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

D2.3 - Quality authenticator scheme

Deliverable Id :	**D2.3**
Deliverable Name :	**Quality Authenticator Scheme**
Status :	**Final**
Dissemination Level :	**Public**
Due date of deliverable :	**M9**
Actual submission date :	**03 March 2009**
Work Package :	**2**
Organisation name of lead contractor for this deliverable :	**Dutch Ministry of the Interior and Kingdom Relations**
Author(s):	**B. Hulsebosch, G. Lenzini, and H. Eertink**
Partner(s) contributing :	**AT,BE,EE,ES,FR,IC,NL,SW,UK**

Abstract: This deliverable combines the work described in deliverable D2.1 and D2.2 and defines the common STORK Quality Authentication Assurance framework. It describes how national authentication levels can be mapped onto STORK QAA levels to ensure eID interoperability. Mapping of these levels onto each other is not always straightforward. Recommendations are given to ensure proper mapping. Furthermore, legal implications regarding the use of qualified certificates are taken into account in the STORK QAA framework. Solution directions are offered to ensure legally allowed use of identifiers in STORK.

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

History

Version	Date	Modification reason	Modified by
0.0	11/11/08	Creation of the Deliverable	G. Lenzini
0.1	01/12/08	added part of the background	G. Lenzini
0.2	01/12/08	added part of the legal implications	B. Hulsebosch
0.3	12/01/09	Draft version for internal review	G. Lenzini, B. Hulsebosch
0.4	17/01/09	Extended table of content, and revised sections	G. Lenzini, B. Hulsebosch, H. Eertink
0.5	19/01/09	All sections have been revised and extended.	G. Lenzini, B. Hulsebosch, H. Eertink
0.8	09/02/09	Processed comments of member states	G. Lenzini, B. Hulsebosch
1.0	10/02/09	Second processing of comments	B. Hulsebosch, G. Lenzini
1.1	17/02/09	Template compliance, risks list section. and minor adjustments	B. Hulsebosch
1.2	18/02/09	Integrated with feedback given during the WP2 meeting at The Hague (18 February)	B. Hulsebosch, G. Lenzini
1.3	19/02/09	Processed comments of WP2 manager	B. Hulsebosch
1.4	23/02/09	Processed comments of various member states	B. Hulsebosch, G. Lenzini
1.5	24/02/09	Added Risk and Quality management	S. Kenswil, G. Lenzini
1.6	27/02/09	Final check by WP2 manager and authors	J. Timmermans, B. Hulsebosch, G. Lenzini

Table of contents

HISTORY **2**
TABLE OF CONTENTS **3**
LIST OF FIGURES **5**
LIST OF TABLES **6**
EXECUTIVE SUMMARY **7**
ACRONYMS **9**
1 OVERVIEW AND INTRODUCTION **10**
1.1 INTRODUCTION 10
1.2 SCOPE AND OBJECTIVES 10
1.3 OVERALL METHODOLOGY 10
1.4 APPROACH 11
1.5 RISK MANAGEMENT 12
1.5.1 IDENTIFIED RISKS 14
1.5.2 MATERIALIZED RISKS 15
1.6 QUALITY MANAGEMENT 15
1.6.1 ACCEPTANCE CRITERIA 15
1.6.2 THE PROCESS 15
2 STORK QUALITY OF AUTHENTICATION ASSURANCE MODEL **17**
2.1 DESCRIPTION OF STORK QAA LEVELS 17
2.2 REQUIREMENTS FOR STORK QAA LEVELS 18
2.3 STORK REQUIREMENTS FOR THE REGISTRATION PHASE 19
2.3.1 QUALITY OF THE IDENTIFICATION PROCEDURE 20
2.3.2 QUALITY OF THE IDENTITY ISSUING PROCESS 21
2.3.3 QUALITY OF THE ENTITY ISSUING THE IDENTITY CREDENTIALS 23
2.3.4 ASSURANCE LEVELS FOR THE REGISTRATION PHASE 24
2.4 STORK REQUIREMENTS FOR THE ELECTRONIC AUTHENTICATION PHASE 25
2.4.1 TYPES AND ROBUSTNESS OF THE IDENTITY CREDENTIAL 25
2.4.2 SECURITY OF THE AUTHENTICATION MECHANISM 26
2.4.3 ASSURANCE LEVELS FOR THE ELECTRONIC AUTHENTICATION PHASE 28
2.5 STORK QAA LEVELS 29
3 MAPPING EXISTING MECHANISMS ON THE STORK QAA LEVELS **30**
3.1 MAPPING THE NATIONAL EID LEVELS TO STORK QAA LEVELS 30
3.2 MAPPING TO THE PEPS AND MIDDLEWARE APPROACH 33
3.3 MAPPING TO SAML 34

3.4 COMPLIANCE AND SUPERVISION 34
4 LEGAL IMPLICATIONS AND SOLUTIONS 35
4.1 ANALYSIS OF THE LEGAL IMPLICATIONS 35
4.1.1 USE OF CERTIFICATES FOR AUTHENTICATION PURPOSES 35
4.1.2 IDENTIFIERS 36
4.2 SOLUTION DIRECTIONS 36
4.2.1 OPAQUE AND TRANSIENT IDENTIFIERS 36
4.2.2 PRIVACY ENHANCING TECHNOLOGIES 38
4.2.3 USER CONSENT 38
4.2.4 USER-CENTRIC IDENTITY MANAGEMENT 39
5 SERVICE PROVIDER PERSPECTIVE 41
6 SUMMARY AND CONCLUSIONS 42
REFERENCES 44

List of figures

Figure 1: Mapping authentication assurance levels. 12
Figure 2: Factors that influence the STORK QAA Levels. 19
Figure 3: Applying the mapping. 30
Figure 4: Legal implications in the framework. 35
Figure 5: Identifier linking. 38

List of Tables

Table 1 Risk analysis template. 13
Table 2: General Risk List. 15
Table 3: Acceptance criteria list and results. 16
Table 4: STORK QAA levels. 17
Table 5: Quality levels of the identification procedure. 21
Table 6: Quality levels of the issuing process. 22
Table 7: Requirements regarding the quality of the entity issuing identity credentials. 24
Table 8: Aggregated quality levels of the registration phase. 24
Table 9: Quality levels of the identity tokens. 26
Table 10: Quality levels of the authentication mechanism. 28
Table 11: Aggregated quality levels for the electronic authentication process. 28
Table 12: STORK Quality of Authentication Assurance levels. 29
Table 13: Mapping of national assurance levels to STORK QAA levels. 31

Executive summary

The STORK project aims to make it easier for European citizens and businesses to access online public services across borders. Authentication is an important element to realize this ambition. However, most individual member states have their own eID solutions for citizen authentication thereby hampering successful provisioning of pan European services. Therefore, a common framework for mutual recognition of national electronic identities between participating countries must be developed and tested. Such a framework provides interoperability of national eID solutions and also ensures that the member states are aware of each other's solutions and of the quality of eID assurance associated to each authentication solution.

In this deliverable we have defined a common framework for eID interoperability. This so-called STORK QAA framework includes four levels of authentication assurance and facilitates mapping of national levels and eID solutions onto each other. The four levels are related to the requirements regarding the needed assurance of the user's identity. The stronger the requirements, the higher the level of assurance will be. The STORK QAA levels contain an organizational and a technical component. Organizational aspects that must be taken into account are the quality of the identification procedure, the process of issuing identity tokens, and the quality of the certification authority. Technical aspects are related to the overall authentication procedure and include the type and robustness of the identity tokens provided and the quality of the mechanisms used for user authentication. Each of these five aspects is individually rated and the weakest component determines the over STORK QAA level for a certain eID. The presented STORK QAA framework allows for mapping of national eID solutions to STORK QAA levels and provides a means for mapping of national levels of different member states onto each other.

This mapping however is not always straightforward. The following situations need attention:

- There are member states that have multiple authentication solutions with different assurance on the national level but with equal assurance in the STORK framework (e.g. Luxembourg and France). To prevent undesired mappings we recommend in this case that the STORK QAA level must always be mapped onto the highest national level corresponding to the STORK level.
- There are member states that have several authentication solutions with equal assurance on the national level but with different assurance in the STORK framework (e.g. Italy and Estonia). In this case a more fine-grained national level specification is required to prevent unsought mapping of levels. We recommend them to adopt the STORK QAA levels. Alternatively, a more detailed specification on the protocol level could be used. However, it is unlikely that SAML, as the default standard for identity information exchange, can facilitate this.
- There are member states that do not have authentication solutions that map onto the highest STORK level (e.g. the Netherlands and the UK). In principle this is not a problem. Many member states are in the process implementing national identity cards (STORK level 4) or are at least thinking about it. This problem will be solved over time when all member states realize their roadmaps.
- There are member states that have only a single authentication assurance level that corresponds to STORKS's highest level (e.g. Austria). Service providers of those member states may be inclined to authenticate citizens with the highest level of assurance: Level 4 in STORK terminology. This inclination, however, implies that many citizens of other member states can never access their services. For these citizens, other more expensive solutions need to be provided. Service providers should therefore make a risk assessment regarding their services and decide for themselves if the highest level is the best choice. Less critical services

may be rated with a lower assurance level thereby allowing more citizens access. This implies that service providers of such member states should have knowledge about other levels, and preferably STORK levels, as well. If service providers are given the option to conform to the STORK QAA framework instead of a national assurance framework, then they must express what type of assurance levels they adhere to (STORK and/or national). Otherwise mapping may go wrong.

Mapping of levels onto each other will be done in a distributed manner and, depending on the solution used, executed at the PEPS or by the middleware.

Legal matters limit the use of eID solutions across Europe and can therefore be a major show-stopper for eID interoperability. They do not have a direct impact on the STORK QAA framework however but they may for instance forbid the communication of persistent identifiers between member states or require the use of qualified certificates. The latter matter is taken into account in the STORK QAA framework. The use of qualified or non-qualified certificates is an important element for the determination of the assurance level. Regarding the prohibition of using persistent identifiers several solution directions are available. These solutions directions include the use of opaque and transient identifiers, privacy enhancing technologies, and explicit user consent via user-centric identity management solutions.

Finally, some form of supervision is required to enforce compliance to the STORK QAA framework and to take care of the contractual aspects regarding trusted eID interoperability. These aspects fall outside the scope of WP2 but should be discussed and solved in STORK.

Acronyms

The following table lists the acronyms and abbreviations used along the document.

AP	Attribute Provider
CSP	Credentials Service Provider
eGov	Electronic Government
eID, eID	Electronic Identity
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens
IDP	Identity Provider
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (in English: Methodology for Information Systems Risk Analysis and Management)
MS	Member State
OCSP	Online Certificate Status Protocol
PEPS	Pan European Proxy Services
PKI	Public Key Infrastructure
RA	Registration Authority
RP	Relying Party
SAML	Security Assertion Markup Language
SP	Service Provider
STORK QAA	STORK Quality Authentication Assurance
WP	Work Package

1 Overview and introduction

1.1 Introduction

STORK is about ensuring access to services supplied by any European service provider using authentication tokens that are provided by or on behalf of any European government. Accepting electronic credentials issued by a foreign country requires being aware of the assurance level associated to that foreign electronic authentication solution. Thus, in order to be able to determine the assurance levels in authentication, we must be able to measure the quality of different authentication procedures. That allows us to claim that a certain solution has the same (a better, a worse) quality assurance level as another solution. The definition of assurance levels in authentication allows one to abstract from concrete authentication tokens and processes, to adapt to new technologies easily, and to compare different authentication solutions in order to ensure interoperability between the different eID solutions that exist nowadays in Europe.

