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

D2.1 - Framework Mapping of Technical/Organisational Issues to a Quality Scheme

Deliverable Id :	**D2.1**
Deliverable Name :	**Framework mapping of technical/organisational issues to a quality scheme**
Status :	**Final**
Dissemination Level :	**Public**
Due date of deliverable :	**M6**
Actual submission date :	**13 October 2008**
Work Package :	**2**
Organisation name of lead contractor for this deliverable :	**Dutch Ministry of the Interior and Kingdom Relations**
Author(s):	**H. Eertink, B. Hulsebosch, and G. Lenzini**
Partner(s) contributing :	**AT, BE, EE, FR, DE, IS, IT, LU, PT, SE, ES, SI, UK**

Abstract: This deliverable explores how member states classify their local authentication solutions into levels of quality, and it investigates on a common framework for expressing authentication assurance levels in STORK. The IDABC *"Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms"* is used as guideline on the definition of a tentative common multi-level authentication scheme. A preliminary mapping between the locally adopted levels and the tentative assurance levels is also proposed.

Project funded by the European Community under the ICT Policy Support Programme
© Copyright by the STORK-eID Consortium

History

Version	*Date*	*Modification reason*	*Modified by*
0.8	22/09/08	Draft of the deliverable	H. Eentink B. Hulsebosch, and G. Lenzini
0.9	26/09/08	Final Draft of the deliverable	H. Eentink B. Hulsebosch, and G. Lenzini
0.10	29/09/08	Included feedbacks from Belgium, Austria, Spain (CATCERT) Iceland, and Portugal. Applied STORK template.	G. Lenzini
0.11	02/10.08	Included feedback from UK, Germany, and France	B. Hulsebosch and G. Lenzini
0.12	06/10/08	Updated sections of Iceland and Spain (José Fernando)	G. Lenzini
1.0	06/10/08	Added more details in the section of UK.	G. Lenzini
1.1	08/10/08	Updated the Portuguese table. Considered the feedback from Spain (CATCERT).	G. Lenzini
1.2	13/10/08	Implemented feedbacks contained in the minute of the Madrid meeting. Removed the glossary. Updated Swedish, French, and Spanish tables.	H. Eertink, B. Hulsebosch and G. Lenzini
1.3	14/10/08	Processed the comments of the WP2 leader.	B. Hulsebosch
1.4	14/10/08	Unified layout of tables	B. Hulsebosch
1.5	25/02/09	Minor amendment on Spanish profile	A. Piñuela (Atos)

Table of contents

HISTORY **2**
TABLE OF CONTENTS **3**
LIST OF FIGURES **5**
LIST OF TABLES **6**
EXECUTIVE SUMMARY **7**
1 GLOSSARY 8
1.1 ACRONYMS 9
2 INTRODUCTION **10**
2.1 SCOPE AND OBJECTIVE OF THE PROJECT 10
2.2 SCOPE AND OBJECTIVES OF THIS DOCUMENT 11
2.3 STRUCTURE OF THE DOCUMENT 12
3 BACKGROUND IN AUTHENTICATION INTEROPERABILITY **13**
3.1 AUTHENTICATION PROCESS REFERENCE MODEL 13
3.1.1 PROCESSES 14
3.1.2 FUNCTIONS 15
3.2 APPROACH TO QUALITY ASSURANCE OF AUTHENTICATION 16
3.3 PROXY VERSUS MIDDLEWARE SOLUTIONS 17
4 STORK QUALITY OF AUTHENTICATION ASSURANCE APPROACH **18**
5 QUALITY ASSESSMENT OF AUTHENTICATION SCHEMES **21**
5.1 IDABC APPROACH 21
5.2 ANALYSIS OF THE IDABC APPROACH 24
5.2.1 TRUST 24
5.2.2 LIABILITY 24
5.2.3 GRANULARITY OF THE LEVELS 25
5.2.4 AUTHORISATION 25
5.2.5 IDENTITY ATTRIBUTES 25
5.2.6 COMPLEXITY 26
5.2.7 LEGAL ASPECTS 26
6 NATIONAL AUTHENTICATION ASSURANCE LEVELS IN STORK-QAA **27**
6.1 AUSTRIA 28
6.2 BELGIUM 29
6.3 ESTONIA 31
6.4 FRANCE 32
6.5 GERMANY 35
6.6 ICELAND 37

6.7 ITALY 39
6.8 LUXEMBURG 40
6.9 THE NETHERLANDS 41
6.10 PORTUGAL 42
6.11 SLOVENIA 43
6.12 SPAIN 44
6.13 SWEDEN 48
6.14 UK 50
6.15 OVERVIEW OF THE STORK-QAA SCHEME FOR THE MEMBER STATES 54
7 CONCLUSIONS AND OPEN ISSUES 55
REFERENCES 56

List of figures

Figure 1: Problem of mapping authentication levels and processes 11
Figure 2: Authentication Process Model (from [1]) 14
Figure 3: The STORK approach to quality authentication assurance 18
Figure 4: IDABC properties for multilevel authentication assurance assigning. 22
Figure 5: Risk management for authentication level assurance assessment. 22
Figure 6: Trust relations in an eID federation. 24

List of tables

Table 1: Number of levels recognized or used for authentication and identification per member state. 27

Table 2: Summary of the Austrian authentication levels, and preliminary mapping according to the STORK-QAA tentative levels. 28

Table 3: Summary of the Belgium authentication levels, and preliminary mapping according to the STORK-QAA tentative levels. 30

Table 4: Summary of the Estonian authentication levels, and preliminary mapping according to the STORK-QAA tentative levels. 31

Table 5: Summary of the French authentication levels, and preliminary mapping according to the STORK-QAA tentative levels. 34

Table 6: Summary of the German authentication levels, and preliminary mapping according to the STORK-QAA tentative levels 36

Table 7: Summary of the Icelandic authentication levels, and preliminary mapping according to the STORK-QAA tentative levels 38

Table 8: Summary of the Italian authentication levels, and preliminary mapping according to the STORK-QAA tentative levels 39

Table 9: Summary of the Luxemburgish authentication levels, and preliminary mapping according to the STORK-QAA tentative levels 40

Table 10: Summary of the Dutch authentication levels, and preliminary mapping according to the STORK-QAA tentative levels 41

Table 11: Summary of the Portuguese authentication levels, and preliminary mapping according to the STORK-QAA tentative levels. 42

Table 12: Summary of the Slovenian authentication levels, and preliminary mapping according to the STORK-QAA tentative levels 43

Table 13: Summary of the Spanish authentication levels, and preliminary mapping according to the STORK-QAA tentative levels 47

Table 14: Summary of the Swedish authentication levels, and preliminary mapping according to the STORK-QAA tentative levels. 49

Table 15: Summary of the English authentication levels, and preliminary mapping according to the IDABC Levels 53

Table 16: Resume of the preliminary mapping, for each member states, between the national levels and the STORK-QAA tentative levels. 54

Executive summary

Member states have adopted a plethora of methodologies: some member states recognise two levels of authentication, other four. Levels are classified according to different strategies. Some states prefer a classification based on the means for authentication (e.g., smart cards with PKI, software certificates, username/password); others on the presence/absence of an authentication step. The same name (e.g., level 3) may be associated to different authentication solutions by different member states. For example, level 3 may be associated, in one state, with an authentication methods based on software certificates obtained trough the Internet without any physical presentation of the owner. In another state, the same level 3 identifies a solution where a username/password combination is obtained via government databases and sent using the official postal address.

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; thus, in the previous example, the software certificate obtained via the Internet without any physical presentation of the owner offers less assurance than the username/password combination that complies with a very high registry authority standards. 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 how these levels can be mapped onto a common framework for expressing authentication assurance levels in STORK.

The IDABC *Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms* [1] is taken as the starting point for the definition of a multi-level authentication scheme for STORK. In [1] the quality of several organisational and technical properties related to the authentication process are both taken into account. This allows for more fine-grained assurance levels if needed.

Further research, however, is required to come to a common way of qualifying the authentication assurance levels. In particular, the legislative implications may have an impact on the definition of such a common framework. This research will be carried out in a subsequent deliverable.

1 Glossary

A common glossary accepted by all STORK participants is under construction. This glossary will be presented as a separate document. For the moment footnotes are used the explain terms when necessary.

