decided to connect to the STORK platform. Its objective is presenting a quick view of what STORK is and how it works, thus those countries may avoid reading the complete documentation.

Thus it presents a brief history, the structure of the platform and collaboration and communication mechanisms.

Finally it includes the cookbook with the recipes to establish yourself as a STORK connected MS and a recommendation of most important documents.

1 Introduction

1.1 Objective

This document presents an overview of STORK for new Member States which consider or have decided to connect to the STORK platform. Its objective is presenting a quick view of what STORK is and how it works, thus those countries may avoid reading the complete documentation. For complete information, these documents are still relevant and valid, but a quick overview is considered a welcome complement.

1.2 Scope

The STORK overview is meant for new Member States, so it focuses on what STORK is, its internal structure, integration of national specific functionalities, etc., as well as agreed procedures for governance, update and maintenance.

It doesn't contain technical or very detailed information; it's not meant as a reference manual.

1.3 Structure of the document

This document presents a brief history of STORK, the structure of the platform and collaboration and communication mechanisms.

2 History

Since decades, the different EU Member States have invested large amounts of money in building their own identity systems, often including citizen cards. Modernisation of those physical credentials led to the inclusion of electronic identity in those tokens.

In some other Member States also businesses, especially banks, have also invested in building electronic identification system based on strong authentication means, especially PKI.

Such electronic identity systems were frequently of little use: there were few applications which allowed people to use their credentials to access their own information. But, as time passed by, the number of applications increased constantly, especially since the EU published its *services directive* and its implementations in the different Member States.

2.1 Cross border use of eID

Acceptance of national credentials was increasing but still, cross border usage was even harder. Not knowing about legal implications, nor knowing about trusted eID providers, nor about internal formats of the different credentials made it in practice impossible to accept any foreign credential. As this was recognised during the Ministerial eGovernment Conference “Transforming Public Services” of the United Kingdom Presidency of the European Council and of the European Commission, in Manchester 2005, they established this as one of the priorities in the initiative *i2010: A European society for growth and employment in Europe*. In 2008 a consortium of 29 participants of 14 European countries was founded, to execute the STORK project. The project had as main objective to establish a European eID interoperability platform, within existing legal restrictions, respectful with all national cultures and complying with the requirements of scalability, trust and security, especially the privacy. This platform was to be piloted during 12 months. There was a clear focus on achieving interoperability on a technical level as each MS has individual legal frameworks for using own and possibly foreign electronic identities.

2.2 STORK architectures

Following development of interoperability models in the eEurope eID subgroup which led to signposts and a roadmap, this objective had been further developed and studied by a working group of the EC, IDABC,- A model that has been recommended by IDABC has been the establishment of national gateways, which it called PEPS: **Pan European Proxy Service**. The main objectives of these gateways were 1) to hide national problems for the other Member States, and 2) to be an anchor of trust, which allows leveraging the national circle of trust to Europe. Furthermore, this gateway guarantees scalability, as any change in a Member State will only affect its own gateway.

Some countries saw serious problems in such a gateway, legal, liability and security problems, as well as compatibility problems with their decentralised national ***Middleware***[1] **architecture**. Basically this decentralised architecture implies that each Service Provider has a software installed (sometimes referred to as SPware), which interacts with the user's credential through some middleware installed at the user's PC.

A direct communication between SP and the user directly using MS-specific SPwares is for several reasons not scalable and a problem for trust in a cross border scenario: first of all, you can't expect all European service providers to support an increasing number of interfaces to SPwares from each country, with all corresponding maintenance consequences. In the second place, you can't really expect thousands of Service Providers to update their trusted (ID)servers list every time a new ID provider is recognised in any of these MW countries, and including them in the ways to verify the validity of the presented credentials.

So an abstraction layer was put above the SPwares enabling the SP to support any number of SPwares using a unified interface and put into a single component, which is called a Virtual IDP, or V-IDP. This V-IDP has the same objectives as a PEPS: to hide the national problems for the other Member States, and to be an anchor of trust which allows to leverage the national circle of trust to the Europe. The main difference is the location: it is supposed to be located as close as possible to the SP, thus enabling true end-to-end communication between SP and user, but also enabling usage of or location beside national gateways, depending on each country's decision.

As far as architectures are concerned the conceptual interoperability model is explained in D5.1. This model explains how these 2 models can interoperate.

2.3 Variety of eIDs

As stated in the first paragraph, since decades governments need to enable users to electronically access their administrations. So each government has implemented some mechanisms to allow such access; some with just the traditional username / password scheme, others use this scheme, and have reinforced it with one-time-passwords generated by specific devices or sent to the citizen by SMS. In most countries also PKI is used, in soft certificates and most of all implementing these certificates in secure crypto-chips on the citizen card.

Not only the identity tokens themselves vary, also the issuing procedures are different: some of them can be achieved with a visit to an Internet site, in which the citizen is requested to type some of his data, others require the citizen to visit a registration office before issuing his credential.

Some countries only allow access with governmental eID, other also or even exclusively with eIDs issued by private organisations, especially by banks.