1.2 Scope and objectives

The aim of WP2 is to define a common framework for the definition of authentication assurance levels for cross-border authentication interoperability among the EU member states. The work accomplished in WP2 should serve as input for several other work packages, in particular WP4, WP5, and WP6.

According to the STORK DoW, WP2 is split up into three successive tasks. The first activity consisted of the definition of a preliminary STORK Quality Authentication Assurance (in short STORK QAA) framework, an inventory of all eID solutions use in Europe, their national ratings and a preliminary mapping of these national ratings onto STORK QAA levels. The results are described in deliverable D2.1 [1]. In the second activity, we analysed the legal implications for eID interoperability in Europe. This analysis included an overview of national legislation regarding the use of identity information and resulted in several STORK QAA framework dependencies with current legislation. The results are described in deliverable D2.2 [2]. This deliverable D2.3 refers to the third task, the final definition of a common framework for quality assessment of eID authentication solutions in Europe. It summarizes and refines the contents of deliverable D2.1 [1] and takes into account the legal implications as described in deliverable D2.2 [2] of the STORK project.

1.3 Overall methodology

The first step to complete deliverable D2.3 was the analysis op the work done in deliverable D2.1 and D2.2. The second step was to map the analysis from deliverable D2.1 and D2.2 to each other and to define a STORK QAA Level. Based on a list of high priority questions for deliverable D2.3 a preliminary draft was sent out to all WPs. This preliminary draft described the planned objectives, tasks and results for each country report. The partners were asked for comments on the conclusion. The comments have been taken into account and the final draft has been created and sent to all WP-partners with request for comments. The received comments have been processed and the document has been adapted (comments from UK, Spain, France, Iceland, Belgium, Sweden, Austria, Netherlands and Estonia). On the 18th of February, the Dutch ministry of the Interior and Kingdom Relations organised a final meeting in The Hague and some fundamental issues for D2.3 were discussed. After this meeting all partners were given a week for final modifications. On the 27th of February, D2.3 has been finalised.

1.4 Approach

The starting point for WP2 was an analysis of the IDABC report on authentication interoperability [3]. IDABC uses a multilevel approach for authentication assurance.

Authentication assurance levels are defined in terms of *organizational* and *technical* factors that characterize the authentication process. Those factors address both the *registration phase* and the (*on-line) electronic authentication phase*, which are two phases composing the authentication process.

Organizational factors, which concern the registration phase, are:

- The quality of the identification process;
- The quality of the issue of the credential;
- The quality of the entity issuing the credential

Technical factors, which concern the electronic authentication phase, include:

- The type and the robustness of a credential (e.g., an ID token);
- The security features of the authentication mechanism in the remote authentication;

Each assurance level describes the degree to which a relying party in an electronic transaction can be confident that the identity information presented actually represents the entity referred to in the identity information. Service providers will have to manage the risk of providing a service to the wrong citizen or user (due to man-in-the-middle attacks, not secure processes of handing out credentials, stolen passwords and so forth). They will have to analyze these risks and map them to an authentication assurance level.

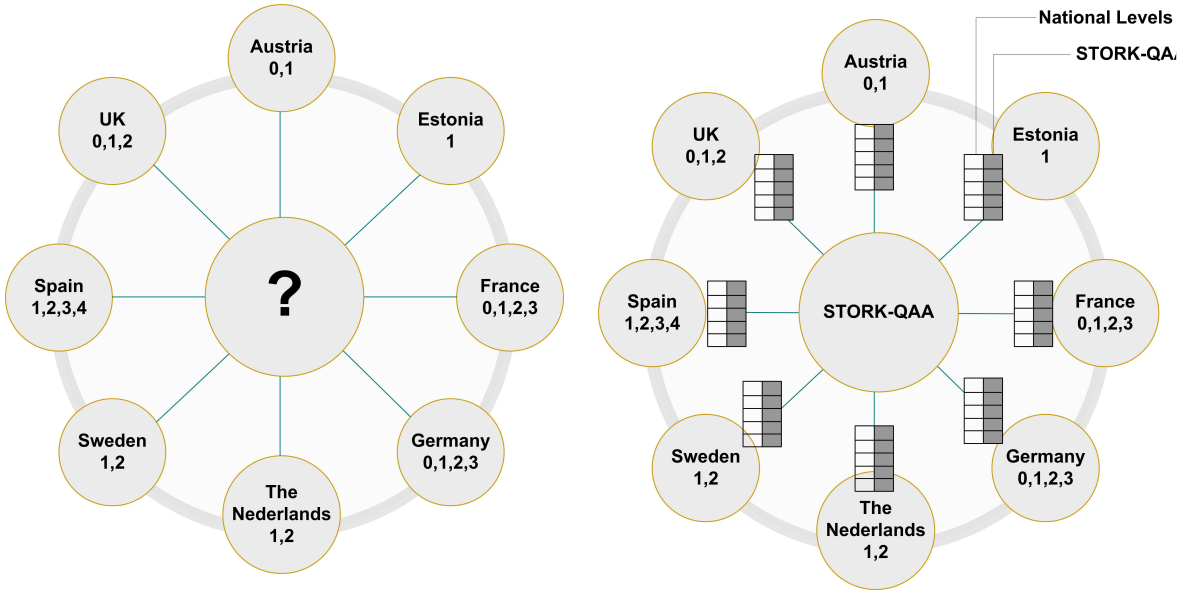
The eID interoperability solution of the STORK project supports four quality assurance levels. In general, levels of eID authentication are classified by the means that are used and the processes via which they are handed out: Smart cards with PKI tend to mean high-end solutions, software certificates are seen as middle-end, and username/password based identification solutions are often considered as low-end. For example, from a process perspective, a software certificate obtained via the Internet without any physical presentation of the owner and without the use of qualified signatures provides less assurance than a username/password combination obtained via a face-to-face verification by the government.

The STORK QAA model focuses on the quality of user identification and authentication. It does not take into account the quality of the STORK infrastructure for communicating eID-credentials and related information. For instance, mapping errors of local to STORK levels and the robustness of the STORK infrastructure against denial of service attacks are outside the scope of this work.

The STORK QAA model updates the IDABC proposal. STORK considers the current need of interoperability of the member states and, as such, discusses and recommends solution that may foster interoperability. It also considers in the model important legal aspects and discusses how they may influence the applicability of the model

In STORK, we have to map the country-specific levels of authentication to the STORK QAA levels as well. It is an explicit objective to have as less impact as possible on existing services. In Figure 1.a the problem is illustrated: there are incompatible definitions of national levels. The STORK QAA levels are defined as a common European understanding for quality of authentication assurance. This solution requires a mapping of local authentication levels (and authentication tokens, Figure 1.b) to the STORK QAA level. Based on the input of the STORK

member states, a mapping of national levels to the STORK QAA levels is described in more detail in Section 3.



a. STORK Problem

b. Solution: define QAA levels and related mappings

Figure 1: Mapping authentication assurance levels.

Most European countries have legislation in place that governs the use of their electronic identities and, sometimes, also the authentication levels. These legal aspects influence the use of electronic identities in cross-border scenarios. Deliverable D2.2 (cf. [2]) of the STORK project contains an extensive analysis of the legal issues of each of the countries present in the STORK project. These are summarised in Section 4 of this report.

Section 5 focuses on the perspective of the service provider, and finally Section 6 summarises the main findings of this report.

Having finished the work the over-all document has been created and sent by the WP2 manager to all WP2 partners and the WP4, WP5 and WP6 work package managers with request for comments. The received comments from UK, Spain, France, Iceland, Belgium, Sweden, Austria, Netherlands and Estonia have been processed and the document has been adapted.

1.5 Risk management

According to the STORK Quality Management plan, each deliverable/task has to follow the agreed quality management process and has to be accompanied by a risk analysis. The following tables comprise the identified risks for this deliverable. According the structure of this deliverable the risks are divided into general risks affecting the whole task 3 of WP2 and risks affecting the individual work items only.

The following table illustrates the template that was used for the risk analysis:

Threat	Description of a potential danger towards the project.
Consequence	Description of the negative effect the threat can have towards the project.

<table>
<tr><td>Measure</td><td colspan="3">Description of the measures that can be taken to prevent a threat from happening or to reduce negative effects.</td></tr>
<tr><td rowspan="6">Chance (C)</td><td colspan="3">Measure defining the likelihood of a threat to happen. The chance is determined as follows:</td></tr>
<tr><td>HH</td><td>Very High</td><td>the threat has very high likelihood to happen (more than 80%)</td></tr>
<tr><td>H</td><td>High</td><td>the threat has high likelihood to happen (from 60% to 80%)</td></tr>
<tr><td>M</td><td>Medium</td><td>the threat may possibly happen (from 40% to 60%)</td></tr>
<tr><td>L</td><td>Low</td><td>the threat has low likelihood to happen (from 20% to 40%)</td></tr>
<tr><td>LL</td><td>Very Low</td><td>the threat has very low likelihood to happen (less than 20%)</td></tr>
<tr><td rowspan="4">Impact (I)</td><td colspan="3">Measure of the negative effect on the project. The impact is determined as follows:</td></tr>
<tr><td>H</td><td>High</td><td>The impact is high; substantial measures are required.</td></tr>
<tr><td>M</td><td>Medium</td><td>The impact is medium.</td></tr>
<tr><td>L</td><td>Low</td><td>The impact is low; few measures are required, usually easily manageable.</td></tr>
<tr><td>Risk (R)</td><td colspan="3">Risk = Chance * Effect, representing the priority. The risk is determined using the following table.
<table>
<tr><td></td><td></td><td colspan="3">IMPACT</td></tr>
<tr><td></td><td></td><td>H</td><td>M</td><td>L</td></tr>
<tr><td rowspan="5">CHANCE</td><td>HH</td><td>HH</td><td>HH</td><td>H</td></tr>
<tr><td>H</td><td>HH</td><td>H</td><td>M</td></tr>
<tr><td>M</td><td>H</td><td>M</td><td>L</td></tr>
<tr><td>L</td><td>M</td><td>L</td><td>LL</td></tr>
<tr><td>LL</td><td>L</td><td>LL</td><td>LL</td></tr>
</table>
HH means very high priority, H high priority, M medium priority, L low priority and LL very low priority.</td></tr>
</table>

Table 1: Risk analysis template.

1.5.1 Identified risks

Table 2 defines general risks that apply for this deliverable.