1.1 Acronyms

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

AP	Attribute Provider
CSP	Credentials Service Provider
eGov	Electronic Government
e-ID, eID	Electronic Identity
IDABC analysis of assessment report	IDABC – European e-Government Service, *eID Interoperability of PEGS: Analysis of Assessment of Similarities and Differences - Impact on eID interoperability* (see [5])
IDABC authentication levels report	IDABC – European e-Government Service, *Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms* (see [1])
IDP	Identity Provider
OCSP	Online Certificate Status Protocol
PEPS	Pan European Proxy Services
PKI	Public Key Infrastructure
RA	Registration Authority
RP	Relying Party
SP	Service Provider
STORK-QAA	STORK Quality Authentication Assurance
WP	Work Package

2 Introduction

2.1 Scope and objective of the project

Across the world, states and businesses are tackling the issue of identification in order to know who their clients are, and to ensure that people only get access to the right information and services that they are entitled to. As "identity" is rapidly becoming the central organizing principle in the information society, managing identity in a proper manner is key.

The availability of an electronic identity[1] (eID) management backbone across Europe will allow citizens to securely interact and make use of services any time, any place and anywhere. If high-quality eID management on a pan European level is made available to the public or private sector, new commercial electronic services that require identity management can be set up that serve the entire European market. Pan European eID management thus exists as enabler for innovation of public and commercial services benefiting citizens, but also businesses, in particular small and medium enterprises. To align actors in the field a powerful shared vision is needed, driven by real user needs and public interest.

User identification and authentication[2] are essential elements for many pan European services to become successful and secure. However, most individual member states have their own solutions for user identification and authentication. Interoperability of these eID solutions is required for efficient usage of pan European services. In other words, the member states must be aware of and trust each other's solutions. This trust is related to the level of assurance that is associated to an authentication solution. If there is common understanding about the levels of assurance then interoperability is ensured.

The following scenario illustrates how an interoperable eID framework with multiple levels of assurance regarding authentication should work:

Imagine a Dutch student that wants to register for a course on the University of Madrid. The student browses to the university's website and clicks on the registration button. Immediately the student is asked to authenticate. For this purpose, the student is first asked to select her country of origin. She selects The Netherlands. Subsequently, she is redirected to the authentication site of DigID. Since the registration application is of moderate security, two possible methods for authentication are presented to the student: DigID and DigID+SMS. The student selects the first option and enters her username and password. However, prior to granting access, the registration application requires evidence that the student really is a Dutch student. For this purpose, the Dutch DigID authentication and identity provider requests at the Dutch IB-group[3] (an attribute service provider) a token proves that the authenticated user is a student. Together with the authentication information, this grants the student access to the registration application. She can register herself for the course.

---

[1] An electronic identity (also digital identity) is a partial identity in an electronic form

[2] Identification is the process of using claimed or observed attributes of an entity to deduce who the entity is. Authentication is the corroboration of a claimed set of attributes or facts with a specified, or understood, level of confidence. In this document authentication is the corroboration to attributes of fact related to an identity; as such the term "authentication" implicitly refers to identification process. Unless explicitly stated, the term authentication is used, in this document, as a shortcut for "identification and authentication".

[3] The Dutch organization that administers the enrollment of students in higher education

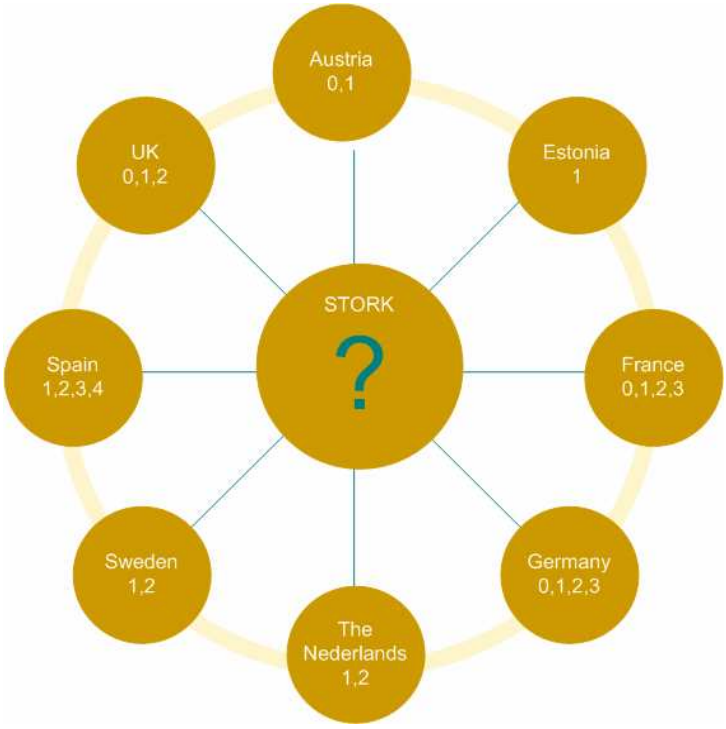


Figure 1: Problem of mapping authentication levels and processes

Figure 1 illustrates the problem that needs to be solved in the STORK project: "How to map the national authentication levels onto a common authentication assurance level framework?"

2.2 Scope and Objectives of this document

This document focuses on the determination of authentication assurance levels for cross-border authentication interoperability among the EU member states. Diverse resources (e.g., data and services, etc) will become available via electronic identification. These resources have varying levels of sensitivity; unauthorized access can result in different types of risks. Moreover, the integration of the different national electronic authentication mechanisms in the EU will result into a more diverse resource-sharing environment. Agreed upon authentication assurance levels are needed and should be linked to authorisation decision making. They determine the application's degree of certainty in the identity assertions made by the authenticating entity (cf. [1]).

This deliverable explores how member states classify their local authentication solutions into levels of quality, and makes a preliminary investigation on how these levels can be mapped onto a common framework for expressing authentication assurance levels in STORK. The IDABC–European e-Government Service, *Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms*[4] (see [1]) is used as the reference framework for this purpose.

Furthermore, this deliverable is the first of three deliverables from WP2 of STORK. Deliverable D2.2 will address issues related to legislation of authentication interoperability across Europe.

[4] From now [1] will be referred as "IDABC authentication levels report".

The final WP2 deliverable D2.3 will define the conclusive STORK common framework for authentication assurance level mapping and interoperability.

2.3 Structure of the document

The structure of this document is as follows. Section 3 provides the necessary background information regarding authentication interoperability and motivates the need for authentication assurance levels. Section 4 describes the STORK approach to a common framework for assurance level assessment. Section 5 describes the IDABC framework and presents several considerations regarding this framework. Section 6 gives an inventory and analysis of all existing authentication solution per member state; an assurance STORK levels is preliminarily associated per solution and per member. Finally, Section 7 concludes the document and lists the open issues.

3 Background in Authentication Interoperability

This section recalls a reference model for authentication, motivates the need for authentication assurance levels, illustrates how to achieve interoperability between the levels, and briefly describes two approaches to eID interoperability.

3.1 Authentication Process Reference Model

It is helpful, for the objective of this document, to have a common understanding on what we mean with authentication. Section 4 of the "IDABC authentication levels report" [1] describes the authentication process clearly and concisely. The following paragraphs are a rewriting of what reported in [1].

The authentication process reference model in [1] recognizes two phases; namely, *Registration* and *electronic Authentication* (Figure 2:. Registration establishes how entities get identity tokens[5]; electronic Authentication establishes how to verify the identity of a claimant given an identity token.

Figure 2: also shows the authorisation process that follows authentication. Authorisation concerns the access privileges of an authenticated identity. It is of concern to the service providers and typically based on the authentication assurance level that emerges from the authentication phase and/or on the value of particular attributes[6] (such as age). The authorisation process will not be considered in this document.

[5] A unique software or hardware object given to a specific user to prove his/her identity.

[6] An attribute is a distinct, measurable, physical or abstract named property belonging to an identity.