It will be clear that so many different types of credentials are not equally trustworthy; the authentication with some tokens is better than with other tokens. And as a consequence, some should not be allowed in some portals as their quality of authentication assurance is considered insufficient for the risks associated with the use of the application.

Thus the STORK project has defined a QAA, Quality of Authentication Assurance, which on a scale from 1-4 expresses this quality. This number takes all 7 underlying factors into account in both the registration and issuing procedure as well as the quality of the credential itself.

[1] Please note that this is the name given to this approach. Client middleware is also required for e.g. the access to crypto cards in PEPS countries.

3 The Interoperability model

A PEPS connects its national eID infrastructure to foreign service providers, as well as its national service providers to foreign eID infrastructure. To be able to use such eID infrastructure, the user plays an important role; without her/his participation there's no way to get data exchanged. Thus a PEPS has 4 interfaces, as made clear in the following chart:

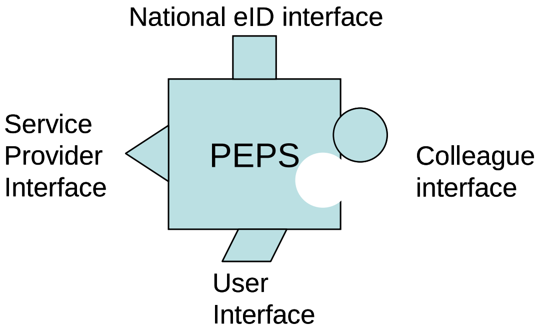


Figure 1 – PEPS and its interfaces

This schema is used to explain briefly the conceptual interoperability model.

3.1 PEPS structure

When connecting a service provider to the STORK platform, this connection will be done through his national STORK node. This node connects to each of the other national nodes of the platform, which on their turn connect to the national eID infrastructure.

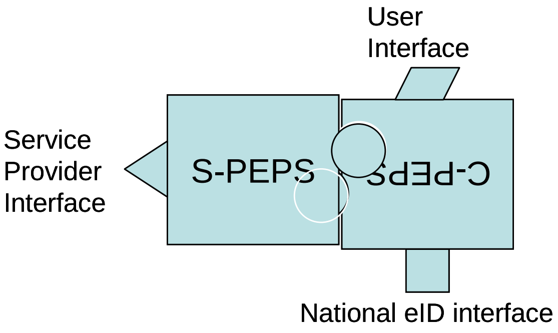


Figure 2 – Two PEPSes communicating

Thus one of the two PEPSes has the role of S-PEPS, attending requests from Service Providers, in the SP country, the other one has the role of C-PEPS, taking care of the interface with the citizen, in citizen's country. This last role also assumes the interface with eID provisioning and possible additional Attribute Providers.

Please note that, even though the redirection from SP to the C-PEPS goes twice through the user's browser and through the S-PEPS, these intermediate steps are transparent for the user.

These roles, S-PEPS and C-PEPS can also be seen within the structure of the PEPS software and the connectors to be interrogated. Normally, in one cross-border transaction, a PEPS will only assume one of these roles; only if SP country and citizen country are the same, this PEPS would assume both roles. But this scenario is not cross-border, so outside STORK's scope, and in some countries wouldn't work.

Of course, the PEPS is designed to be adapted to whatever your country may need, so for each of these interfaces standard examples are included, which may or should be personalised or substituted by the software of your needs. In the diagram just below this text, the Member State where the Service Provider is located may determine the specifications for his SP interface, the citizen's Member State will personalise the user interface (at least to national language) as well as the interface with the national eID infrastructure.

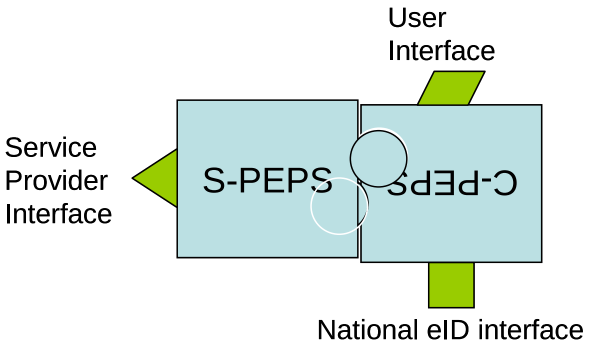


Figure 3 – PEPS interfaces which may be personalised

3.2 V-IDP structure

Internally a V-IDP has a modular backbone, called MARS, which can be personalised with "plug ins" and "plug-ons".

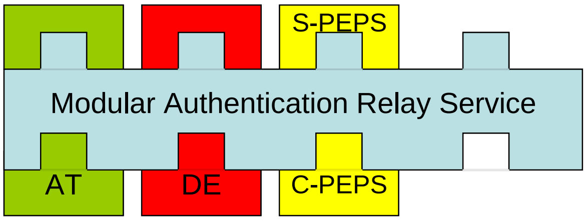


Figure 4 – V-IDP internal structure

These pieces of software allow the system to behave like a C-PEPS or S-PEPS when communicating with the rest of Europe, but also as an AT / DE service provider or eID provider, depending on its usage. When communicating with PEPSes, exactly the same protocol is used as the one used between PEPSes.