Threat	Consequence(s)	Measure(s)	Chance	Impact	Risk
Few MS-assurance levels cannot be mapped onto STORK Assurance levels	*Limited eID interoperability between the MS.*	• Review by WP2, WP4, WP5, and WP6 • acceptance of the WP2 results by MS	*M*	*H*	*H*
Most MS assurance levels cannot be mapped onto STORK Assurance levels	*No eID interoperability between the MS.*	• Review by WP2, WP4, WP5, and WP6 • acceptance of the WP2 results by MS	*L*	*H*	*M*
STORK-levels are not adopted in the project	*Delay of the project and this may lead to short term, ad-hoc based solutions for eID interoperability. WP6 may, in the absence of assurance levels, define their own levels for the pilots.*	• Involve all partners and take input seriously in order to achieve consensus • Accept D2.1, D2.3 as project standards • Use these standards in the review process of the results of other Work packages	*M*	*H*	*H*
Member states deliver incorrect or incomplete information	*May result in incorrect mapping of the STORK assurance levels. These member states may not be able to participate in the pilots*	• Review by WP2, WP4, WP5 and WP6 members	*M*	*M*	*M*
MS do not recognize their contributions in D2.3	*May delay the delivery of the assurance level mapping framework for STORK.*	• Review by WP2, WP4, WP5, and WP6 members	*L*	*M*	*L*
Providers do not accept the STORK-assurance levels.	*Limited eID interoperability between the MS. No eID interoperability between the MS.*	• MS take responsibility in this. • Monitoring during the pilot phase	*M*	*H*	*H*
Not all members give	*May result in incomplete mapping*	• Ask them at least 3 times	*M*	*H*	*H*

information.	*of the STORK levels. These member states may not be able to participate in the pilots.*	• Escalate to executive-board			

Table 2: General Risk List.

1.5.2 Materialized risks

The risk that actually materialized was a slight delay in returning feedback on the first draft of the deliverable. The work package leader managed this situation by sending a reminder and by extending the actual deadline for feedback. In December, at the STORK General meeting the first results were presented and another WP2 meeting was held in which the first final draft was discussed. It was then opened for comment for all MS-partners. On the basis of their input, a new final draft was prepared. On the 18th of February the Dutch ministry of the Interior and Kingdom Relations organised a final meeting in The Hague and the last fundamental issues for deliverable D2.3 were discussed. After this meeting all MS-partners were once more given a week for giving their final comments on deliverable D2.3.

1.6 Quality Management

1.6.1 Acceptance criteria

The acceptance criteria used to evaluate the quality of the deliverable are defined considering the following parameters:

- Deliverable - a description of the deliverable.
- Acceptance criterion – a description acceptance criterion.
- Norm – a description of the norm that is applied to measure conformance.
- Process – a description of the process that is used to test conformance.
- Priority – the priority to meet a acceptance criterion (Low = nice to conform to, Medium = important to conform to, High = necessary to conform to).

1.6.2 The process

The following table reports the criteria adopted for deliverable D2.3 and the ensuing results.

Deliverable	Acceptance criteria	Norm	Process	Priority	Checked
Deliverable D2.3, as mentioned in the DoW	• Conform to STORK template	• Template issued by QM on 25-11-2008	*Checked against template.*	*high*	*Yes*
	• Language & Spelling	• English (UK)	*Reviewed by native speaker.*	*high*	*Yes*
	• Each member state in WP2 and WP6 (pilots) are represented	• Use appropriate communication procedures	*Check against sending an*	*high*	*Yes*

	in deliverable D2.3		*e-mail.*		
	• Consistency with description in DoW	• DoW version 1.5	*aligned with DoW.*	*high*	*Yes*
	• Contents is fit for purpose	• DoW version 1.5	*Reviewed by WP2 and MS-partners*	*high*	*Yes*
	• Contents is fit for use	• DoW version 1.5	*Reviewed by WP2 and MS-partners*	*high*	*Yes*
	• Commitment within WP	• DoW version 1.5	*Reviewed by WP2 and MS-partners*	*high*	*Yes*
	• Delivered on time	• Planning for the Work Package	*Discussion of the final draft by WP2, The Hague the 18th of February.*	*High, deadline is 20/02*	*Yes*
	• Content of D2.3 satisfies to the edge conditions for starting WP2.3	• DoW version 1.5	*Reviewed by WP2 and MS-partners*	*high*	*Yes*

Table 3: Acceptance criteria list and results.

2 STORK Quality of Authentication Assurance model

This section describes the STORK Quality of Authentication Assurance model. That means to define the STORK QAA levels and to describe a set of requirements used to determine to which level an authentication solution belongs. STORK QAA levels are described in Section 2.1. The requirements, based on an analysis of the process of giving out credentials and the strength of the authentication token and protocols, are given Section 2.3

2.1 Description of STORK QAA levels

STORK recognizes four QAA levels, numbered from one to four. They are described in the following table:

STORK QAA level	Description
1	No or minimal assurance
2	Low assurance
3	Substantial assurance
4	High assurance

Table 4: STORK QAA levels.

The four levels are similar to the "IDABC authentication levels report" [3]; they are also quite compatible with the "Liberty Identity Assurance Framework" [4]. A four-level scale is used to keep the complexity and the costs to maintain both the authentication information to operate the corresponding processes and the underlying infrastructure manageable. Conversely, it offers sufficient granularity to match the different business requirements with the potential protection mechanisms resulting in a complete coverage of the risks. A larger number of levels is not desirable, as it may lead to a fuzzy distinction between the levels and it may compromise the trustworthiness in the interoperability framework. Similarly, too many QAA levels might confuse the user and consequently might decrease his confidence and trust in the authentication framework and the applications using the framework.

STORK QAA levels are layered according to the severity of the impact of damages that might arise from misappropriation of a person identity. The more severe the likely consequences are the more confidence in an asserted identity will be required from a service provider's perspective to engage in a transaction.

STORK QAA level 1 is the lowest assurance level; it either assures a minimal confidence in the asserted identity or no confidence at all. Identity credentials are accepted without any form of verification. If the subscriber provides an e-mail address, the only check that is performed is the verification of the correctness of the e-mail address. This level is appropriate when negative consequences that result from an erroneous authentication have a very low or a negligible impact. This level suits recognized on-line services implementing either a minimal set of security protection mechanisms or no set at all.

STORK QAA level 2 defines the level used by those services where damage from a misappropriation of a real-word identity has a low impact. Even if the claimants are not required to appear physically during the registration, their real-word identities must be validated and a token issued by a body subjected to specific governmental agreement. Identity tokens must be

delivered with accuracy and security guarantees. Sufficiently robust authentication protocols must be used during the electronic authentication phase.

STORK QAA Level 3 defines the level used by services that may suffer substantial damages in case of an identity misuse. The registration of an identity is processed with methods that unambiguously and with a high level of certainty identify the claimant. The identity providers are supervised or accredited by the government. The credentials delivered are at least soft certificates or hard certificates. The authentication mechanisms used in the remote authentication phase are robust.

STORK QAA Level 4 is the highest assurance level and addresses those services where damage caused by an identity misuse might have a heavy impact. The registration requires at least once (i.e., the very first time of the request but not for a later renewal) either the physical presence of the claimant or a physical meeting with the claimant (e.g., a certificate is requested on-line, delivered at home, and deployed in the hands of the claimant after a physical check of his/her identity). Alternatively, in case of on-line registration, a claimant identity is validated using trusted e-signatures. Annex II of the e-signature Directive 1999/93/EC leaves the details of identity verification to national law. Therefore, level 4 is fulfilled if the national legal requirements for issuing a qualified certificate have been met. Furthermore, the identity provider must be a qualified entity according to the Annex II of the e-signature Directive. The certificates are hard certificates qualified according to the Annex I of the e-signature Directive. The most robust authentication mechanisms are used during the authentication phase.

2.2 Requirements for STORK QAA levels

Each STORK QAA level is defined in terms of a series of *requirements* on relevant authentication *factors*. So we have a set of requirements for STORK QAA level 1, STORK QAA level 2, and so forth. Each requirement defines the functional and technical properties that must be satisfied by a factor to belong to the specified level. The number and the kind of factors, reported in Figure 2, slightly deviates from those defined in the IDABC report [3]. WP2's analysis resulted into a merge of several IDABC factors; new factors were not needed. Organisational factors, which concern the registration phase, are on the left side of Figure 2; Technical factors, which concern the electronic authentication phase, are on the right side of Figure 2.

The requirements on the factors of eID are organized hierarchically. The requirements for a STORK QAA level are constituted by the requirements for the (offline or online) *registration* phase and requirements for the on-line *electronic authentication* phase. The requirements of each of the two phases are a combination of requirements over sub-factors relevant for each of the phases.

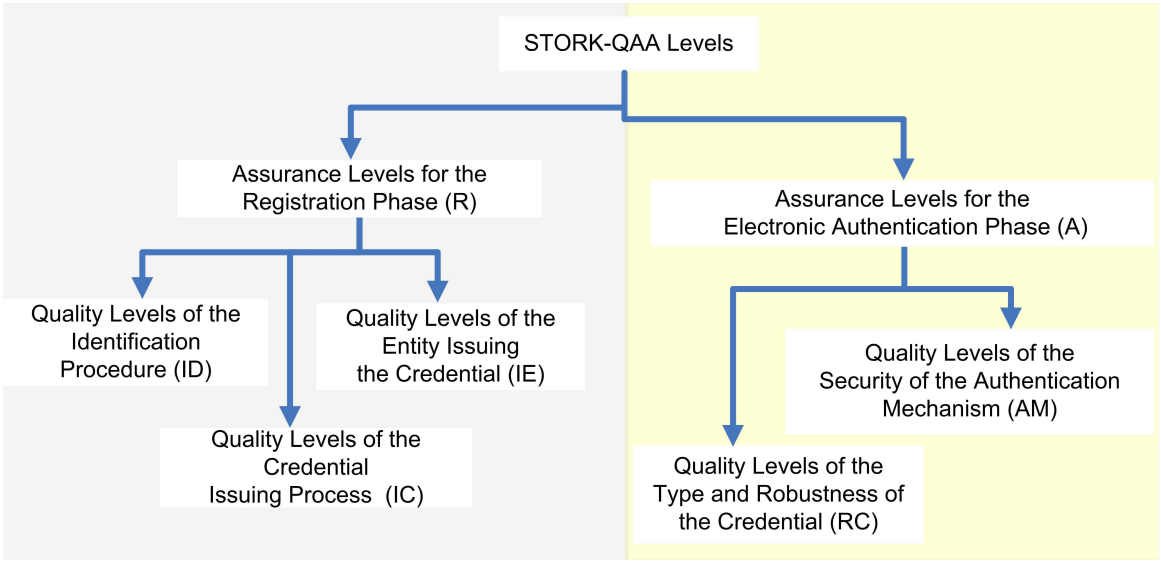


Figure 2: Factors that influence the STORK QAA Levels.

Each STORK QAA level thus is represented by a set of organisational (ID, IC, and IE) and technical (RC and AM) factors and their individual quality level. The lowest value of the individual quality levels will ultimately determine the overall STORK QAA level.

In the remainder of this section we look first at the registration aspects (Section 2.3), then to the authentication aspects (Section 2.4), and finally come up with the resulting STORK QAA level.

The model and approach here can be applied for all registration processes and authentication processes deployed in a member state. It will result in the STORK QAA level for that particular means of authentication.