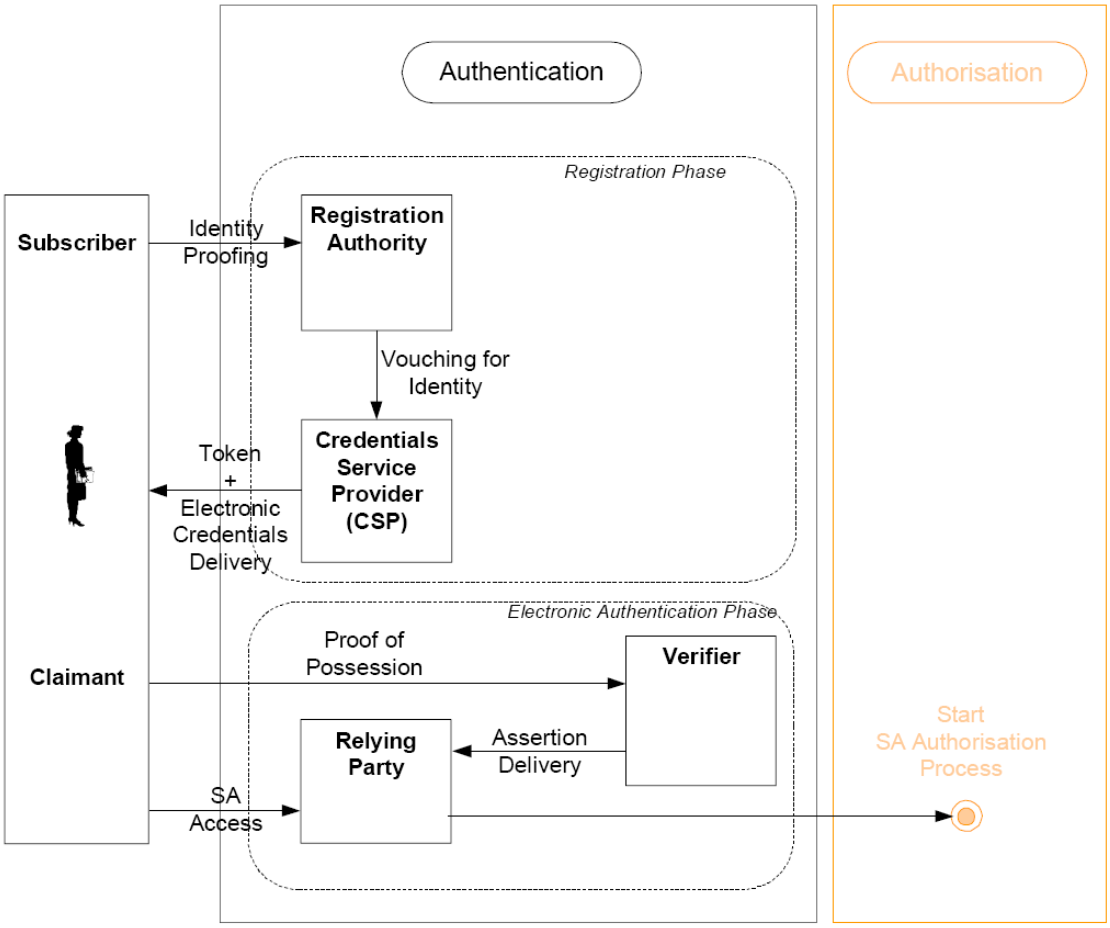


Figure 2: Authentication Process Model (from [1])

3.1.1 Processes

Four main processes can be identified in the authentication process reference model, namely, the *identity proofing*, the *token and credential delivery*, the *proof of possession*, and the *assertion delivery*. We briefly explain them:

- **Identity Proofing**: The process of ensuring that an identity actually corresponds to a real entity, with correctly associated attributes (which can be very limited, e.g. perhaps only a name). Increasing levels of assurance require increasing effort to establish the identity of subscribers.
- **Token and Credentials Delivery**: The process where the credential service provider (see next section) registers or gives the subscriber a token to be used in an authentication protocol; it also issues credentials as needed to bind that token to the identity, or to bind the identity to some other useful attribute(s).
- **Proof of Possession**: The process where a claimant successfully demonstrates possession and control of a token and/or credential during on-line authentication to a verifier. By mean of an authentication protocol, the verifier can establish the identity of the subscriber. A verifier can pass along an assertion about the identity or provide an attribute of the claimant to a relying party. The relying party can use the authenticated identity and other factors to make access control or authorisation decisions.

- **Assertion Delivery**: If the relying party and the verifier are separate entities, the relying party receives an assertion from the verifier. The relying party is responsible to validate that the received assertion came from a verifier trusted by the relying party. Where the assertions indicate time of creation or attributes associated with the claimant, the relying party is also responsible for verifying this information.

3.1.2 Functions

Different functions are involved in the previous processes, namely, the *subscriber* (also claimant), the *registration authority*, the *credential service provider*, the *verifier* and the *relying party*. In certain realities, the same entity can play more than one function.

- **Subscriber** or **Claimant:** The entity claiming an identity. Before an entity can claim an identity, he or she must demonstrate that the identity is a real identity, and that he is entitled to use that identity. For this reason, the claimant (in an authentication protocol) must be a subscriber to some Credentials Service Provider. The subscriber has a duty to maintain exclusive control of his token and/or credentials, since this is used to authenticate the subscriber's identity.
- **Registration Authority (RA):** The entity responsible for verifying the identity of the subscriber, typically through the presentation of paper credentials and by records in databases. The RA, in turn, vouches for the identity of the subscriber to a Credential Service Provider.
- **Credentials Service Provider (CSP):** The CSP registers or gives the subscriber a token to be used in an authentication process and issues credentials as needed to bind that token to the identity, or to bind the identity to some other useful attribute. The subscriber may be given electronic credentials to go with the token at the time of registration, or credentials may be generated later as needed. Note that is always a relationship between the RA and CSP. In the simplest and perhaps the commonest case, the RA/CSP are separate functions of the same entity. However, an RA might be part of a company or organization that registers subscribers with an independent CSP, or several different CSPs. Therefore, a CSP may have an integral RA, or it may have relationships with multiple independent RAs, and an RA may have relationships with different CSPs as well.
- **Verifier:** In any authenticated on-line transaction, the verifier must verify that the claimant has possession and control of the token and/or credential that verifies his identity. A claimant authenticates his identity to a verifier by the use of a token and/or credential, and an authentication protocol. This is called Proof of Possession (PoP). The verifier and CSP may be the same entity, the verifier and relying party may be the same entity or they may all three be separate entities. Where the verifier and the relying party are separate entities, the verifier must convey the result of the authentication protocol to the relying party. The electronic object created by the verifier to convey this result is called an assertion.
- **Relying Party**: A relying party relies on results of an on-line authentication to establish the identity or attribute of a subscriber for the purpose of some transaction. The verifier and the relying party may be the same entity, or they may be separate entities. If they are separate entities, the relying party receives an assertion from the verifier.

The Relying Party, or service provider, determines what credentials need to be provided in order to grant the Claimant or Subscriber, i.e. the user, access. It is therefore the Relying Party that determines the required authentication level for getting access.

It is the aim of WP 2 to offer the service providers (i.e., the relying parties) a suitable framework to allow them to determine what level of authentication assurance is required for the services they are providing. This deliverable provides the preparatory work leading up to such a framework.

We note that the STORK description of work (DoW) uses different terminology from that of IDABCS. STORK has *Identity provider* (IDP) instead of CSP, and *Service Provider* (SP) instead of Relying party. Moreover, STORK recognizes the *Attribute Providers* (AP), the entities who

provide attributes about the user (e.g., age, gender). The remaining of the document adopts the STORK terminology.

3.2 Approach to Quality Assurance of Authentication

"*If you can not measure it, you can not improve it.*" (1883) is one of the quotations of Lord Kelvin (the famous British mathematical physicist and engineer) that may be very applicable to the authentication assurance levels approach.

In order to be able to identify different assurance levels, we must be able to measure the "quality" of different authentication solutions. We also desire to be able to compare different authentication solutions and, for example, to claim that a solution has the same (a better, a worse) quality assurance of authentication than another does.

Each assurance level describes the degree to which a relying party in an electronic transaction can be confident that the identity information being presented by an IDP actually represents the entity referred to in the identity information. Several approaches for defining authentication assurance levels are possible; for example, criteria of classification can be based upon the importance of transactions, or on the severity of the consequences from misuse of a credential, or on the likelihood of the consequences of an authentication error. Managing risk in electronic transactions requires authentication and identity information management that provide an appropriate level of identity assurance. Because different levels of risk are associated with different electronic transactions, a multi-level approach seems the most appropriate. Each level describes a different degree of certainty in the identity of the claimant.

For example, the "IDABC authentication levels report" [1] bases the definition of authentication assurance levels on the likelihood of the consequences of an authentication error and misuse of credentials. They focus on the *possible* risks for abuse of the authentication method and the *possible* damages incurred by such abuse. The *likelihood* of those risks and, hence, the potential damage, are also taken into account.