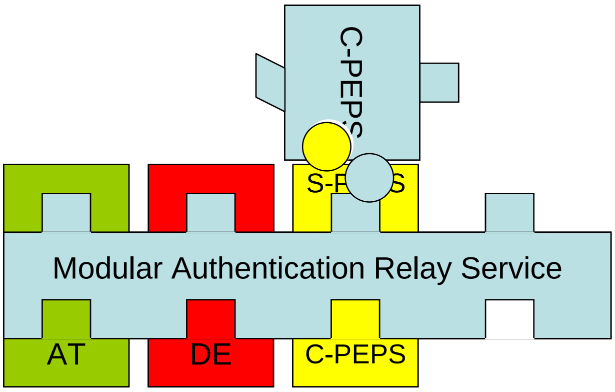


Figure 5 – V-IDP Communicates with a PEPS

In figure 5 a AT or DE service provider may request credentials from citizens of PEPS countries. A similar scheme applies for PEPSes requesting credentials from AT or DE.

3.3 PEPS or MW: Centralized or Decentralized Deployment

As indicated in 2.2, each country should have his PEPS located in his own installations, except for the MW countries which have their V-IDP located in each of the other countries. Additionally, in MW countries there may be several additional V-IDPs. When choosing on PEPS or MW architecture, you will of course choose the most convenient one; for this reason we have summarised the advantaged and disadvantages of each solution in the following table:

	PEPS	MW
Scalability: more users, more transactions	We may foresee the need for cryptographic hardware (HSM) in the PEPS	Fully Scalable.
Scalability: New SPs, IDPs, or countries	IDPs: Inclusion in the circle of trust of its country's PEPS SP: if trust is required, inclusion in the circle of trust of PEPS of its country Country: inclusion in all PEPS	IDPs: Inclusion in the circle of trust of its country's SPWare SP: if trust is required, inclusion in the circle of trust of SPWare Country: inclusion in all SPWare; and in all cases distribution of the SPWare
Flexibility (more attributes)	Architecture foresees APs to be attached to the systems. Each country should consider the need for such APs.	Extra attributes can be negotiated between SP and AP, but outside the SPWare.
Availability	Some measures should be taken to guarantee High Availability	Is guaranteed
Mobility	On user's own PC guaranteed. With username / password guaranteed With token, limited by presence of card-readers	On user's own PC guaranteed. On other PC's, limited by presence of card-readers
ID Federation	Yes, within limits to be defined.	Technically not, but this functionality could be built, so that is would be transparent to user.
Implementation & maintenance issues	Limited amount of installations, so easy. Restricted interventions due to high availability.	Larger amount of installations, more complex. Restricted interventions due to software distribution procedure.

Table 1 PEPS vs MW evaluation

A brief discussion. The MW architecture looks like easier, as you don't exploit your own hardware. Furthermore, it has better guarantees for security: it allows you to build tunnels from the users crypto-card to the endpoint of communication, immune to infection of the user's PC.

On the other hand it has a more problematic procedure on changes of parameters and software, as these need the collaboration of each of the involved countries. This limits in practice the scalability of new ID providers, and new countries, and limits the flexibility with additional attributes.

3.4 Systems in the STORK platform

As indicated, each country should have his PEPS located in his own installations, except for the MW countries which have their V-IDP located in each of the other countries. Additionally, in MW countries there will be several additional V-IDPs.

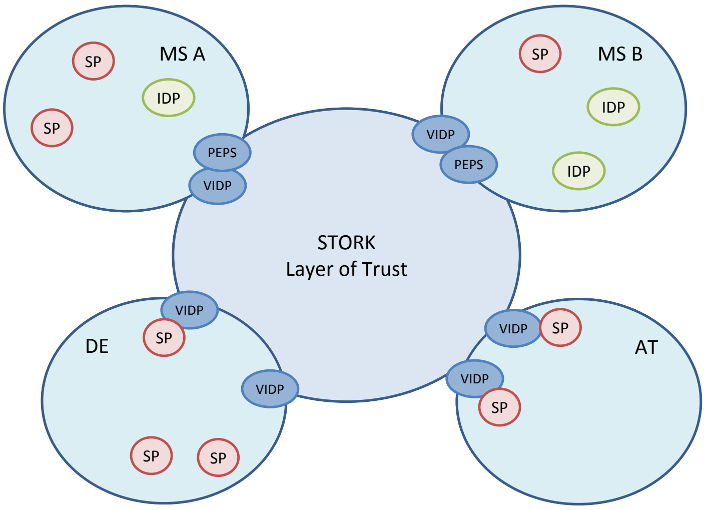


Figure 6 – PEPSes and V-IDPs in Europe

3.5 Communication structure

When a user from one country connects to a service provider in another country, and accesses the personalised part, the Service provider will request the user to authenticate. If he chooses to authenticate with foreign credentials, he is requested to answer the "from where" question. So the service provider sends this request to its national STORK node, which redirects the user to the authentication portal of the country of his choice. All these redirections pass through the user's browser. This is presented in the following (simplified) diagram.