As the number of national assurance levels can be higher or lower than the STORK QAA, the mapping between the national levels and the STORK QAA levels can mean that more national levels map into one STORK QAA level. It may also occur that the mapping is not exhaustive for certain member states (e.g., some STORK QAA levels cannot be reached by any national level). As consequence of this, some STORK levels may not be achievable by some national authentication solutions and citizens of such member states might not be able to access a service that requires that particular STORK QAA level. A discussion about how to apply the mapping, and an analysis of the specific mapping cases is the topic of Section 3.

2.3 STORK requirements for the registration phase

The STORK QAA levels of the registration phase are defined as a function of the assurance levels of the following quality factors: the identification procedure, the process of issuing identity credentials, the entity issuing the certificate. The requirements extend those in the IDABC proposal for a multi-level authentication mechanism [3] that, in turn, were inspired by the authentication policies of the UK and Germany, the IDABC Authentication Policy, and the NIST Guidelines for registration. The current requirements also look at the e-signature Directive 1999/93/EC [5], in regard of the definition of qualified identity providers and qualified certificates.

2.3.1 Quality of the identification procedure

This is the mechanism through which the citizen/user is identified before an authentication token is given out. The level assigned to the identification procedure depends upon a number of factors:

(i) The physical presence of the claimant in some moment of the identification process:

a. The identification of the claimant does not require his/her physical presence at all. In other words there is no physical meeting with the claimant ever.

b. The identification of the claimant requires a physical meeting with the claimant during the registration. This must happen at least once (e.g., it may be not required for a renewal).

c. The identification of the claimant requires a physical presence when the certificates is delivered to him/her (e.g., the claimant may register on line, but must be present when the certificate is delivered to him/her). This must happen at least once (e.g., it may be not required for a renewal)

(ii) The quality of assertions about the identity of the claimant:

a. Single assertion of data related to the claimant that is not necessarily known by the claimant only (e.g., her/his name, the date of birth). This does *not* necessarily result in a unique identification.

b. Multiple assertions of data related to the claimant that are not necessarily known by the claimant only (e.g., her/his name, the date of birth, residential address). These must result into a unique identification.

c. Assertions that at least refer to some unique piece of information that only the claimant is assumed to know (e.g., his/her social security number, his/her passport number) and that can be checked against some official register. These do result in a unique identification.

(iii) The validation of the assertions given by the claimant about his/her identity, according to the following cases:

a. The validation is limited to a verification of an email address, if an e-mail is provided. Otherwise no verification is performed.

b. The validation of an assertion is performed by cross-referencing the provided assertions with an official identity source or identity database from a neutral and trustworthy source such as a bank, an insurance agency or a government department.

c. The validation requires the assertion to be signed with a non-qualified digital signature.

d. The validation requires the exhibition of a physical and official government identity document such as an identity card, a passport or a driving license which, at least, contains a photo and/or signature.

e. The validation requires the assertion to be signed with a digital signature which is verified by a Certificate Service Provider (CSP) before issuing the token/credential.

The following table shows the Levels for the Quality of the Identification Process (ID1 - ID4). They correspond to the amount of requirements that they satisfy.

Requirements	Quality Levels of the Identification Procedure			
	ID1	ID2	ID3	ID4
• *Physical presence*: not required, i.e. of type (i.a). The registration is on-line • *Quality of assertion:* of at least type (ii.a) • *Validation of assertion:* of at least type (iii.a)	•			
• *Physical presence*: not required, of type (i.a) • *Quality of assertion:* of at least type (ii.b) • *Validation of assertion:* of type (iii.b)	•	•		
• *Physical presence*: required, of type (i.b) • *Quality of assertion*: of at least type (ii.b) • *Validation of assertion:* of at least type (iii.c)	•	•	•	
• *Physical presence*: not required, i.e., of type (i.a). The registration is on-line • *Quality of assertion:* of type (ii.c) • *Validation of assertion* of at least type (iii.d)	•	•	•	
• *Physical presence*: required, i.e., of at least type (i.b) • *Quality of assertion:* of type (ii.c) • *Validation of assertion:* of at least type (iii.d)	•	•	•	•

Table 5: Quality levels of the identification procedure.

2.3.2 Quality of the identity issuing process

The second registration factor concerns the process via which an identity token or credential is issued. The quality of an issuing process depends upon whether the delivery happens via e-mail or via surface mail, and upon whether the token is delivered as one piece of information or as separated pieces that must be combined later.

The higher the quality of the issuing procedure, the stronger the binding between the claimant's claimed identity and his real-life identity in the successive electronic authentication phase. The highest level (limited to the issuing process) is reached when the delivery is conducted in the physical presence of the claimant. Note that in order to obtain an highest level in the overall registration phase the delivery in person must be associated with the highest identification process; this requires that the identity of the receiver is validated using an official government identity document (either at the location of the issuing party, or by authenticated delivery at a selected address).

The following table defines the minimal requirements for each level of the issuing procedure.

Requirements	Quality Levels of the Credential Issuing Process			
	IC1	IC2	IC3	IC4
The credential is obtained without any form of verification.	•			
The credential is obtained with light-weight verification of the claimant's identity credentials (e.g. name and/or address). The following examples illustrate this type of credential issuing: • Username and password are sent out by two separate mailings, at least one of which must be by surface mail (not e-mail) to the address of the claimant as shown in an official government identity database in which the physical address was registered. • The credential is downloaded directly by the claimant following the registration procedure. The downloading happens by providing a link which was sent to an e-mail address communicated by the claimant during the registration process; in this case, the e-mail link must expire after an appropriate time (e.g., 24 hours).	•	•		
The credential is obtained with a medium verification of the claimant's identity credentials (e.g. name and/or address). The following examples illustrate this type of credential issuing: • The credential is sent out by registered mail after prior validation of the claimed address against an official identity database in which the physical address was registered. • The credential is downloaded on the Internet after the request assertion is signed by the claimant with a qualified signature according to the terms of the eSignature Directive and verified by a CSP. Immediately after the verification, the credential is generated on the fly by the CSP and downloaded at the claimant's browser. • The credential is downloaded directly by the claimant after entering a private password which was given physically to the claimant during the course of a registration of at least level 3 (see Table 3).	•	•	•	
The credential is obtained with a strong verification of the claimant's identity credentials. The following examples illustrate this type of credential issuing: • The credential is given to the claimant in person after validation of the identity. • The credential is sent to the claimant and activated after validation of its identity (e.g. via physical registration).	•	•	•	•

Table 6: Quality levels of the issuing process.

2.3.3 Quality of the entity issuing the identity credentials

The third aspect that influences the quality assurance of the registration phase is the quality of the entity that issues the identity credentials (certificates, passwords, tokens). Such an issuing entity could for instance be a traditional or electronic identity provider or a Certificate Authority (CA).

Whilst the issuers of traditional identification documents (e.g., passports and identity cards) are usually public governmental bodies, the issuers of digital identity tokens can be either entities of the public sector or third parties. The role of the certification authority and the identity provider is usually played by the same physical entity, which we call the certification service provider.

We make a distinction between entities that are qualified according to what is stated in the Annex II of the Directive 1999/93/EC and those that are not; only the qualified entities can offer the highest level of assurance.

Among the non-qualified entities, we distinguish between entities that apply mechanisms that are approved, supervised, or accredited by the government and entities that run mechanisms which do not benefit from a governmental supervision, approval, or accreditation (e.g. banks).

Qualified entities are those that meet the requirements of Annex II of the EU Directive 1999/93/EC [5]. A qualified entity is allowed to deliver qualified certificates (compliant with the constraints expressed in Annex I of the same directive; see also part II of deliverable D2.2 [2][1]). Another document of interest here is the Policy requirements for certification authorities issuing public key certificates" (ETSI TS 102 042) [6]. This latter document is relevant for all PKI installations in Europe and concerns all aspects of the registration process in STORK QAA definition.

Note that some of the requirements mentioned in the directive describe the obligations that must be fulfilled when, for example, the certification service provider verifies the identity of the subscriber or when it generates the identity token. Therefore there is overlap between the requirements requested for a certification service provider to be certified (according to the directive) and the requirements that are contained in the STORK model. This overlapping is perfectly licit. For example, the obligation (d) in Annex II of the Directive 1999/93/EC states that "*the certification authority must verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to whom a qualified certificate is issued.*" This obligation overlaps with the requirement for the registering process (Section 2.3.1). Because both requirements are associated with the highest level it is still possible to have an overall STORK level four at the end of the evaluation. Differently, if a registering process of level four is performed by a non-qualified entity it is not possible to reach an overall STORK-level four, because the assurance level of non-qualified entities is less than four. This situation matches perfectly the intention of STORK where technical and legal aspects contribute to the specification of a quality of assurance level.

Another factor that should be taken into account is the absence or presence of a strategy to retain the facts occurring during the registration procedure. A log of the registration data makes it possible, for example, to perform an investigation in case of fraud. The existence of a retention mechanism is one of the requirements contained in the EU Directive 1999/93/EC [5]. Item (i) of Annex II of the directive says that "*record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done*

[1] We are aware that this Directive is meant for digital signatures only and not for authentication purposes. Nevertheless the Directive offers a definition of qualified certificates that can be used for qualifying user authentication as well.

electronically". Issuing entities that operate in accordance with the Directive thus also meet the retention requirement and enjoy the highest level of assurance. There must, however, be agreement about the meaning of "*an appropriate period of time*". This may be application or member state specific. Entities that do not operate in accordance with the Directive may still have retention mechanisms in place but will never obtain a level of assurance higher than 3.

Requirements	**Quality Levels of the Entity Issuing Credentials**			
	IE1	**IE2**	**IE3**	**IE4**
No government agreement (no supervision, no accreditation) mechanism is in place.	●			
With government agreement.	●	●		
With government accreditation or supervision.	●	●	●	
Qualified according to Annex II of the Directive 1999/93/EC e	●	●	●	●

Table 7: Requirements regarding the quality of the entity issuing identity credentials.

2.3.4 Assurance levels for the registration phase

The table below aggregates each of the registration process aspects into a single quality level for the overall registration phase.

	Quality assurance levels for the registration phase			
	R1	**R2**	**R3**	**R4**
Quality of the Identification Process (Table 5)	ID1	ID2	ID3	ID4
Quality of the Credential Issuing Process (Table 6)	IC1	IC2	IC3	IC4
Quality of the Entity Issuing the Credential (Table 7)	IE1	IE2	IE3	IE4

Table 8: Aggregated quality levels of the registration phase.

The overall level for the registration phase consists of a set of levels corresponding to the different registration process aspects. The general rule is that the overall registration process level can never exceed the required levels of individual aspects.

2.4 STORK requirements for the electronic authentication phase

In the electronic authentication phase, the proof of identity supplied by a claimant (i.e., an identity token, a credential) is verified for its authenticity. The quality of this phase depends on factors like the type of the identity token that is used, the remote authentication protocol adopted in the authentication check, and the mechanism used to communicate the result of the remote authentication to the claimant.