A similar approach is described in the Liberty Alliance assurance framework document [15]. There, the levels reflect the levels of trust[7] associated with a credential as measured by the associated technology, processes, and policy and practice statements. The choice of the Liberty Alliance assurance levels is based on the degree of certainty that is required in the identity in order to mitigate risks. The degree of assurance required is determined by the relying party through a risk assessment processes covering the electronic transaction system.

Factors that affect the authentication assurance levels occur at all the steps of an authentication process. *Organisational* and *technical* factors can be distinguished. Organisational factors include the registration, issuance and revocation of identities, how/where credentials are used, and record keeping and auditing. Technical factors of influence include types/strengths of authentication credentials, strengths of authentication protocols/services, and the extent to which an authentication event is coupled to an authorisation event.

However, authentication assurance alone does not suffice in general. From the perspective of an application, there also needs to be interoperable on the attribute level (i.e. how reliable is the value of a particular attribute). Such attributes may be required for authorisation purposes (e.g. being a registered student, not being a minor). This requires a trust-relationship between the application, the user, the IDP and potentially also an attribute SP. These topics are addressed as well in this deliverable, and they will influence the requirements on the WP5 results and approach.

[7] Here with trust we intend "the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context" [14]

3.3 Proxy versus Middleware solutions

Two solutions for the communication of identity credentials are being discussed in Work Package 5: the proxy and middleware.

In the proxy approach, a 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, on its turn, proxies the request to the either the remote PEPS or the remote IDP of the member state from which the claimant originates. In the former case, the local PEPS communicates with the remote PEPS, who on its turn contacts the remote IDP. In the latter case, there is direct communication between the local PEPS and the remote IDP. In both cases, the IDP authenticates the user and returns the claims or assertions. Eventually, the local PEPS subsequently forwards the claims or assertions to the SP. The SP uses them to grant/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 own 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 them to levels that are understood by these IDPs. Of course, all nations will need to deploy such a proxy service.

The middleware approach is specifically suitable for smartcard usage and provides the necessary IDP discovery and user authentication in a transparent manner. This makes it easier to deal with the situation of multiple IDPs per member state, as the middleware relies on a public-key infrastructure to validate the information. However, it does require 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 on the card; in those cases, either another card must be used, or an AP may need to be accessed as well, requiring again a proxy-like model between the SP and AP.

Both models are currently under discussion in WP5. Independent of the outcome of this discussion, however, both models must be able to deal with authentication assurance levels.

4 STORK Quality of Authentication Assurance Approach

A STORK quality authentication assurance (in short, STORK-QAA) Scheme is used to define STORK-QAA levels, which are the levels used internationally among member states. Each member state maintains its local definition of authentication assurance levels. An initial mapping is provided between the national levels and the STORK-QAA levels. This mapping will eventually express the trust agreement between member state solutions and the STORK-QAA levels. The mapping can be guided by the requirements expressed in the STORK-QAA Scheme but may also be influenced by legal issues (that are identified in deliverable D2.2). Deliverable D2.3 will present a more elaborate description of the STORK QAA model, that also includes reflections on the applications (coming from WP6) and legal issues (described in deliverable D2.2)

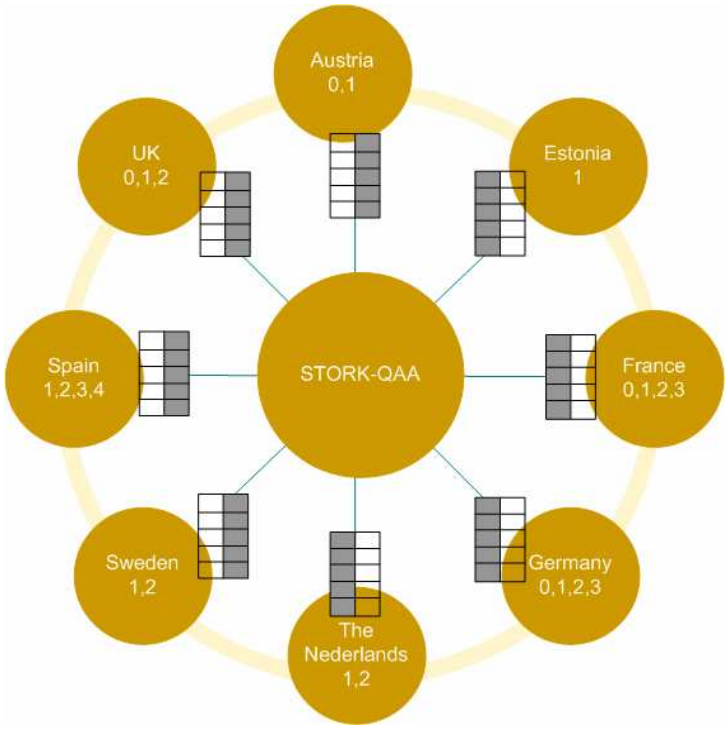


Figure 3: The STORK approach to quality authentication assurance

Figure 3 illustrates the main features of the WP2 approach. The authentication levels recognized by the member states are mapped into the STORK-QAA levels. The small tables represent the mapping that rules how the member states' assurance levels (the white columns of the tables) relate to the STORK-QAA levels (the grey columns of the tables). As the number of national assurance levels can be higher or lower than the STORK-QAA, it may happen that multiple national levels are mapped to a single STORK-QAA level (hence, loosing granularity). In addition, some STORK levels may not be achievable by some national authentication solutions; this implies that citizens of such member states will not be able to access a service that requires that particular STORK-QAA level.

Of course, if a citizen is authenticated at a certain STORK-QAA level, it is entitled to use all services that are available for STORK-QAA levels up to and including that level.

For the definition of the STORK QAA levels, several authentication quality assessment strategies can be adopted:

1. Adopt an existing approach, and let each member state map its solutions to the levels defined in the approach chosen.

2. Refine or extend an existing approach. This would allow for supporting finer granularity at each of the authentication properties that together determine the level of authentication. We can also let each SP decide whether it has specific requirements for some of these elements.
3. Define a completely new approach.

This deliverable opts for the option 2, and it identifies two reference documents that might be used; the first is the "IDABC authentication levels report" [1] by IDABC, and the second is the "Liberty Identity Assurance Framework" [15] by the Liberty Alliance.

As a preliminary choice, this deliverable chooses the "IDABC authentication levels report" [1] as a starting point. The IDABC authentication levels report (summarized this report in Section 5) specifies four authentication assurance levels, provides a set of definition of registration and authentication requirement for solutions to be used at each of the four assurance levels. The formal status of [1] is that it has not been accepted by all member states. Hence, we need to adapt it for the needs of STORK member states and STORK SPs.

The by IDABC suggested four levels of authentication assurance are adopted tentatively as STORK levels; we call them "STORK QAA tentative levels" to distinguish them from the final STORK-QAA levels that will be described in deliverable D2.3. For the moment we leave open the possibility of extending the model proposed in "IDABC authentication levels report" [1] to better match further requirements of the member states. Extending the IDABC approach may be motivated by legal considerations (work to be done in D2.2) or may be driven by trust issues such as the trustworthiness of the attributes provided. The latter aspect depends on the overall STORK architecture and the role of separate attribute providers therein.

The STORK QAA tentative levels and they are numbered 1, 2, 3, and 4, and they correspond to IDABC level 1, 2, 3, and 4 respectively. STORK-QAA tentative levels are described as in the following table:

STORK-QAA tentative level	Corresponding IDABC level	Description
1	1	minimal
2	2	low
3	3	substantial
4	4	high

Like in the "IDAC authentication levels report", the STORK-QAA tentative levels are based on 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 to engage in a transaction. See [1] and the next section for more details.

As said: deliverable D2.3 will present a more elaborate description of the STORK QAA model, that also includes reflections on the applications (coming from WP6) and legal issues (described in deliverable D2.2). More details will be needed to accommodate particular requirements coming from applications or member states, for instance in terms of more granularities in quality of authentication tokens or the enrollment process of obtaining these tokens. In this sense,

deliverable D2.1 is the first step in obtaining a fully accepted STORK QAA model with eventual STORK-QAA levels.

Section 6 describes the quality assurance authentication levels of the member states; it also discusses how those national authentication levels relate to the proposed approach, and how they can be preliminary mapped onto STORK-QAA tentative levels.