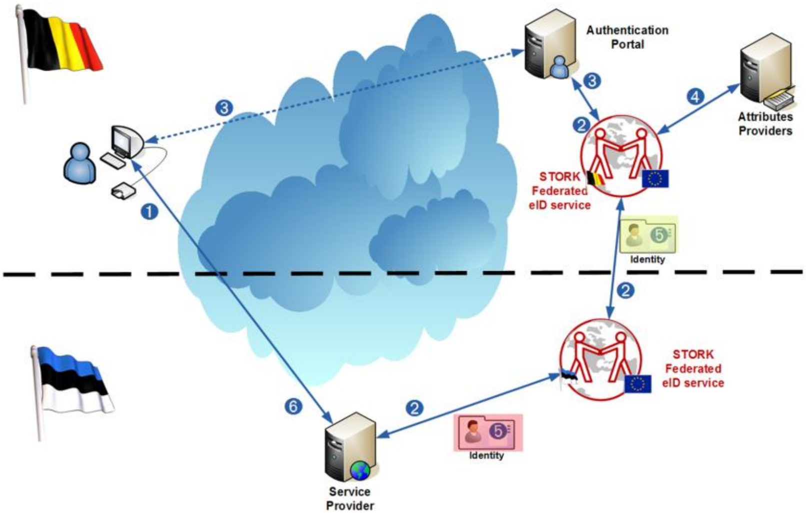


Figure 7 – PEPS-PEPS communication structure

In case of MW countries this scheme is of course very similar; just the national node is located in the other country, and optionally the SP can also have a V-IDP.

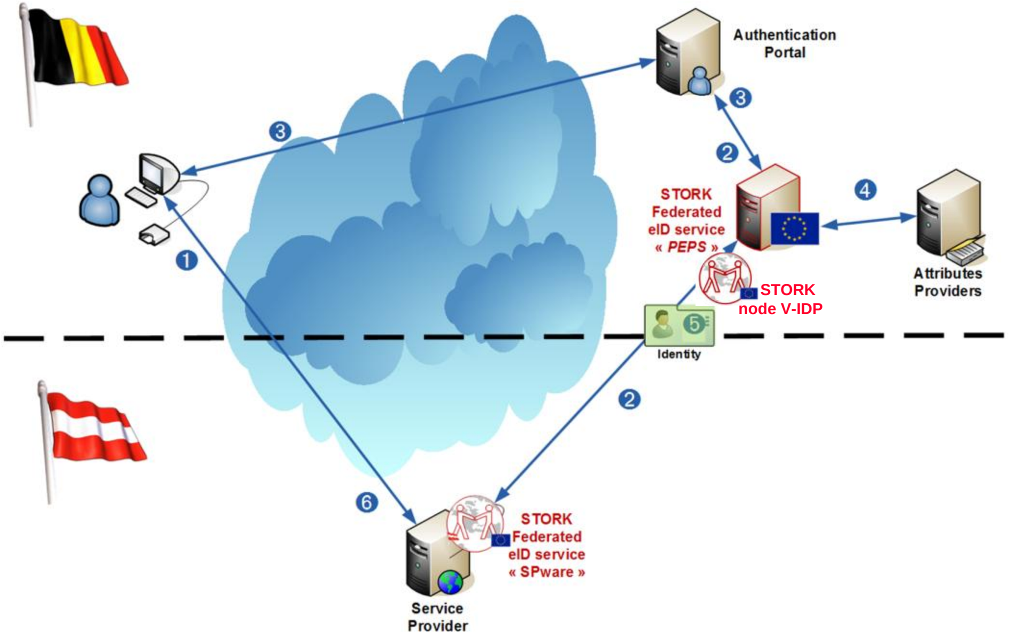


Figure 8 – PEPS-V-IDP communication structure

3.6 Authentication and registration

Most eID management systems are about authentication, understood as the application obtains just the user’s identifier. The STORK platform promotes the minimal disclosure, so allows authentication even without such an identifier; if only age and gender are needed the application may request these attributes.

More in general, the STORK platform defines the authentication process to be able to obtain any combination of the data items defined in the platform. Thus, the process of registering for a service is only different from re-entering this same service in the amount of attributes, but both send an authentication request to the STORK infrastructure.

Some parts of the STORK documentation is about attribute transfer, understood as the business process which obtains additional attributes for already identified users. The idea behind this process is that some applications first request only the user’s identification number, and, if the user is unknown, request those additional attributes. For the moment no such application has been found, so this business process hasn’t been implemented.

Please note that attribute transfer as a business process is different from attribute provisioning, the process of completing the user’s data requesting additional attributes from attribute providers.

3.7 Certificate Validation

Most people, when referring to STORK they limit themselves to the Authentication process, which is defined as the same as the registration process. Another process included in STORK is the Certificate Validation.

Right from the start, STORK was thought of as to support digital signature. As there are so many signature formats the consortium considered it little useful to support the validation of the signatures themselves; normally a service provider which has decided to use one of these formats already has implemented the software to verify the signature on mathematical correctness (does it match the document which is supposed to be signed), is the signer authorised, does the certificate have the right characteristics, etc.