2.4.1 Types and robustness of the identity credential

The first factor that influences the quality of assurance of the electronic authentication phase is the type of the electronic identification token that is provided as proof of possession. The token types that we consider in STORK are as follows:

Username/Password or PIN: is a character string, expected to be memorized and kept secret by the claimant. This kind of token is used in many member states, especially for low-risk services. Often, a particular username/password combination, or the PIN code, is associated with and allows use of a set of services. For example, some member states have dedicated portals that generate and issue this kind of tokens to citizens and that handle the authentication of citizens for a number of services. The username part of the combination can either be self-chosen by the claimant or generated by the identity provider. Since it is public, it does not have an impact on the authentication level. For the password or PIN part this is different; there is a different level associated to claimant chosen or automatically generated passwords or PINs.

Password list: Is a personal soft token (paper list) that the claimant possesses. A list contains PIN codes often in combination with a static password or PIN within the authentication system.

One-time password device: Is a personal hardware device that generates a “one-time” password that is valid for only one authentication session. In certain cases the one-time password is generated as a timestamp, by using a cipher algorithm that combines the current time and a secret seed stored in the device. In other cases, a dedicated reader device combines a symmetric key stored on a personal hardware device (e.g., a card) with a nonce. The nonce can be current time, a counter generated on the reader device or, if the device has input capabilities, a challenge sent from the verifier. The generated one-time password that is typically displayed on the reader device, is communicated (e.g., manually digitized on the portal of the service, automatically uploaded on the portal, or sent via SMS) to the remote service.

Soft certificate: is a cryptographic key that is typically stored on a disk, USB stick or some other media. Authentication is accomplished by proving possession and control of the key. Usually the soft certificate is encrypted under a key derived from a password known only to the user; therefore the password is required to activate the certificate.

Qualified Soft certificate or equivalent: is a soft certificate whose technical features are compliant to the requirements laid down in Annex I of the EU Directive 1999/93/EC [5]. Even though there are differences in the transpositions of the Directive into national legislation there is also much common ground in how the certificates are created and in their legal effects. In this definition we also include those soft certificates that are issued by the national government (e.g. Belgium and Estonia) with exactly the same processes as the qualified ones, i.e. normalized certificates.

Hard certificate: is a smartcard or similar media that contains a protected cryptographic key. Authentication is accomplished by proving the possession of the device and control of the key.

Qualified hard certificate or equivalent: is a hard certificate whose technical features are compliant to the requirements laid down in Annex I of the Directive 1999/93/EC [5]. Even though there are differences in the transpositions of the Directive into national legislation there is also

much common ground in how the certificates are created and in their legal effects. In this definition we also include those hard certificates that are managed by the local government with exactly the same processes as the qualified ones.

A specific quality aspect that is of relevance for identity tokens is their freshness: how often does the issuing entity updates its revocation lists. Issuing entities should express the revocation list update frequency in their certification statement. The quality of the freshness of the identity tokens is part of the quality of the issuing entity and therefore addressed in Annex II of the Directive and therefore tackled in Section 2.3.3.

The following table shows the mapping of token types to quality levels. Criteria for rating the tokens are their robustness against copying, the use of multiple independent channels and those mentioned in the Directive.

Requirements	**Quality Levels of the Type and Robustness of the Credential**			
	RC1	RC2	RC3	RC4
Password or PIN-based token, chosen by the claimant or automatically generated but not conform common guidelines for strong passwords or PINs (e.g. insufficient length, no mixture of characters, reused, etc.) and therefore vulnerable to guessing or dictionary attacks.	●			
Password or PIN-based token, chosen by the claimant or automatically generated but conform common guidelines for strong passwords or PINs (e.g. sufficient length, mixture of characters, not reused, etc.) and therefore not vulnerable to guessing or dictionary attacks.	●	●		
Soft certificates or one-time password device token.	●	●	●	
Qualified Soft certificates according to Annex I of Directive 1999/93/EC.	●	●	●	
Hard certificates.	●	●	●	
Qualified Hard certificates according to Annex I of Directive 1999/93/EC.	●	●	●	●

Table 9: Quality levels of the identity tokens.

Note that if a certificate is a qualified certificate, then the proof is stronger (assurance level is higher) than for other advanced certificates because qualified certificates are verified in a more tightly controlled process. Furthermore, the used encryption algorithms should provide sufficient protection against forgery using currently available technology (see also Annex III of the e-signature Directive 1999/93/EC).

2.4.2 Security of the authentication mechanism

The level of trust that can be posed on a remote authentication mechanism depends upon its security robustness. The robustness of the authentication mechanisms is here judged with respect

to the most serious threats that concern authentication: the identity theft. In most cases, a criminal needs to obtain personally identifiable information or documents about an individual in order to impersonate him/her. This can be done in different ways among which, for example retrieving information from redundant equipment, like computer servers that have been disposed of carelessly, e.g. at public dump sites, given away without proper sanitizing etc, or doing research on the victim in government registers, internet search engines, or public records search services., or eventually browsing social network (e.g., MySpace and Facebook) sites, online for personal details that have been posted by users.

These kinds of attacks are basically social engineering, a serious discipline who watches at the user as the weakest point in a security system. Our analysis of the assurance levels of the remote authentication will focus to the threats that come from attacks directed only to the authentication protocol itself. In this case identities can be stolen via a list of attacks against the remote authentication procedure. This can happen via the following types of attacks:

(1) Guessing is a simple attack where a malicious entity tries to guess a secret used in a communication (e.g., an encryption key, a PIN). This attack works in cases where the secret is weak. For instance a simple password can be easily guessed using dictionaries.

(2) Eavesdropping is an attack that consists in observing the messages passing through a communication channel, where for example an authentication protocol runs. The messages are stored usually for performing some off-line analysis of the information, used for launch successive attacks; for example eavesdroppers generally attempt to obtain tokens to pretend to be the claimants.

(3) Hijacking is an attack that consists in taking over an already authenticated session by an attacker and to learn sensitive information.

(4) Replay is a form of attack where a malicious entity repeats or delays previously intercepted messages in order to gain access to sensitive information.

(5) Man-in-the-middle is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones.

There is direct relationship between the assurance level of the authentication protocol and the robustness against these kinds of attacks. Anyhow being robust is a property that can be checked only with respect to the current status of the technology. Attacks and defenses evolve mutually in time. Thus in the following table we classify an authentication remote procedure according their provable (in the current technology and knowledge) security or proved insecurity against the previously mentioned attacks. Proved insecure means that it is known that the protocol to be vulnerable to the attack. Provable security is a delicate terms. It may refer to the robustness *de facto* as in the case, for example, of mechanisms that have been in use since quite a time without that an attack was reported. Alternatively, provable secure means formally secure, when studies and tests on the security of the mechanism have been conducted all with positive outcomes. In this context, it must be noticed that certain kind of attacks, like the hijacking and the man-in-the-middle attacks, are very difficult to detect. Moreover, when we say that a mechanism offers protection (or strong protection) against an attack, we mean that with respect to the current technology, the mechanism implements defenses that are recognized to be robust against to that specific attack. So for example a randomly generated password longer than 8 characters and with alpha and numerical characters is known to be robust to guessing and dictionary attack. This implies that only the 4th level can be described in formal terms. For the other levels a self

assessment will have to take place. We refer to the evaluation assurance levels (EAL) of the Common Criteria for guidance on assigning the appropriate levels [7].

The following table summarizes the requirements for the authentication mechanism assurance level.

Requirements	Quality Levels of the Security of the Authentication Mechanism			
	AM1	**AM2**	**AM3**	**AM4**
Authentication mechanisms that offer little or no protection against the above-mentioned attacks.	●			
Secure authentication mechanisms that offer some protection against the above-mentioned attacks.	●	●		
Secure authentication mechanisms that offer protection against most of the above-mentioned attacks.	●	●	●	
Recognized secure authentication mechanisms that offer protection against all of the above-mentioned attacks. Comparable with EAL4+ or higher of the Common Criteria.	●	●	●	●

Table 10: Quality levels of the authentication mechanism.

2.4.3 Assurance levels for the electronic authentication phase

The table below aggregates the various factors that determine the quality levels of the electronic authentication process. The general rule is that the overall authentication process level can never exceed the level of an individual aspect. Again, this implies that the overall STORK QAA level can never by higher than the lowest value of one of the individual electronic authentication aspects.

Aspects relevant for electronic authentication	**Quality assurance levels for electronic authentication phase**			
	EA1	**EA2**	**EA3**	**EA4**
Type and Robustness of Identity Token (Table 9)	RC1	RC2	RC3	RC4
Security of Authentication Mechanism (Table 10)	AM1 - 3	AM1 - 3	AM1 - 3	AM4

Table 11: Aggregated quality levels for the electronic authentication process.

2.5 STORK QAA levels

Using the same techniques as used for the electronic authentication process (Section 2.4.3) and the registration process (Section 2.3.4), we can now compute the overall STORK QAA level. This computation is based on the common paradigm that security is as strong as the weakest link. Therefore the overall STORK QAA level is determined by the lowest assurance level for registration and for electronic authentication. Table 12 below summarizes the results.

		Assurance Levels for Electronic Authentication phase			
		EA1	EA2	EA3	EA4
Assurance Levels for Registration phase	RP1	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1
	RP2	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 2	STORK QAA Level 2
	RP3	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 3
	RP4	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 4

Table 12: STORK Quality of Authentication Assurance levels.

Now that we have defined the framework for assessing STORK QAA levels, the next step is mapping them onto authentication quality assurance levels that are recognized by the member states. This mapping will be explained in the next chapter.

3 Mapping existing mechanisms on the STORK QAA levels

The STORK approach is that service providers should be allowed to use the nationally recognized assurance levels for authentication. To ensure interoperability with other member states, these national levels must be (automatically) translated into corresponding STORK QAA levels. This is depicted in Figure 3, below.

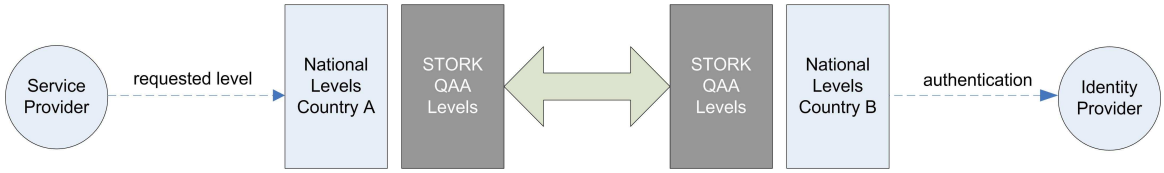


Figure 3: Applying the mapping.

This corresponds to the following scenario:

1. A foreign user requests access to a local service offered by a service provider. The service provider expresses its authentication requirements in terms of a locally, i.e. nationally, recognized assurance level.
2. This local QAA level is mapped onto a STORK QAA level and subsequently from the STORK QAA level onto a level that is recognized by the foreign user's member state. An appropriate authentication request in that member state is created.
3. The foreign user is authenticated and an assertion is created corresponding to the foreign local assurance level which, on its turn, corresponds back to a STORK QAA level.
4. This STORK QAA level links also back to the compatible assurance level of the service provider's member state, which eventually received the assertion of authentication with the desired quality of assurance level.