First, Section 5 describes the quality assessment of the STORK-QAA levels.

5 Quality assessment of Authentication Schemes

The starting point for WP2 is the work done by the "IDABC authentication levels report" [1], which is briefly summarized in Section 5.1. Section 5.2 analyses the approach, and presents the issues that have been identified in this report from a STORK application-perspective and interoperability-perspective.

5.1 IDABC approach

The IDABC approach defined in [1] encompasses a multilevel authentication policy and suggests a possible mapping of the existing authentication solutions observed in the EU countries into the defined authentication levels. The "IDABC authentication levels report" [1] proposal consists of the following components:

- Four authentication assurance levels, in terms of risk and potential damage in case of abuse, and taking into account organizational and technical aspects of the authentication process.
- A definition of registration requirements for solutions at each of the four assurance levels.
- A definition of authentication requirements for solution at each of the four assurance levels.

The registration requirements and the authentication requirements are cumulative to determine the classification of an authentication mechanism, i.e. in order to qualify as a level 3 a qualification mechanism, the presented solution must meet all requirements for level 3 mechanisms, both with regard to registration and authentication. Therefore, the mere fact of using a specific token (e.g. a soft PKI certificate) is insufficient to decide that the presented solution is a level 3 authentication mechanism, since all other level 3 requirements (e.g. with regard to registration before a token is issued) must all be met. The assurance level of an authentication mechanism can only be determined by examining the whole of the qualities and circumstances surrounding its availability and use.

The four levels of authentication assurance suggested by IDABC describe the application's degree of certainty that the authenticating entity has presented a credential that refers to his identity and are defined as follows:

Level 1	minimal assurance
Level 2	low assurance
Level 3	substantial assurance
Level 4	high assurance

These 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 to engage in a transaction.

Each layer is associated to potential *risks* and potential *damages* an application owner is willing to accept and to the likelihood that a vulnerability might be exercised. Figure 4 depicts the IDABC approach. For each property, an assurance level ranging from 1 to 4 is assigned depending on the quality of its implementation. All the details can be found in [1] (section 5).

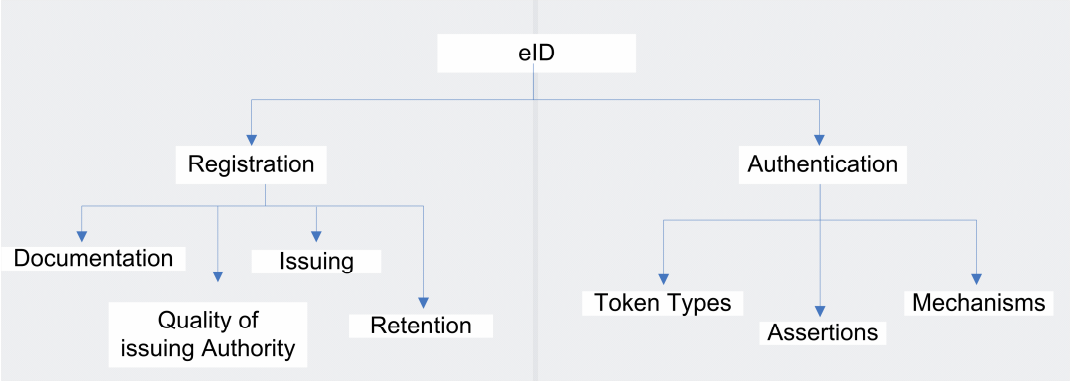


Figure 4: IDABC properties for multilevel authentication assurance assigning.

From a security perspective, the authentication process can be characterized in terms of *vulnerabilities*. The environment in which the authentication takes place is characterized by a number of *threats*. The *subject* of authentication has a certain value. A certain *risk* can then be derived for the parties involved in the authentication process, which expresses the *likelihood* that some part of the subject's value is lost due to the threats that successfully exploit existing vulnerabilities of the authentication system including its technological and organizational properties. If this risk is too high then either the assurance level of the authentication is lowered or measures are taken to reduce the risk. The latter decision involves better *safeguards* to reduce the vulnerabilities of the authentication (and consequently the likelihood of successful attacks) and/or measures to reduce the consequences of a potential attack. A safeguard in this context is a high-level abstract resource providing security functionality to increase the level of authentication assurance. Such risk management behavior is depicted in Figure 5.

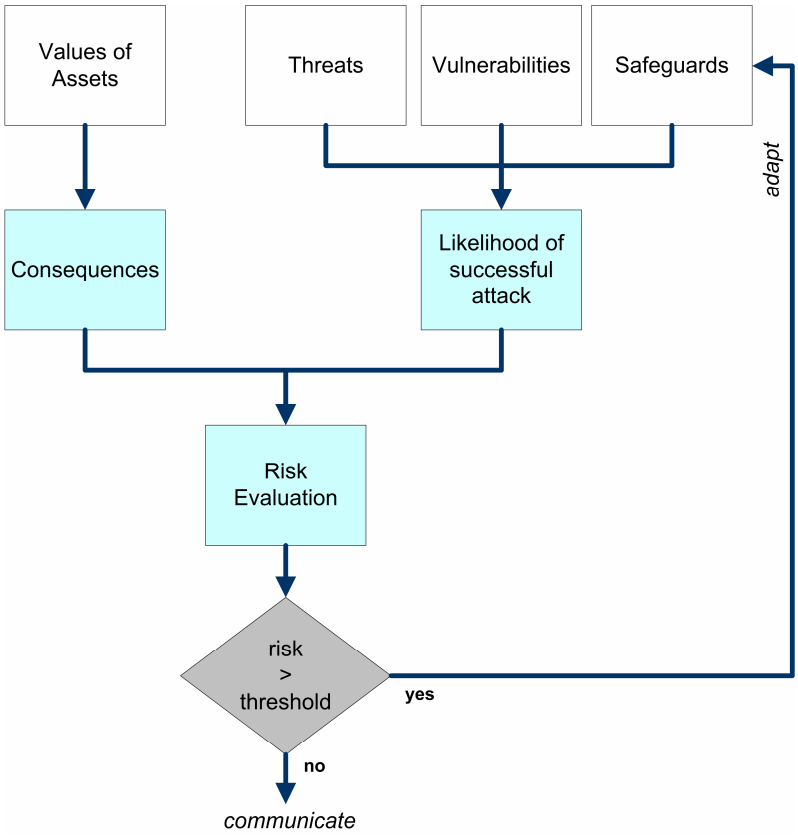


Figure 5: Risk management for authentication level assurance assessment.

Such a risk analysis should be done by the project for each pilot. When new SPs want to connect to the platform, each of them should perform a similar risk analysis.

In the "IDABC authentication levels report" [1] the overall assurance level assignment is related to the quality of the registration mechanisms and of 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.

After assigning a level to each registration and authentication methods, the "IDABC authentication levels report" [1] specifies the requirements and the possibilities for each of the four authentication levels as a next step. As an example, the requirements for the assurance IDABC level 1 are shown in the table below.

	Registration Phase	
Level 1	**Procedure for identity proofing, user details registration, delivery of token and credentials:**	1. Definition Level 1 registration is appropriate for application transactions in which damages that might arise from misappropriation of real world identity would have a Negligible or Low impact. The registration is purely claims based This registration level is heavily used by lots of Internet applications (webmails, on-line, auctions, etc.). 2. Requirements The RA can be any entity whose authentication methods are accepted in an eGovernment application. There is no requirement to prove the identity or maintain a record of the facts of registration. Identity assertions of claimants are accepted. Only the e-mail address must be unambiguous and valid. 3. Delivery There is no specific requirement for delivery of the token or credential.
	Retention period for registration data:	none

	Electronic Authentication Phase	
Level 1	**Authentication Protocol for Proof of Possession (PoP):**	Most of the time: ▪ challenge-reply password proof-of-possession However, according to risk assessment, could also be: ▪ Tunnelled password PoP ▪ One-time (or strong) Password PoP ▪ Symmetric Key PoP ▪ Private Key PoP
	Token Type:	All token types are acceptable. Most commonly Password or PIN tokens will be chosen.
	Requires the application owner to implement protection against:	▪ Replay ▪ On-line guessing

The requirements for assessing other IDABC levels can be found in chapter 5 of [1].