But what a SP can't always do, is to verify that the certificate was valid when the signature was produced. Not all CA's publish their OCSP service or CRL freely in the Internet. Thus the STORK project built an OCSP gateway, which allows SPs of any country to validate the certificate. Not all countries have implemented this facility.

The STORK project team was aware that developments in its sibling LSP PEPPOL on eProcurement and/or the Commission Decisions on signature formats and trust lists related to the Services Directive may enable a comprehensive cross-border infrastructure. Thus, STORK limited itself to the helper functions described above until it can adopt those developments.

3.8 Circles of Trust

The STORK circle of trust is formed by each of the national PEPSes, together with each of the corresponding V-IDPs. These systems, which in figure 6 are on the border of the "STORK layer of trust", trust each other explicitly. This explicit trust means – translated in more technical terms - that the relevant data of these "colleagues" are stored at each of the other colleagues' sites. Relevant data are e.g. the certificate which is used for signing, the URL where to send requests to, the country's name and abbreviation, etc.

This trust requires that each of these systems is secure; thus each of them has passed a "Security Self Assessment[2]", with which each of the Member States makes sure to fulfil most usual security criteria.

3.9 User control and Consent

When designing the STORK authentication business process, one of the requirements was that the user should always be in control of his data. Thus the platform is build around the user centric approach. One of the steps is the user consent. No data item is being sent abroad unless the user allows the administration to do so.

The user can give his consent in various different ways:

1) Implicitly. By introducing his credential, he implicitly allows the included data to be transferred to its destination service provider.
2) Explicitly for data types. Such consent can be given before data is collected, it just needs to know the requested data. This consent may allow the user to exclude some of the attributes to be sent.
3) Explicitly with data values. Such consent is after having collected all data, and shows the data which will be sent to the SP. Due to legal restrictions in some countries, this process is implemented in the following way: the data is signed by the authority, and these signed data are given to the user. This procedure is very similar to the authorities giving the user an official document like a passport, which the user may present to others, like the customs office. As the data are signed, the user may not exclude any item.

[2] For the moment, within the STORK project, there hasn't been enough time to execute a normal security audit by the competent accreditation body. So this *Security self assessment* is considered as the only feasible assessment as comparable as possible – within the limited timeframe – to a full accreditation.

Also both consents may be requested. In some cases intermediate “consent” may be advisable: if data are retrieved from external sources others then the credential, such consent should be considered.

4 Governance

This infrastructure needs several procedures to be in place to be operational; procedures to control any type of change. Below we describe the practice in the pilot scope. As a main sustainability and governance action, handover of STORK common component maintenance and infrastructure governance to the European Commission's ISA Programme is being worked on. This may lead to governance structures different from and – with mission critical applications being connected to STORK – probably exceeding the parameters given here.

4.1 Support

During the lifetime of the STORK project, a "Change Control and Support Procedure" was accepted, which in the first place describes the support organisations. Please remind that STORK is a platform integrating systems of many organisations, and each of these organisations may (will) have their own support organisation; normally even organised for information systems, and not for the complete organisation. Thus many of such organisations need to have a common understanding of how support of the platform is organised.

In general we may expect that, if they experience any problem, the users will contact the service provider who has STORK integrated. So if this service provider can't solve the issue, he'll have to contact his local STORK representative. If this representative can't solve the problem, he'll get into contact with the representative of the country the user is from, which on his turn could need the help from the eID provider or attribute provider.

Each representative has a list of contacts, as well the STORK national partners (Service Providers, ID providers and Attribute Providers), as the international partners: the STORK support colleagues.

In general, this STORK second line support has an availability of 8x5, excluding official bank holidays. This support is in general available, also if there's no problem of a user; you can also count on it if you have problems installing or integrating the STORK common software.

4.2 Change control

The same procedure as above also applies to the change control. Change control has 2 objectives:

1) to make sure that any change applied to the common STORK software is correctly agreed, and

2) to make sure that any change is correctly assigned a priority.

The document describes the procedures of change control, both for error corrections and for improvements. In general it describes the use of the OSOR[3] platform for bug-tracking, although email may/should also be used. For this reason we can also use the distribution list stork-support@lists.atosresearch.eu.

Changes of the specifications are to be discussed by email, to get all points of view clear, and possibly by phone to achieve, through an interactive discussion, getting those points of view as close as possible, and the best decision for the STORK community. Such email discussions may start somewhat informally, but should always end with some proposed updated formal documents with specifications, for which a reasonable time is given to all involved parties to read and

[3] See http://www.osor.eu/projects/stork

comment it. Normally a reasonable time is 2 weeks, but typical holiday periods like Easter, summer and Christmas oblige us to increase this period.

If any priority issue or major changes would arise, these will be discussed by the Change Control Supervisory Board, which will adopt decisions concerning as well the issue on itself, as the migration strategy, as far as necessary. This board is composed of the responsible persons of the development teams of common code, as well as the persons responsible for development of independent implementations.