The STORK QAA level framework thus allows for mapping locally accepted levels to the levels of the user's member state. For example, if we assume that a citizen of a member state asks for a foreign service that requires authentication at a certain local level then the mapping is used to understand which authentication solutions of the country of origin of the citizen can be used to authenticate that citizen. The STORK QAA level of this authentication solution must be compliant with the STORK QAA level requested by the service provider. Here, "be compliant" means possessing the same or a higher STORK QAA level.

This section discusses how to apply such a mapping (in section 3.1); and subsequently, it discusses the implications of mapping of national and STORK levels onto each other for the middleware and the proxy models (from section 3.2 to section 3.4).

3.1 Mapping the national eID levels to STORK QAA levels

The following Table 13 presents a proposed mapping of the national authentication levels of each member state to the four STORK QAA levels as defined in the previous chapter. This table is based on an inventory of all member states' authentication solutions described in STORK deliverable D2.1 [1]. The authentication solutions adopted by the member states (analyzed in deliverable D2.1) have been associated with STORK QAA levels by applying the scheme described in Section 2; it does not include the legal implications yet; these will be addressed in Section 4. The cells of the table contain the names of the levels (*e.g.*, "Level 1", "Level 2", etc.) as defined by the member state.

	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 4
Austria				Level 1
Belgium	Level 1	Level 2	Level 3	Level 4
Estonia		Level 1 (username and rotating passwords)	Level 1(one-time password token)	Level 1(with ID-card or Mobile ID)
France			Level 1	Level 2, Level 3
Germany	Level 0	Level 1	Level 2	Level 3
Iceland	Level 1	Level 2	Level 3	Level 4
Italy		Level 1 (PIN + password)		Level 1 (digital certificate in smart card)
Luxembourg				Level 1, Level 2
The Netherlands		Level 1	Level 2	
Portugal		Level 1	Level 2	Level 3
Slovenia	Level 1		Level 2	Level 3
Spain	Level 1	Level 1	Level 2	Level 3
Sweden			Level 1	Level 2
UK	Level 0	Level 1	Level 2	

Table 13: Mapping of national assurance levels to STORK QAA levels.

The definition of the scheme that maps national levels to STORK QAA levels is the first step towards interoperability. However, the STORK QAA mapping, as reported in Table 13, hides a wide record of cases that must be clearly addressed and analyzed. The key issues are discussed below.

- *Some member states (e.g., Austria and Luxemburg) have only authentication assurance levels that correspond to the STORKS's highest level*. Service providers of those member states may be inclined to authenticate citizens with the highest level of assurance: Level 4 in STORK terminology. This inclination, however, implies that many citizens of other member states can never access their services. For these citizens, other more expensive solutions need to be

provided. Furthermore, all European citizens are obliged to use STORK QAA level 4 authentication tokens to access any service in those member states. This may lead to a situation where a citizen will be asked for a smart card authentication for a very basic service. Service providers should therefore make a risk assessment regarding their services and decide for themselves if the highest level is the best choice. Less critical services may be rated with a lower assurance level thereby allowing more citizens access. This implies that service providers of such member states should have knowledge about other levels, and preferably STORK levels, as well. If service providers are given the option to conform to the STORK QAA framework instead of a national assurance framework, then they must express what type of assurance levels they adhere to (STORK and/or national). Otherwise, mapping may go wrong (see also Section 3.4 and Section 5).

Recommendation: Service providers may consider supporting assurance levels that are appropriate for the service, even if their home member state only support high levels of assurance.

- *Some member states (e.g., The Netherlands and UK) do not have authentication solutions that map to the STORK level 4*; therefore, citizens from those countries may not have access to a service of another member state if the service requires an authentication level classified STORK QAA level 4.

Recommendation: Member states that currently do not offer STORK QAA Level 4 eID solutions may consider offering solutions in the near future that satisfy the requirements for STORK QAA level 4.

- *Some member states (e.g., France and Luxembourg) have multiple authentication solutions with different national assurances but with equal assurance in the STORK model*. This means that those national levels are equivalent from the STORK's point of view. In general, this is not a problem but attention is required when the mapping is applied, from STORK levels back to national levels. For example, let us assume that a French service provider demands a Belgium citizen to authenticate himself with a French assurance level 2; this maps to STORK level 4. Then the Belgian citizen can be authenticated with his national identity card, which has Belgian assurance level 4 that, in turn, is compatible with STORK QAA level 4. The authentication assertion (reserved for the French service provider) is then mapped back from STORK level 4 to either the French assurance level 1 or French assurance level 2 (i.e., both levels are possible according to the mapping). *If the latter mapping is applied without any additional intelligence*, the French service provider may assume that the citizen was authenticated with a French assurance level 1 (i.e., the service provider chooses the lowest) and, consequently, it may deny the access to the service. Such situations must be avoided, for example, by choosing to map back to the requested level or always to map back to the highest level (in case of multiple possibilities).

Recommendation: the translations between STORK QAA levels and national levels must be carefully designed to prevent unwanted degradation of assurance.

- *Some member states (e.g., Italy and Estonia) have several authentication solutions with equal assurance with respect to the national level but with different assurances in the STORK model*. Estonia, for example, defines only one level (indicated in the table as "Level 1") but three levels are used in practice; if we stick to the level name (e.g., "Level 1") it seems that one national level is mapped onto different STORK QAA levels.

Recommendation: Member states without a formal assurance level, or with a single national level mapped to multiple STORK levels, require a solution that is able to diversify the assurance levels indeed hidden within a single definition, preferably in a way compliant to the STORK. This can be realized at the protocol level or by the adoption of the STORK model. Both solutions have implications (see Section 3.3 and Section 5, respectively).

In the following.sections we will discuss design aspects. The first subsection focuses on architectural issues; the next subsection on potential issues regarding the use of SAML for assertions.

3.2 Mapping to the PEPS and middleware approach

Two solutions for the communication of identity credentials are being discussed in STORK: the proxy and middleware. Each solution may provide mapping of assurance levels (from national to STORK and *vice versa*) at different locations.

In the *proxy approach*, a service provider (SP) always contacts its own national (i.e., local) Pan European Proxy Service (PEPS) and requests for credentials including the proper authentication assurance level. The local PEPS proxies the request to a remote PEPS of another member state that on its turn forwards it to the IDP. The IDP authenticates the user, and returns a claim/assertion to the PEPS. This PEPS forwards the claim/assertion to the local PEPS that subsequently forwards it to SP. The SP uses the assertions to grant or to deny the claimant access to the service. The proxy approach allows the SP and the local PEPS of the same member state to use their national authentication assurance levels. Only the local PEPS, while communicating with the remote PEPS or the remote IDPs of other member states, has to map a national assurance level into a correspondent STORK QAA level, which is understood by the remote PEPS or by the remote IDPs. Of course, all Member States need to deploy such a proxy service.

The *middleware approach* is specifically suitable for smartcard use and provides the necessary IDP discovery and user authentication in a transparent manner. This makes it easier to deal with in the situation of multiple IDPs per member state, as the middleware relies on a public-key infrastructure to validate the information; moreover, it requires a distributed mapping of authentication assurance levels onto each other. Either the IDP has to provide European-wide standardised assurance levels or he has to do the mapping himself. The middleware exploits the fact that smartcards contain particular security tokens and identity attributes that are securely transferred to the SP. However, not all attributes required for authorisation may be present in the card; in those cases, either another card must be used, or an Attribute Provider (AP) may need to be accessed as well, requiring again a proxy-like model between the SP and AP.

Likely, both models will be implemented by WP5 but independently of the outcomes of the discussion, both models will be able to deal with STORK QAA levels.

3.3 Mapping to SAML

The STORK QAA levels somehow need to be communicated between all involved entities. SAML2.0 has the potential to provide this functionality. SAML is a framework for exchanging security and identity assertions in a federated environment. Very likely SAML will be chosen in STORK as the common identity management framework. However, a recent IDABC report [8] on the mapping of IDABC Authentication Assurance Levels to SAML2.0 shows that there are several important gaps in mapping SAML Authentication Context directly to IDABC concepts, which could be filled by using SAML's extension mechanism. Since the STORK QAA model is based upon IDABC, it may face similar problems regarding SAML2.0. This is particularly the case for the situation that multiple STORK QAA levels correspond to a single national level (e.g., Estonia). SAML2.0 then just lacks the expressiveness to describe the possible authentication solutions and configurations corresponding to a certain assurance level. To solve the problem, IDABC proposes the use of links to human-readable policy documents. In this case, each STORK QAA level (one of the four levels) would be characterised by a URI attached to a SAML token which contains a reference to the external human-readable documentation that defines the STORK QAA level in a natural language format.

3.4 Compliance and supervision

One important topic of discussion is about who is going to supervise the application of the STORK QAA framework. It is advisable that some authority is in charge of facilitating the adoption of the framework, and as such, defines control-strategies to check whether the framework is applied according to its principles. In case multiple versions of the framework exist, the authority is also entitled to define and interpret the guidelines so that all the member states adopt the same correct version. For the pilot, this role could perhaps be delegated to a board of members of the Executive Board. The Executive Board will have to discuss this at their next meeting.

Another important aspect is auditing. The implementation of the framework must allow auditing procedures to promote adherence to the framework. The current framework description allows for new eID solutions (of new member states) to be evaluated and assigned a proper level. This process, however, should be carefully monitored by an entity that is responsible for the overall quality and integrity of the STORK framework. Likely, this entity should have sufficient authority to solve sensitive liability issues that may occur between member states. In order to reach the desired interoperability, contracts between member states should perhaps be signed. These contracts must specify the quality of service that member states can expect from each other. Again, all of this has to be discussed at the Executive board.

4 Legal implications and solutions

This section describes the legal implications of cross-border use of national authentication solutions on the STORK QAA model. It also suggests possible solutions to overcome the legal implications identified in deliverable D2.2 [2] (see also Figure 4).

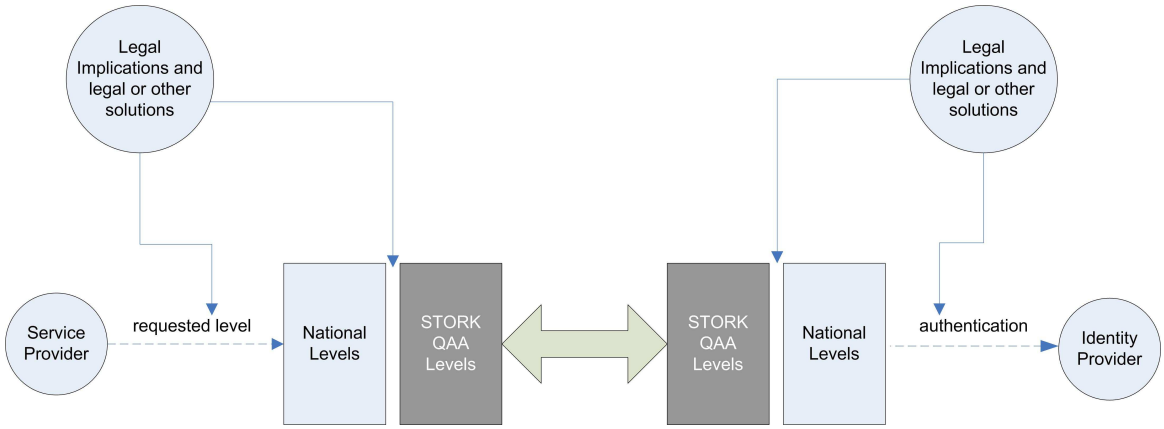


Figure 4: Legal implications in the framework.