5.2 Analysis of the IDABC approach

Though the IDABC approach seems promising, several drawbacks can be identified. Moreover, several other relevant aspects are not considered by the "IDABC authentication levels report" [1] and these might have an impact on the proposed methodology. The drawbacks and missed aspects will be discussed in the following sections.

5.2.1 Trust

The chosen middleware or proxy-infrastructure for implementing STORKS eID interoperability needs to be trusted. It must not only guarantee the integrity and confidentiality of the credentials exchanged but excludes attacks as well. This also includes the use of trusted hardware for user identification and authentication. Figure 6 shows the diversity and quantity of trust relations (arrows) between the different entities involved for pan European eID management. It involves trust between multiple IDPs and SPs. Depending on the solution (proxy or middleware) there is trust required between the national IDPs (proxy) and between the IDP and foreign IDPs (middleware). Additionally, if attribute service providers are active in the network in providing user-related attributes towards the IDPs; a mutual trust relationship between the two parties must therefore exist as well. Furthermore, the provided attributes must be trustworthy, i.e., the IDPs must be able to enforce access based on these attributes.

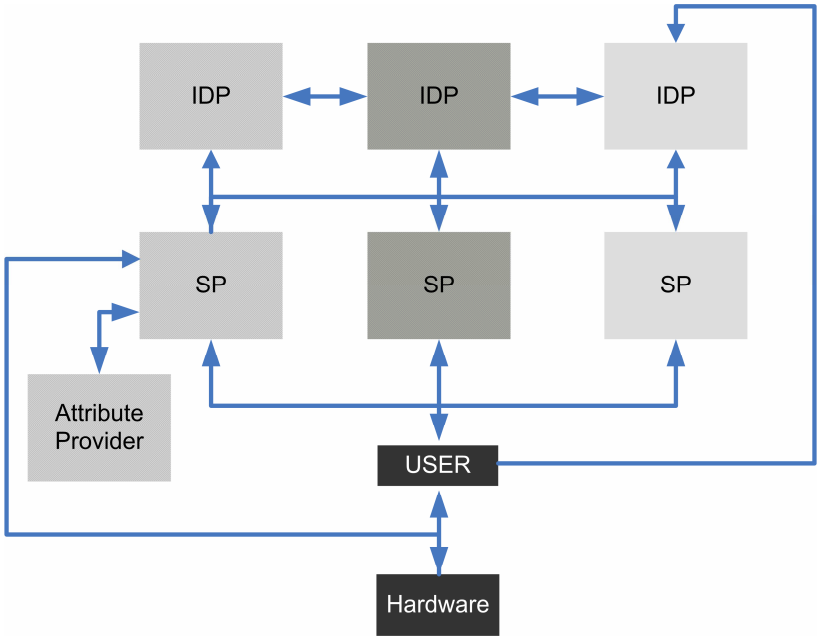


Figure 6: Trust relations in an eID federation.

A proper trust model for the STORK eID interoperability framework is therefore required. It is therefore required to define a trust model for the STORK interoperability framework. The following key principles of this trust model are discussed in the next subsections.

5.2.2 Liability

Related to trust is the aspect of liability. Who is liable in case of an error situation? Is it possible for each member state to map its own solution(s) to the levels that will be supported by the STORK federation and make them liable for their choices? This is not only an issue for authentication, but also for the correctness of attributes that are exchanged. Who will be responsible for maintenance of the solution, in case changes have to be made? Deliverable 2.2. will go into liability in more detail.

5.2.3 Granularity of the levels

In the “IDABC authentication levels report”, the different properties are plainly mixed and assigned to an assurance level (Section 5.5 of [1]). This method of plain mixing of different properties of the eID (e.g. registration mechanism and token type) into a plain model is arguable. Different qualities of the eID properties frequently do not fall into the same level. There may be variances to fit existing eID into one plain assurance level. For example, a token (smartcard) with a low-quality profile might be issued very thoroughly or vice versa. A finer-grained granularity could be used for several properties, and/or a more sophisticated method could to be developed to assess the "final level" of assurance. There is one other reason why a higher granularity (or a "multi-dimensional view") is useful: some RPs are very "jumpy" with regard to security levels. Too rough ones do not satisfy them - they want details and make their own decision based on those details. It is specifically true for banking industry but it may apply to (certain) eGov applications as well. A closer look at the different properties of the eID as done in the “IDABC authentication levels report” [1] is required.

A more fine-grained approach would be to take organizational and technical aspects apart. Fine-grained solutions will be taken into account only if RPs indeed require such granularity. Work Package 6 will estimate whether a finer granularity is a requirement or it is not, depending on the needs of the SP participating in the pilots. Deliverable D2.3 (WP2) will discuss possible solutions in favour or against a more fine-grained approach and, in this case, it will evaluate possible solutions. Most WP2 members seem to favor the 4 levels.

5.2.4 Authorisation

Another aspect of gaining access to public services is that of authorisation. As explained in Section 3.1, authorisation is out of scope for WP2. It will be each SP to decide upon who is authorized to perform a certain action, or benefit to a certain service depending on the identity, of the quality of the identification, the claimant and so forth. The risk analysis described in Section 5.1 can be used for this purpose.

5.2.5 Identity attributes

One could for instance think of the user’s age or gender. Getting these and other attributes is not evident. The integrity and authenticity of the attributes needs to be guaranteed. The party that provides the attributes can be either the IDP or an attribute SP. Besides the IDP, this requires that the attribute SP is trusted as well (see Trust section above). IDABC does not consider this aspect, which, indeed, may impact on the overall assurance level framework.

Furthermore, applications need to be able to specify and communicate the attributes they need for access control and further personalization of the service (e.g. language). From a privacy perspective, only a minimal set of necessary attributes should be communicated and with the consent of the user.

Therefore, what is required is an assertion expressing the authentication status of the user and relevant attributes for authorisation. Alternatively, instead of attribute communication, the user’s IDP may present an assertion that authorizes the user to use the service.

Summarizing:

- Often not only related to identity
- Additional attributes required (attribute assertions)
    - Age, gender, profession, etc.[8].

[8] Data and process flows will be established by WP4 and WP6 of Stork respectively.

- Issues:
  - Implicit or explicit (e.g. signed by SURFnet implies 'Student')?
  - Syntax (1-Sept-2008 or 9-1-08?)[9]
  - Meaning (what is a 'student'?)
  - What set of attributes to communicate?
    - Privacy
    - Application specific Agreements needed?
  - Relation to authentication assurance level?
    - What if the Authentication is solid but the Authorization is poor?

5.2.6 Complexity

From a user's perspective, it is not desirable to have too many levels of assurance. Research proves that a user can handle at most three levels of granularity/complexity [13]. The user may be confused and lose confidence (trust) in the authentication framework and the applications using this framework. There might be the need of asymmetric requirements (citizens point of view), despite this seems much more relevant to gov-citizen than pan-government. Furthermore, in case particular attributes are requested for authorisation purposes, user consent is required before the attributes are provided to the SP.

SP, IDP, and AP. also use assurance levels. They might prefer to have more or less granularity for what concerns the number of levels of assurance. Different solutions in the number of levels of assurance also bring to different confidence (trust) in the authentication framework.

In a scenario with PEPS, for example, Belgium prefers to have granular levels combined with a general level calculated by the national PEPS on the base of Belgian criteria. Thus, the SP would receive all assurance levels plus a Belgian one; the SP can then decide to use Belgium one, the other, or a combination of them.

Deliverable D2.3 will discuss upon the need of a finer granularity in the definition of levels of assurance; it will also collect the requirements of each member state and decide upon possible solutions.

5.2.7 Legal aspects

The legal aspects of eID interoperability will be addressed in deliverable D2.2.

[9] Format of data is outside the scope of this work and will established by WP5.

6 National Authentication Assurance Levels in STORK-QAA

Several applications will be piloted in WP6. They will run a number of e-ID interoperability pilot services. Each pilot application will request for a specific authentication assurance level, according to the member states' local understanding of the term "level". Member states have adopted different solutions in defining or adopting authentication assurance levels. States like, for example, Austria and Italy have an all-or-nothing approach: either the citizen is identified or not. This division is based purely on legal reasons: national laws define only one level of authentication. In other countries, the law recognizes a more fine grained division. It may also happen then a fine grained division exists despite the law. In other words, more solutions for authentication methods may be used within a member state despite the fact that a member state may not have a formal policy or law/regulation stating those authentication levels clearly. In these cases, the identified levels are based on the quality of the technology used for user identification. These existing and more fine-grained divisions must be considered as well.