Any disagreement should be elevated to the MS Council.

4.3 Version control

The major problem the STORK countries have faced has been version control. In the first place when going live it cost quite some effort to be compatible with every country. But once achieved this compatibility, things all of a sudden stopped working, due to the fact that someone changed something in his installation and didn't test this change with every other country.

So after some time, knowing the problems with version control and foreseeing many changes, a proposal was made and accepted to include an automated version control facility in STORK. Basically this is a program which executes every day, and extracts from the software its version number, and from the configuration files the modification date, and publishes this in an XML file accessible to other STORK partners.

This way all partners can at least know when changes have taken place.

The same mechanism is proposed to apply changes of your own parameters at all partner's sites, like renewing your SAML signing certificate, or changing the name of your STORK connector. Such changes need this file to be signed; with the old certificate in case of certificate renewal.

All partner's version control files are downloaded on a daily basis, and a similar version control file is composed to be published to all service providers in a country. This file includes the same description for the national PEPS as previous file, and additionally for each other country a summary of available data and QAA. A *country selector updater* downloads this file every day, and updates this service provider's country selector, taking into account the attributes and QAA level required by the service, as well as countries to be excluded. This way, new countries will automatically be included in all country selectors of all service providers, once the national STORK node includes this country.

On the other hand, this SP version control facility also publishes the version data of this installation, thus allowing the national PEPS organisation to see whether or not patches have been applied, and on this basis decide if a new patch, depending on previous patches, may be applied.

4.4 Relationship with your national service providers

The STORK circle of trust is between all STORK countries and their national STORK nodes (PEPSes or V-IDPs). A similar circle of trust is proposed for your national service providers: you explicitly trust each of them. The common code proposes that you store their certificate in the keystore, using as an alias of their provider name, just as they'll use it in the SAML token.

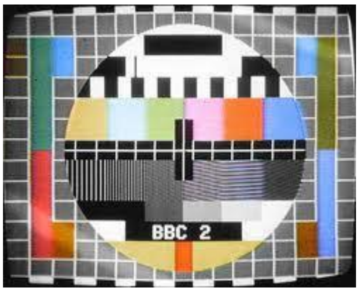
Any country may establish alternative mechanisms to verify that a SP is allowed to request foreign users' credentials, according to its own policy. There's just one restriction: it must check that the provider name is correct. This name may be a commercial name, which is known to European public, instead of the official name if this is less known. E.g. "Mercedes-Benz" may be used instead of "Daimler AG". This name is shown on the user consent page, before the data is sent to the service provider.

Apart from the provider name, it would be useful to store some more data about the SP, like contact persons.

In the STORK integration package (for SPs) some easy procedure and connection request form is included. In your national implementation you'll have to adapt these to what you estimate best.

In STORK nearly all countries consider any nationally authorised SP as valid. No checks are done in Spain on Belgian SPs: any SP the Belgian authority accepts is accepted all over Europe. Thus, once they're connected to your national S-PEPS, they can accept nearly all foreign credentials. One of the exceptions to this general rule is Germany, which requires an additional validation of the SP before any data from German citizens can be transferred.

4.5 Testing and Going Live



As STORK isn't a system, it's a platform consisting of systems. Before we can add a new node to the platform, exhaustive testing must be performed. After unit and system test, integration tests are performed in preproduction environment in several stages.

In the first stage, exhaustive testing should be performed with the DemoSP, a standard testing tool which is delivered in the STORK toolkit. At first, these tests should be performed against the system itself, i.e. the system simulates that a citizen from this country accesses services in the same country.

Once these tests have been successful, the second stage of testing includes involving real national service providers; of course also in preproduction environment. As SPs will normally not have many different requests (one for authenticating known users and a few for new users), this task will usually be done in less time than the previous step.

The third stage includes cross border testing with the DemoSPs of different countries; first of one country, and later on expanding this to all countries. All tests are against the eID infrastructure of the new country. Getting things working with one country will cost some time, but the expansion to all countries can be relatively quick, as all use the same protocol and there are only few implementations of it.

The last stage of testing is cross border testing with of the eID infrastructure of the new country against real foreign SPs.

Although in each stage we test all components, the accent of testing in stage 1 and 3 is on the C-PEPS/V-IDP, the one which will request the user's credentials and send these data abroad. In stage 4 the accent is on integrating national or foreign credentials in applications. As a consequence, the responsibility for stage 1-3 is mainly for the owner of the national STORK node, often the owner of the eID infrastructure. For testing purposes he'll need testing credentials of his own eID. In stage 4 however, testing is done by foreign organisations with test credentials of the new country. These foreign organisations are responsible for executing these tests, but need the new country to send them test credentials.

An excellent “draft” test plan with a detailed description of test cases is available at the STORK website. In this description you’ll find a more or less exhaustive enumeration of tests you’re suggested to execute, and you’re encouraged to personalise this list, adding your cases and stating that you don’t need to do other cases.