4.1 Analysis of the legal implications

Deliverable D2.2 Legal Implications of STORK mentions two major legal implications for the pan European eID interoperability [2]:

1. The legal status of the digital certificates used for authentication purposes.
2. The use of identifiers across member states.

Both, however, have a minor impact on the overall STORK QAA model itself but have a major impact on its usefulness. We explain this in the following sections.

4.1.1 Use of certificates for authentication purposes

A certificate is an electronic attestation that links signature-verification data to a person and confirms the identity of that person. Certificates therefore are to authenticate a person. Certificates can be *qualified* and *non-qualified*. A qualified certificate is a certificate that meets the requirements written in Annex I of the e-Signature Directive [5] and is provided by certification service providers who fulfil the requirements reported in Annex II of the directive[2]. A non-qualified certificate is a certificate that does not meet the requirements of this Directive.

Qualified certificates are given significant legal effect because they can be trusted on the basis of the certificate issuing process. Qualified certificates provide a higher assurance level than other (advanced) certificates because they are issued in a more tightly controlled process. Moreover, users of qualified certificates may expect to be certain that a verified certificate meets particular quality requirements regarding content and validity; hence, CSP issuing qualified certificates have a certain liability as described in article 6 of the e-Signature Directive. These observations are

[2] See Article 2 (9) and (10) of directive 1999/93/EC.

taken into account in the STORK QAA model: the use of qualified certificates is rewarded with a level 4 assurance level, whereas the use of non-qualified certificates is level three rated. Whether a member state implements qualified certificates in their eIDs depends on a weighing of costs involved (issuing qualified certificates is expensive) against the necessity of higher levels of trustworthiness. As the analysis of the country reports shows [2], the various member states reach different conclusions. Some countries use qualified certificates for their eID's, others don't. Though this may lead to difficult liability issues because the liability in the case of qualified certificates rests on the CA that issued the certificate and this is more complicated for non-qualified certification-service providers, this is independent of the STORK QAA model.

4.1.2 Identifiers

Many eIDs contain identifiers that are based on, or are equal to, national identification numbers (e.g., Estonian Personal Identification Code, Dutch BurgerSeviceNumber, Spanish DNI number). In most countries, the use of these numbers is restricted and regulated by law. This means that they cannot be processed in across-border eGovernment interactions, which includes storage. The Dutch BSN, for instance may only be used by authorized entities that are listed in the Act on the Citizen Service Number, all of which are within the Dutch jurisdiction, which limits the use of the BSN to Dutch (e)Government interactions.

In some member states, identification numbers may be processed only if the data subject gives his explicit consent (e.g., Estonia, Italy, and Spain). In these cases, the identification numbers may also be processed (and stored) by relying parties in other member states if the claimant agrees to the processing.

Germany does not have national identity numbers, but instead uses combinations of other attributes such as name and date of birth as an identifier for individuals. Within certain public sectors, such as taxation, national identifiers do exist, but these may only be used within the context within which they are created, which again prevents using the numbers as identifiers in pan-European eGovernment services.

In Austria, the base identifier (sourcePIN) may not be used at all. Instead, derived ssPINs can be used but only within Austria.

D2.2 shows significant differences in the STORK member states regarding (national) identifiers and the restrictions on the use of these numbers. Some STORK members have expressed a need to be able to store identifying data of foreign claimants in the eGovernment transaction process. The brief overview above shows that such identifying data cannot be identical to the national identifiers in many member states.

4.2 Solution directions

Two legislative issues thus can be identified that affect the use of eID interoperability between EU member states: the use of persistent identifiers is not allowed in several member states (e.g. Germany) and several national identifiers (e.g. BSN in The Netherlands) may not be used outside the member state.

Several solutions directions are possible to realize lawful eID interoperability in Europe. This section describes them.

4.2.1 Opaque and transient identifiers

Obviously, the provisioning of persistent user identifiers to service providers and relying parties is not always an option. In this case, identifiers that are used by the identity provider and service provider are directly linked to each other without any obfuscation. Alternatively, identifiers could

be indirectly or transiently linked. Indirect linking provides a pseudonym for a user or a completely new persona to the target site, i.e. service provider or relying party. The pseudonym is an identifier that is different to the primary user identifier established with the source site, i.e. identity provider, but is fixed in time for the same persona and the same target site. For instance, a one-way hash function of the user's national identifier can perhaps be used and still be in accordance with national legislation. Indirect linking may be used to implement pseudonymity [9]. Transient linking does not provide an identifier or provides a temporary anonymous handle that is valid for a single session or a part of session. Transient identifiers may be completely anonymous or may contain service provider or country specific elements. The latter elements may be useful for efficient service discovery and additional attribute collection but has privacy drawbacks. Transient linking is typically used in anonymity scenarios [9].

In addition to the user identifier, the source site or identity provider may also provide other user attributes. These attributes for instance may be personal data (first name, last name), attributes used in authorization decisions (privileges, roles) or pointers to personal services (calendar service). Note that the user's pseudonym may also be regarded as an identity. Hence, identifiers must be mapped onto pseudonyms; this mapping requires additional functionality at the identity provider.

The use of opaque identifiers (opaque means unstructured and with no semantic meaning to its value) during information exchange between stakeholders guarantees the privacy of the user. The opaque handle has meaning only in the context of the relationship between the Identity Provider and the service provider during the active session. Thus, a user's identity and actions are harder to track as the user navigates among service providers. Only the identity provider is able to map the different identities onto each other via the opaque handles.

SAML 2.0 provides a facility enabling a user's identity to be presented to service providers and other relying parties anonymously, using non-persistent identifiers. The relying party upon request may obtain identifiers of this type at the identity provider. Additionally, users may designate that they are to be represented with a certain identifier to relying parties within the scope of a session. This facility shall be applicable independent of whether or not the user has a federation relationship between the SAML identity provider and any of the relying parties receiving assertions within the session. Desirably, it should be possible for a user to request and/or configure use of this facility at the granularity of individual relying parties.

From different perspectives, it is not desired to perform opaque identifier creation and linking at the service provider's side. Identity providers or proxies are ideally positioned for this purpose. They can create and link (or federate) identifiers in a privacy preserving manner. Moreover, they can also be used for identifier discovery and attribute aggregation. This is illustrated in Figure 5.

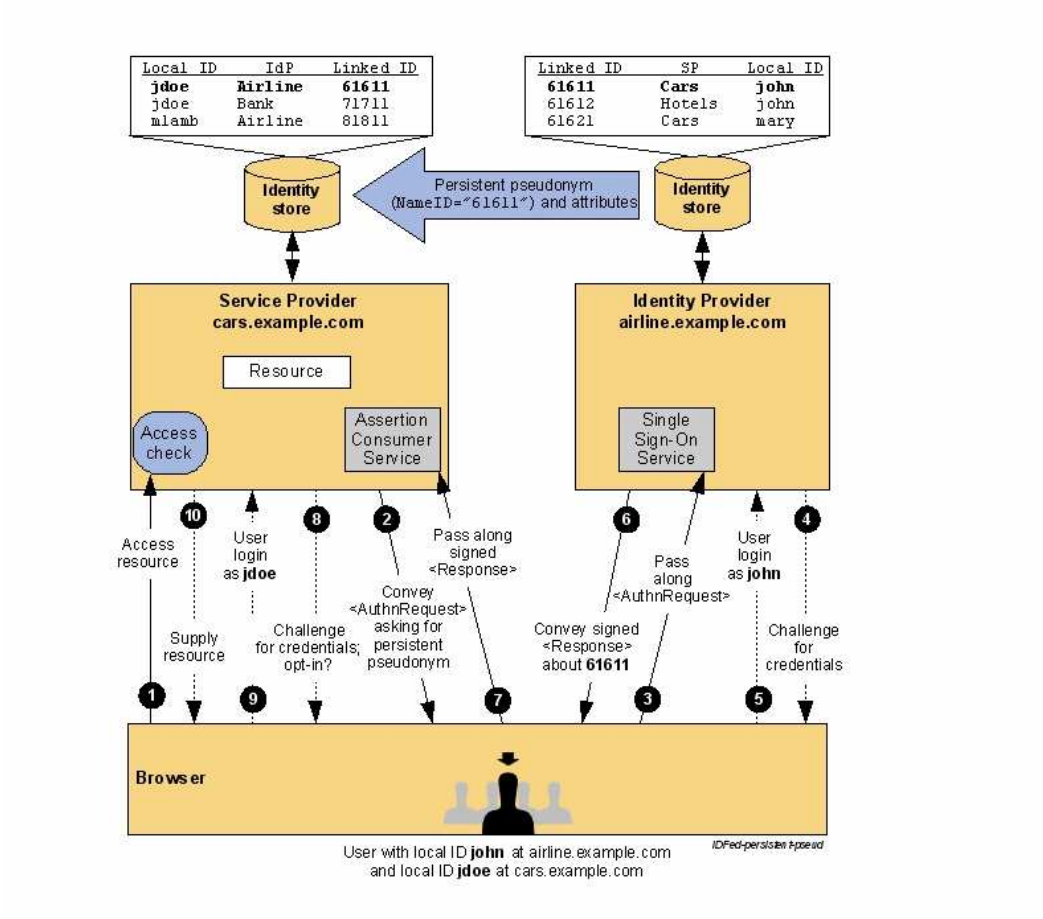


Figure 5: Identifier linking.

4.2.2 Privacy enhancing technologies

Privacy enhancing technologies such as Credentica [10] and Idemix [11] can be used to hide the true identity of the user. The possible use of such anonymous credential systems for eID interoperability can be explored in the STORK project but falls outside the scope of this deliverable.

4.2.3 User consent

User consent will not be too problematic when data is provided by the user directly (e.g., in an online form), or when data can be obtained from a certificate presented by the user (for instance, taken from a certificate on a smart card inserted into a reader attached to the device the user uses in the interaction). It becomes more complicated when the service provider (relying party) needs to obtain additional data, such as (certified) attributes, that has to be obtained from other sources than the user. In some cases, it may be possible, for instance, to collect the data from authentic registers in the user's home member state. In these cases, also consent of the user may be required in order to make the processing legitimate.

When registering for using online services (public or private) the user consent for identity information exchange and/or verification is given implicitly or must be given explicitly (online agreement "accept", physical legal contract, etc.). Possible solutions for user consent may depend on the model that is chosen for eID exchange. Three possible models are:

1. The data is provided by the user into an online form on the service provider's web site. The data is validated by the service provider at the appropriate data controller in another member state based on the user's consent.
2. The user authenticates to the data controller's web site so that he can view his data that is necessary for his request of a service. The user can then instruct the data controller (including consent) to send this data to the service provider in another member state.
3. The users are in control of their data. The user authenticates to the data controller's web site and can download his data in a read only format and the user passes this on to the service provider. This refers to user-centric identity management (see Section 4.2.4)

The STORK interoperability solution for electronic identity (eID) is based on a system that will take into account specifications and infrastructures currently existing in EU Member States and be compatible with national legislation's data protection legislation and other national legislation relevant to the project.