A mapping between the authentication assurance levels recognized by each individual member state and the STORK-QAA levels is required. In the eID interoperability framework, this mapping will allow each the pilot application's request to be assigned with at a STORK-QAA level ensuring that the member states mutually speak the same 'language'.

As explained in Section 3.2, we propose to base the tentative STORK-QAA levels on the IDABC trust levels. Most of the member state solutions have already been mapped to the four IDABC levels (see sections 6.2 and 6.3 of the "IDABC authentication levels report" [1] and Section 5.1 of this report). In many cases, the authentication methods used by a member state correspond to multiple IDABC levels despite the fact that a member state may not have a formal policy or law/regulation stating authentication levels. Table 1 gives an overview of the authentication assurance levels of the member states involved. (Details are given in following sections).

Member State	Number of levels	Member State	Number of levels
Austria	2	**Italy**	2
Belgium	5	**Luxemburg**	3
Estonia	4	**The Netherlands**	4
Sweden	3	**Portugal**	3
France	4	**Slovenia**	4
Germany	4	**Spain**	3
Iceland	4	**UK**	4

Table 1: Number of levels recognized or used for authentication and identification per member state.

In the following sections, we present a mapping between the levels identified by each member state into the corresponding STORK-QAA tentative levels. This mapping is mainly based on what proposed in the "IDABC authentication levels report" [1] enhanced with input from WP6. WP6 is

still in the process of defining trust levels for each pilot application and further input may be considered during the WP6 run.

6.1 Austria

Austria recognizes just two levels of authentication [4], namely (1) without identification, and (2) with identification. Level (1) is used for open access services and get-and-pay services. Level (2) is used whenever an identification must take place because, for example, personal data is involved that needs to be protected or there is a legitimate interest by the authority. Identification is performed via a recognized "Citizen Card" concept that is implemented in a national ID card, but can also be implemented on a SIM-card or other types of (commercial) smart cards. Law defines the citizen card; the implications of that will be discussed in deliverable D2.2.

The following Table synthesizes the situation for Austria.

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA Level
0	No identification	None	None	Open access services and get and pay services (e.g., parking, gas, electricity, garbage)	
1	With identification	Source PIN Register Authority or, on its behalf, by other authorities or other appropriate bodies	Accredited Citizen Card, then validated by the electronic signature contained in the Citizen Card	Whenever privacy relevant data held by the administration or delivered with previous application is used for processing or delivery with the service	4

Table 2: Summary of the Austrian authentication levels, and preliminary mapping according to the STORK-QAA tentative levels.

The last column of the table indicates the mapping from the national Levels to the IDABC Levels (here adopted as STORK-QAA tentative levels), according to the "IDABC authentication levels report".

6.2 Belgium

At the current time there is no official document describing the levels of trust associated with the different authentication methods that Belgium has in place to offer e-Services to its citizens. However, in practice, several systems for authentication are available and, based on their quality and security aspects. Belgium has adopted the following five levels of authentication ([6], [5], [12]):

- Level 0: No identification
- Level 1: Identification using username and user-selected password
- Level 2: Identification using username and user-selected password and a random strong from a paper token.
- Level 3: Authentication using the authentication certificate of the eID with PIN
- Level 4: Authentication using the authentication certificate of the eID with PIN + digital signature using the signature certificate of the eID.

Each level is used to provide services with different sensitivity of user data (low, medium and high). A service can also explicitly request a digital signature.

The following Table synthesizes the situation for Belgium.

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA tentative level
0	No identification	None	None	Public Services	
1	With identification level 1	On line input of national registration number + identity card number + social security card (SIS) number	Username and user-selected password	Services of low sensitivity	1
2	With identification level 2	Level 1 + e-mail with activation URL to citizen (e-mail address selected by citizen) + paper token sent from National Register to citizen's address	Level 1 + one of the 24 textual strings from the paper token	Services of average sensitivity	2

3	With identification level 3	Physical registration at the community for reception of the eID	Authentication certificate on the eID + session based password	Services of high sensitivity	3
4	With identification level 4	Physical registration at the community for reception of the eID	Authentication certificate on the eID + signature using the signature certificate of the eID + password per transaction	Services that require a digital signature	4

Table 3: Summary of the Belgium authentication levels, and preliminary mapping according to the STORK-QAA tentative levels.

The last column of the table indicates the mapping from the national Levels to the IDABC Levels (here adopted as STORK-QAA tentative levels), according to the "IDABC authentication levels report".

6.3 Estonia

According to [12] Estonia has not adopted an official policy for authentication. Currently, Estonian applications tolerate authentication level 2, level 3, and level 4 in IDABC terms (cf. [11] and [1]). In practice, it means that two authentication options exist:

(1) Identification using a mobile-ID or the National ID-card (with PKI certificate), which is assigned mandatory to each Estonian citizen over the age of 15, and to non-Estonian with a permanent residence permit

(2) Identification through the bank identification system.

In this latter case, different solutions are possible:

- identification with a user password card (using username/password and a random string from a paper token issued by Estonian banks which allow 24 rotating passwords)
- identification with one-time-password token (PIN calculators generating live passwords, issued by Estonian banks)
- identification using an ID-card or Mobile-ID

Banking cards (which are not national cards) together with calculators are used as a mean of authentication (also in public sector applications). Such systems are quite popular; e.g. in Estonia the bank authentication system is significantly more popular than the e-ID card system using PKI certificates, despite the advanced status and highly secure nature of the eID card system. The national policy is to override, in the future, the bank authentication for governmental services. There is a massive campaign/program to make people use their ID-card or Mobile-ID so that, by the end of 2009, it will be possible to end the bank authentication. The situation of Estonia is summarized in Table 4.

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA tentative level
1	National identification		With ID-card or Mobile-ID (PKI certificate)	Public sector applications	4
1	Bank identification		Use a password card (24 rotating passwords)	Private or public sector services	2
1	Bank identification		Use a one-time-password token (bank calculators)	Private or public sector services	3
1	Bank identification		With ID-card or Mobile-ID (PKI certificate)	Private or public sector applications	4

Table 4: Summary of the Estonian authentication levels, and preliminary mapping according to the STORK-QAA tentative levels.

6.4 France

France recognizes four level of authentication. A basic level is used for authentication via login/password and three additional levels (middle, strong/standard, and strengthened) are devoted for authentication with PKI certificates. The definition of the level depends mainly on the registration process and the key storage device. Other aspects that affect the definition of the levels are listed below:

- the delivery of the certificate
- the process of acceptance of it
- the certificate revocation policy
- the certificate revocation list
- the certification authority protection features (e.g., certificates protected in a cryptographic module certified at a level CC EAL+2 or CC EAL+4)
- the process of generation of the private key
- the authentication key length
- the authentication device
- the authentication application
- the module used to verify the authentication process.

Detail of the French solution can be found in the www.synergies-publiques.fr web site. In particular, see the presentation http://www.synergies-publiques.fr/article.php?id_article=463. The following table resumes the situation for France. Now, the level 0 is the more common used. All applications use username and password with the exception of TeleIR (Income declaration) which uses their own certificates. (level 1)

Mon.service-public.fr which will be announced in December 2008, will be an entry point for the citizen to the government electronic services. He/she can create a username and password and after he/she can federate his/her identities (based on Liberty Alliance) to all other applications.

Mon.service-public.fr allows to enforce security level to log on as a first step with username and password and after to use an OTP sent by SMS by the application.

When the national eID card will be available, it will be a smart card (qualified as a SSCD) and with 2 certificates one for qualified signature and one for authentication. The authentication level will be the French level 4

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA tentative level
0		None	Login and password	All egov services Mon.service-public.fr	
1	Middle	Registration via sending of a registration file in paper form (with certified copy of the identity papers) or in electronic form or communication of a specific element of the subscriber allowing to identify it within an administrative data base. Delivery by email, and tacit acceptance Or login and password + OTP by GSM	Using PKI certificates compliant to requirement specific to this level (see [16])	Mon.service-public.fr	(3)
2	Strong or Standard	Registration face to face Delivery in person with face to face if not done during registration phase if possible. Explicit acceptance of the certificate by the subscriber or tacit acceptance starting from a sufficiently reliable handover date	Using PKI certificate compliant with requirements specific to this level (see [16]) Hardware token protected by PIN CC EAL3+		(4)
3	Strengthened	Registration face to face Delivery in person with face to face if not done during registration phase IF the AC does not generate the key, to check if the certificate is well associated with the corresponding private key Explicit acceptance of the certificate by the	Using PKI, with requirements specific to this level (see [16]) Hardware token protected by PIN CC EAL4+ ie National eID card		(4)

		subscriber			

Table 5: Summary of the French authentication levels, and preliminary mapping according to the STORK-QAA tentative levels.