Once testing is completed, you should migrate to production. In production environment you should execute a security self assessment, also mentioned in 3.8, replying a set of questions. Obviously in production several of these tests should be repeated. The report on Security Self Assessment, together with the test reports should be sent to all other member States, to approve you connection to the STORK platform. These other member states will also need some data, like the certificate you use for signing the SAML tokens and where requests for your eIDs should be sent to.

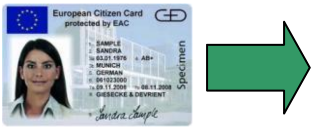
When going live, you should make sure to notify all partners on time, thus they’ll be able to verify that everything is working.

5 The “How to connect to STORK” Cookbook

This section will describe in a nutshell, what a country needs basically to carry out, if connecting to STORK. The two underlying use cases “granting foreign citizens access to my services” and “getting my citizens’ electronic identity accepted by STORK” are discussed separately – this as also MS can connect Service Providers to STORK even if no national eID system is yet in place (consider e.g. connecting your Points of Single Contacts under the Service Directive to STORK).

A first step to be taken by the country is the decision if the centralised model (PEPS) or the decentralized model (Middleware) better fits the national legal and organisational environment. Both cases are discussed below.[4]

5.1 Getting national credentials accepted



This assumes that the country connecting to STORK has an eID infrastructure in place and that national protocols are employed (that not necessarily need to adhere to international standards). In both models (PEPS/MW), the eID tokens to be used need to be assessed against the Quality Authentication Assurance (QAA) scheme developed by STORK. The QAA labelling (ranging from 1 – low to 4 – high assurance) is based on the quality of the eID issuance process and the security of the eID token. It allows the service provider to request credential fitting its needs.

If the central PEPS-model is opted for, the country needs to

1. Deploy a C-PEPS (common open source code is provided)
2. Integrate the national eID protocols at the C-PEPS national interface (cf. figure 2)
3. Carry out a security self-assessment of its implementation and deployment
4. Communicate its C-PEPS parameters (addresses, SAML signers, etc.) to the governance body (ISA), which will distribute them to the partner MS

If the decentralised V-IDP model is chosen

1. Implement a national protocol plug-in for the V-IDP MARS components (cf. figure 4)
2. Carry out a security self-assessment of its implementation
3. Deploy the plug-in at all other V-IDPs (hosted at the S-PEPS or SP)

5.2 Allowing my services to obtain foreign credentials

To be able to allow SPs to connect to STORK, the corresponding actions depend on the architectural model you have chosen:

If the PEPS-model is opted for, the country needs to

1. Deploy a S-PEPS and a V-IDP (common open source code is provided)
2. Integrate the national SP protocols at the S-PEPS national interface (cf. figure 2)[5]
3. Communicate its S-PEPS parameters (addresses, SAML signers, etc.) to the partner MS

[4] Please note that V-IDP could also be deployed centrally

[5] Most countries implement just the STORK protocol, without any change. This is the easiest and existing solution if you start from scratch. If needed you may implement other protocols instead

If the MW model is chosen the country needs to

1. Implement SP-connector plug-on for the V-IDP MARS components (cf. figure 4)
2. Deploy this connector at each V-IDP attending SPs.

5.3 Connecting my service

Each Service Provider which wants to connect to STORK needs to integrate the *Integration Package* for his country into his application. Apart from the technology, he'll need to decide the minimum QAA level he'll require for his service, and which attributes he'll request as mandatory and which ones as optional. This, and the criteria for making these choices, is explained in the manuals in the integration package.

If the PEPS-model is opted for, the Service Provider needs to

1. Integrate the *Integration Package* into his application

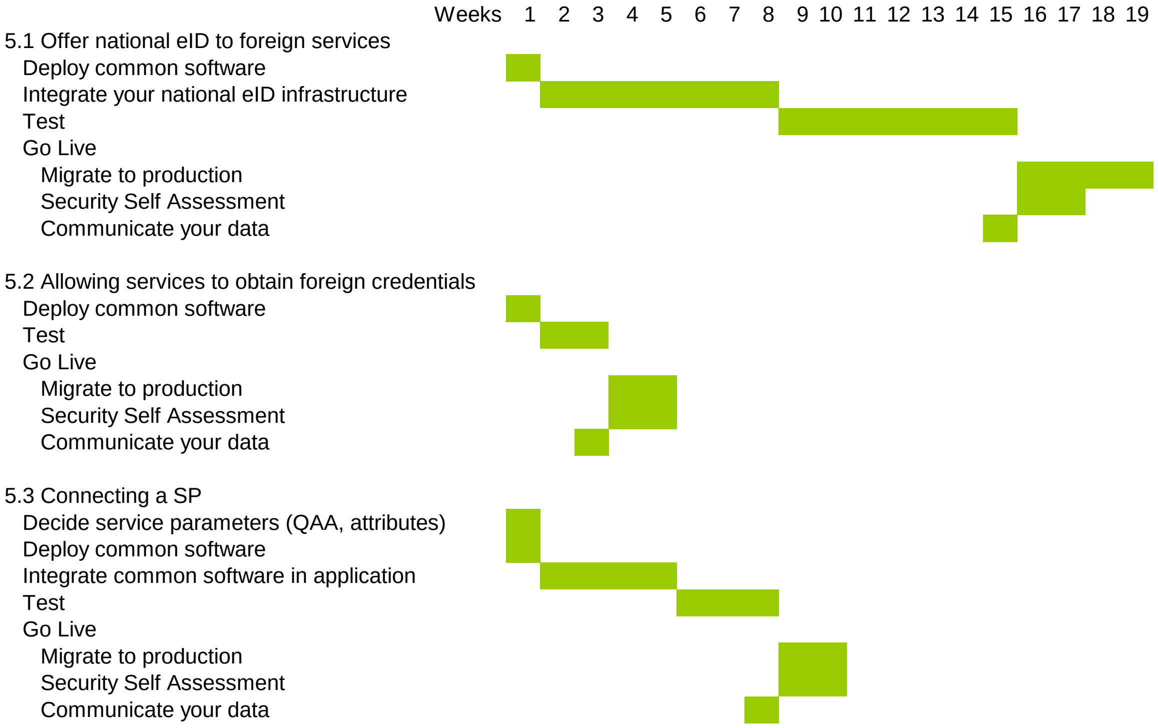
If the MW model is chosen, the Service Provider needs to