The user can either be directly involved in the attribute communication path via e.g. information cards (see Section 4.2.4) or asked for consent prior to data exchange via e.g. the Liberty Alliance Interaction Service [12].

4.2.4 User-centric identity management

So-called user-centric identity management systems, which focus on the users' rather than the service providers' perspective, have increasingly come forward in the past few years. This approach lets users choose, for example, what personal data to disclose under various conditions, and which credentials to present in response to authentication or attribute requests.

User-centric identity management - also referred to as Personal Identity Frameworks (PIF) or Identity 2.0 - focuses on user empowerment in sharing personal information and self-determination in establishing relationships with relying parties. User-centricity distinguishes itself from other notions of identity management by emphasizing that the user maintains control over 'what, where, when, and to whom' a user's identity attributes are released. The primary approaches behind the user-centric model are identifier-based (such as OpenID) and information card (such as InfoCard) systems.

In contrast, user-centric identity is an architecture where individuals present the credentials of their choice for authentication at online services. Instead of the vendor-to-vendor systems integration and trust contracts of federation, service providers or relying parties authenticate a visitor by relying on the identity services of an identity provider of the visitor's choice. Relying parties may not accept all identity providers, but in general, the choice of who authenticates the identity lies with the user. Key technologies in this space are OpenID, InfoCards, and a variety of standards from Liberty Alliance.

User-centric identity models can be disruptive to existing federation strategies that are identity provider centric. Given that the latter centralized systems usually let the identity provider monitor all activities this privacy-invasive approach is less suitable for user-centric models in which the user can decide in each specific situation what to reveal and who to trust.

The flipside of users' offering data only under conditions is the requirement that enterprises connect their databases and business processes to privacy policies and accountability systems. Today's policy languages and identity systems only partially serve this requirement, and new research challenges continue to arise as data and policies are aggregated across different domains [13].

A few remarks need to be made regarding user-centric identity management [14]:

- User-centric identity frameworks provide technical solutions to help users easily register with and sign on to web-based services. However, these frameworks alone cannot solve the human problem of establishing and maintaining trust.
- User-centric identity management is not meant to prevent the misuse of data once it is stored on service provider or identity provider sites. Other traditional and evolving data protection control mechanisms must be used.
- Convergence between user-centric and established federation standards and the incorporation of merged functionality into products are needed to bring user-centric identity management functionality to the mainstream. Most identity and access management vendors are developing solutions. InfoCards can be used as a front-end authentication component to federations in some vendors' prototype products.

The two major emerging implementations of user centric identity are the before mentioned OpenID and Microsoft's CardSpace. We refer to STORK's deliverable D3.2 for a more detailed overview of these technologies [15].

5 Service Provider perspective

Service providers have to determine the assurance level that best fits their service offering(s). For this purpose they have perform an assessment of the risks involved regarding the use of the service by users whose identities are determined with varying levels of assurance. Threats and their likelihood should be considered as well as the sensitivity and confidentiality of the information exchanged. The outcome of this risk and threat analysis yields a measure of the severity of potential harm of adverse impacts to the system if there is an error in identity authentication. IDABC [3], NIST, and the Spanish MAGERIT approach [16] amongst others provide guidelines or methodologies for service providers to conduct such an analysis. Other approaches are listed in [17]. Once the risks have been identified, countermeasures should be identified and implemented that mitigate the risks associated to flawed identity authentication. These countermeasures determine the minimal assurance level of authentication assurance that is required to mitigate the risks. It must be noticed that some of the risks will be mitigated in the technologies designed in WP4 and WP5.

In STORK we have to assume that service providers will adopt the levels of authentication as defined by their member states. Therefore, the authentication assurance level will result in the specification of national levels of assurance. Sometimes, however, it may be better for a service provider to as well look into the STORK levels instead of just national levels. For instance, several member states only define a single national level of assurance and for instance offer a Level 4 authentication assurance in terms of STORK levels, i.e. citizens only have a qualified hardware token to authenticate. Service providers in those member states may be inclined to accept only Level 4 authentication for service access. The consequence of this inclination is that citizens of other member states that do not have the capabilities for Level 4 authentication will be excluded from service use. If the service provider's risk profile, however, is such that he does not really need Level 4 but can also use STORK level 2 or 3 authentication, he will miss out on potential users form other member states. Lower levels should be considered from a service provider point of view in order to stimulate pan European use. This requires, however, that service providers have knowledge of the existence of the STORK levels. Allowing them to adopt the STORK framework may solve this issue. Consequently, the STORK infrastructure somehow must be able to distinguish between service providers that have adopted the STORK QAA levels and those that choose to use national levels.

6 Summary and conclusions

The ambition of STORK is to create an infrastructure for eID interoperability to allow intuitive citizen access to pan European services. A variety of eID solutions have been adopted by the member states, which have implemented their own solution or, in certain cases, their own multiple solutions. Moreover, member states have different ways to assign assurance levels to the eID solutions they offer. These levels vary per member state and, generally, do not correspond to each other.

In order to obtain e-ID interoperability, a broad understanding of the spectrum of existing solutions and a common way to qualify the authentication assurance levels required by the member states are needed. This qualification should be based upon the means used for identification/authentication rather than on the quality of the authenticators. Finally, this common qualification scheme must complement (and not override) the authentication assurance levels used within the member states.

This deliverable explores how member states classify their authentication solutions into levels of quality and shows how these levels can be mapped onto a common framework for expressing authentication assurance levels in STORK.

The common STORK QAA framework offers four overall levels of assurance. Each overall STORK QAA level assignment is related to the quality of the registration mechanisms and to the authentication methods.

Organizational aspects relevant to assurance include registration mechanisms being applied for the issuance of tokens and/or credentials. More specifically, fulfillment to identification registration requirements, the issuing process following registration, the identity/quality of the issuing authority, and the retention of the registration information are important elements for assessing a quality parameter to the overall authentication process. Technical properties relate to the strength of the authentication method chosen (i.e. is it a username/password combination or are soft or hard crypto tokens being used), the authentication protocol, and the assertion mechanisms.

Based on a number of requirements, each of the seven organizational and technical aspects related to authentication assurance has been individually valued. The overall STORK QAA level consists of this set of valued aspects and the lowest individual value ultimately determines the overall STORK QAA level.

The definition of the STORK QAA framework allowed us to map national assurance levels onto each other. For this purpose an overview of all eID solutions and related national assurance levels was made. Based upon the organizational and technical implementation of these national eID solutions we were able to rate them in terms of STORK QAA levels. Mapping of national levels to STORK QAA levels, however, was not always straightforward and resulted in a number of recommendations:

- Member states that have multiple authentication solutions with different assurance on the national level but with equal assurance in the STORK framework must always be mapped onto the requested or higher national level.
- Member states that have several authentication solutions with equal assurance on the national level but with different assurance in the STORK framework should adopt the STORK QAA levels. Alternatively, a more detailed specification on the protocol level could be used. However, it is unlikely that SAML, as the default standard for identity information exchange, can facilitate this.

- Member states that do not have authentication solutions that map onto the highest STORK level may have limited access to pan-European services and should strive to implement a level 4 solutions as soon as possible.
- Service providers in member states that have only a single authentication assurance level that corresponds to STORKS's highest level should consider making a risk assessment regarding their services and decide for themselves if the highest level is the best choice. Less critical services may be rated with a lower assurance level thereby allowing more citizens access.

The latter recommendation, however, implies that service providers of such member states should have knowledge about other levels, and preferably STORK levels, as well. If service providers are given the option to conform to the STORK QAA framework instead of a national assurance framework, then they must express what type of assurance levels they adhere to (STORK or national). Otherwise mapping may go wrong.

Mapping of levels onto each other will be done automatically and in a distributed manner and, depending on the solution used, executed at the PEPS or by the middleware.

Legal matters limit the use of eID solutions across Europe and therefore are a major show-stopper for eID interoperability. They do not have a direct impact on the STORK QAA framework however but they forbid in many cases the communication of persistent identifiers between member states and require the use of qualified certificates. The latter matter is taken into account in the STORK QAA framework. The use of qualified or non-qualified certificates is an important element for the determination of the assurance level. Regarding the prohibition of using persistent identifiers several solution directions are available. These solutions directions include the use of opaque and transient identifiers, privacy enhancing technologies, and explicit user consent via user-centric identity management solutions.

So far, the work on the STORK QAA framework has been a theoretical activity. The final test should be its use in the pilots. We hope it will pass the test and offer new member states that want to join the project sufficient handles to easily become eID interoperable.

Another challenge to be addressed in the near future is the supervision of the overall STORK framework and infrastructure. The success of STORK largely depends on proper supervision and auditing procedures to promote adherence to the STORK framework. Service providers, identity providers and users should have confidence the reliability of the framework and infrastructure otherwise the STORK concept will fail.

References

[1] D2.1 - Framework Mapping of Technical/Organisational Issues to a Quality Scheme, STORK deliverable.

[2] D2.2 - Report on Legal Interoperability, STORK deliverable.

[3] IDABC – European e-Government Service, Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms, December 2007 (http://ec.europa.eu/idabc/en/document/6484/5938).

[4] Liberty Identity Assurance Framework, Liberty Alliance Project, Nov 2007 (http://www.projectliberty.org/liberty/files/whitepapers)

[5] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[6] ETSI TS 102 042 V1.3.4 (2007-12) by the European Telecommunications Standards Institute, Technical Specification, Policy requirements for certification authorities issuing public key certificates, 2007.

[7] The Common Criteria, see http://www.commoncriteriaportal.org/thecc.html.

[8] Mapping IDABC Authentication Assurance Levels to SAML v2.0, Gap analysis and recommendations. Enisa Report, November, 2008.

[9] R. Anderson, Security Engineering (2nd Edition), Ch. 8: Multilevel Security, 2008, Wiley.

[10] Microsoft, Credentica, http://www.credentica.com/

[11] IBM Zürich Research Laboratory: Idemix http://www.zurich.ibm.com/security/idemix/

[12] Liberty ID-WSF Interaction Service Specification, Version 2.0, see www.projectliberty.org/liberty/content/download/885/6231/file/liberty-idwsf-interaction-svc-v2.0.pdf.

[13] P. Bramhall, M. Hansen, K. Rannenberg, and T. Roessler, "User-Centric Identity Management: New Trends in Standardization and Regulation," IEEE Security and Privacy, vol. 5, no. 4, pp. 84-87, Jul/Aug, 2007.

[14] G. Kreizmann and R. Wagner, Identity 2.0: Tomorrow's Promise and Today's Reality, Gartner Research, 11 December 2007.

[15] M. Ivkovic et al., STORK deliverable D3.2 List and assessment of priority technologies, December 2008.

[16] MAGERIT, Methodology for Information System Risk Analysis and Management, Ministerio de Administraciones Públicas, June 2006, http://www.epractice.eu/document/3215

[17] ENISA: Inventory of Risk Management Methods and Tools, see http://www.enisa.europa.eu/rmra/