1. Integrate the *SPware* into his application (part of the integration package)

Of course, a country opt for either or both cases 5.1 and 5.2/5.3. The combination of the steps described needs to be carried out then. Please note that, even though the actors are different, 5.2 and 5.3 should be done together; one doesn't make sense without the other.

5.4 Estimated timeline

This paragraph has the objective to give you some orientation of times in which you may be able to do this integration. We're quite aware that every country has its own problems with legal and technical issues, so there can't be a universal planning. But as a first approach it might be useful for new partners. A recipe should include some time indications.



Weeks	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
5.1 Offer national eID to foreign services																			
Deploy common software	🟩																		
Integrate your national eID infrastructure		🟩	🟩	🟩	🟩	🟩	🟩	🟩											
Test									🟩	🟩	🟩	🟩	🟩	🟩	🟩				
Go Live																			
Migrate to production																🟩	🟩	🟩	🟩
Security Self Assessment																🟩	🟩		
Communicate your data															🟩				
5.2 Allowing services to obtain foreign credentials																			
Deploy common software	🟩																		
Test		🟩	🟩																
Go Live																			
Migrate to production				🟩	🟩														
Security Self Assessment				🟩	🟩														
Communicate your data			🟩																
5.3 Connecting a SP																			
Decide service parameters (QAA, attributes)	🟩																		
Deploy common software	🟩																		
Integrate common software in application		🟩	🟩	🟩	🟩														
Test						🟩	🟩	🟩											
Go Live																			
Migrate to production									🟩	🟩									
Security Self Assessment									🟩	🟩									
Communicate your data								🟩											

Figure 9 – Estimated Gantt chart

Some notes on this planning. In the first place it doesn’t take into account that there may be holidays. In the second place, as mentioned, the authors of this document can’t really estimate the difficulty of integrating your systems into STORK.

In the third place, in our experience testing takes quite more time than in ordinary systems. This is due to the fact that we’re not working with a system; this is a platform of many systems, which makes it more complicated to execute all tests thoroughly.

In the fourth place, the migration to production, which should be a matter of very little time, in practice has always resulted far more than what was expected, due to the same reason.

And, last but not least, this plans to have the core operational. Getting several add-ons, like administration tools, statistics, version control, etc. into operational state will take several weeks more.

As a summary, half a year is an optimistic planning.

6 What documents to read

The STORK has produced a large amount of documents. All of them are necessary to better understand STORK, its achievements, and why where things were done in specific way. In order make it easier and faster to get into the project and to be able to connect to STORK platform, below is a suggestion of documents to read before starting to integrate your country in STORK.

Name	Who	Description
D2.3 - Quality authenticator scheme	Leaders,[6] Legal experts	Defines the STORK QAA framework, including the four levels of authentication assurance, also facilitates mapping of national levels and eID solutions onto each other.
D4.3 Updated Report on eID Process Flows	Leaders Legal experts	Provides generic process flows for authentication, attribute transfer and e-signature transfer. It also reflects the demonstrators for the attribute transfer and authentication process flows showing the user experience.
D5.1 Evaluation and assessment of existing reference models and common specifications	Leaders, development team	This document evaluates the PEPS and MW model, and describes the interoperability model in detail.
D5.7.3 Functional Design for PEPS, MW models and interoperability	Development team	This document is the functional design of the STORK platform, and the interoperability of electronic identifiers.
D5.8.3 Technical Design for PEPS, MW models and interoperability with annexes	Development team	In this document the specification of the two STORK systems is presented: PEPS and V-IDP. This document is divided in four annexes where the main content is presented: D5.8.3a SoftwareArchitectureDesign, D5.8.3b InterfaceDesign, D5.8.3c Software design PEPS, D5.8.3d Security principles and best practices and 5.8.3e Software Design MW

Table 2 Documents suggestion

[6] Leaders is thought of as the leader of the STORK integration project, as well as the leader of the development team.