In the last column of the table, we have indicated our proposal (numbers in brackets) for a mapping from the national Levels to the STORK-QAA tentative levels.

6.5 Germany

Germany is one of the two European countries (the other is Hungary) that oppose the use of general identifiers for identification purposes on constitutional grounds. In effect, this renders the examination of general unique identifiers somewhat moot, as the use of general identifiers for the identification of natural persons would at any rate be unacceptable; it can render them unusable for cross border authentication purposes.

Which level of trust regarding information provision and authentication is acceptable is subjective to e-SPs. In other words, SPs might have their own view about trust. Thus, the German policy regarding authentication levels will be specific from the viewpoint of the pilots scheduled in WP6. According to [8], the following levels are recognized:

Level 0 (low): no certainty about the information, low level of authentication

Level 1(normal): solid identity proof in registration, authentication with username and password

Level 2 (high): solid identity proof and authentication with hardware token and PIN

Level 3 (very high): same as high but usage of certified hardware token and card reader

The applications in the German pilots require Level 0 and Level 3; the use of other levels is still being discussed. The authentication means accepted for Level 0 is a user ID and password. The authentication means accepted for Level 3 is a qualified signature card and the upcoming e-PA, the German eID card; a PIN might also be required. The following Table summarizes the situation for Germany.

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA tentative level
0	Low level	Use of shared secret		(e.g., log on to mein-service-BW)	1
1	Medium	Registration with a solid proof of identification	Username, password-		(2)
2	Strong	Registration with a solid proof of identification	Hardware token with PKI functions + PIN-		(3)
3	Very Strong	Registration with a solid proof of identification	Certified hardware token with PKI functions + PIN	(e.g. registration / authentication to mein-service-BW)	(4)

Table 6: Summary of the German authentication levels, and preliminary mapping according to the STORK-QAA tentative levels

In the "IDABC authentication levels report" there is no mention of Germany's levels. In the last column of the table, we have indicated our proposal (numbers in brackets) for a mapping from the national Levels to the STORK-QAA tentative levels.

6.6 Iceland

Today the Icelandic Governmental agencies use a variety of eIDM systems, most of which are username/password-based. Some central governmental agencies have been using soft X.509 certificates in eGovernment since 2003, for example The Internal Tax Revenue Directorate and The Directorate of Customs.

Today the government is implementing a central eIDM system in Iceland that is based on X.509 Client certificates. The main objective of this project is to build an open and standardized PKI environment in Iceland. Based on this structure eIDs will be distributed to all citizens in the country. Citizens can use the eIDs in relations to both central and local government as well as any other business in Iceland. The Icelandic Government co-operates with the Federation of Icelandic Banks in building, implementing and maintaining this infrastructure. The Ministry of Finance has created a root certificate, named Iceland Root (Íslandsrót), that issues intermediate certificates to Identity providers (subordinate certificates authorities) in Iceland. An intermediate certificate has been issued to banks and is it planned that another certificate will be issued to National registry for the planned issuance of citizen cards. The banks have started to distribute certificates on debit cards to citizens. National registry is planning to start issuing certificates 2009.

Persons (both natural persons and legal entities) are identified with a ID-number (SSN#) in the National Register of Persons or in the National Business Register. This ID number is used in certificates as the unique identifier.

It is expected that after 2009 the certificates on bank cards will be the main means for citizens to identify themselves. Most governmental services that have used other ways for authentications do now except eID´s on bank cards in communications.

The following table summarizes the situation for Iceland.

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA tentative level
1	Other username passwords	Various ways	Username/password	Local and central e-governmental service	(1) Originally asked for (1.5)
2	Tax username/password	Password sent to citizen's legal address	Username/password	Tax declarations; student login	2
3	Soft PKI-certificate (Stjornarrad root)	Personal appearance showing legal ID document	PKCS#12, or other soft tokens	Tax declarations; governmental service portals	3
4	Hard PKI-token (Islandsrot)	Personal appearance showing legal ID document	Public key infrastructure based smart token. X.509 Client certificates on bank cards. Validation is done through standard OCSP / CRL lookup.	Local and central e-governmental service portals. Internet banks, and more	4

Table 7: Summary of the Icelandic authentication levels, and preliminary mapping according to the STORK-QAA tentative levels

The last column of the table indicates the mapping from the national Levels to the IDABC Levels (here adopted as STORK-QAA tentative levels), according to the "IDABC authentication levels report". A note; Iceland suggested mapping level 1 into STORK level 1.5, which is not a STORK level. This means that Iceland consider its level 1 a bit "higher" than STORK level 1. The table suggests, in agreement with the STORK level mapping presented so far, that Icelandic level 1 corresponds to STORK QAA tentative level 1.

6.7 Italy

The Italian policy for e-services is to adopt, by the end of 2008, authentication solutions based on digital certificates on smart cards. Two national cards will be available for citizens to access national-wide services (e.g., services from the revenue agency, and national heath care services): the electronic Italian identity card (carta di identità elettronica or CIE) and the national service card (Carta Nazionale dei Servizi or CNS). Until the end of this year, services deployed by the public administration offices (e.g., the revenue agency and National Body for Social Services) can still use the methods that they have been using so far, namely, PIN and password. Italian regional bodies may have adopted local solutions, e.g., based on regional smart cards; these solutions are used for local regional services and they will coexist with the electronic national card when it is in use.

The two major examples of Central Agency currently using PIN + PWD are INPS (National Body for Social Services) and Agenzia delle Entrate (Revenue Agency). PIN and PWD can be obtained partially (first digits) online, and completed (after some verification procedures) with the postal delivery of the complete pin code and password.

Also at local level, public administrations are allowed to use the current authentication method (also typically USERNAME + PWD). Nevertheless, they are also obliged to conform, starting from January 2009, to the use of digital certificates.

The authentication methods (smart-card based or PIN+PWD) have not been mapped by IDABC with respect to the level defined in IDABC. The following table summarizes the situation for Italy.

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA tentative level
1	Italian ID card, and CNS	Governmental and regional bodies	digital certificate on smart cards	National and some regional services	(4)
1	none	national and regional bodies (till December 2008)	PIN and password	National and regional services	(2)

Table 8: Summary of the Italian authentication levels, and preliminary mapping according to the STORK-QAA tentative levels

In the "IDABC authentication levels report" [1] there is no mention of Italian levels of authentication nor they are classified in terms of the IDABC Levels. In the last column of the table we have indicated our proposal (numbers in brackets) for a mapping from the national Levels to the STORK-QAA tentative levels.

6.8 Luxemburg

According to [12] Luxemburg has not adopted any authentication policy, and the situation for Luxemburg is summarized in the following table.

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA Level
0	Simple or weak identification	None	None		
1	Strong authentication	(to be provided)	Qualified Electronic Certificates (QEC) using smart card or USB tokens	(to be provided)	(4)
2	With signature	(to be provided)	Advanced Electronic Signatures based on Qualified Electronic Certificates (QEC) using SSCD or non SSCD USB tokens		(4)

Table 9: Summary of the Luxemburgish authentication levels, and preliminary mapping according to the STORK-QAA tentative levels

In the "IDABC authentication levels report" [1] there is no mention of Luxemburgish levels of authentication nor they are classified in terms of the IDABC Levels. In the last column of the table, we have indicated our proposal (numbers in brackets) for a mapping from the national Levels to the STORK-QAA tentative levels.

6.9 The Netherlands

E-government services in The Netherlands use a user name / password mechanisms called DigID. DigiD offers governmental agencies sufficient assurance of your identity, in addition to the registered address at your municipality, to which the code is send. Authentication assurance can be improved by using a one-time password sent via SMS to the user's mobile phone after having logged in using the DigiD. At most 1 DigID can be associated to a single mobile phone number. The Netherlands is considering the roll-out of a Dutch identity card (eNIK) or the associated functionality on other cards to provide higher levels of authentication.

The government agency (as a SP) decides upon which of these security levels it requires for authentication.

The following table summarizes the situation for The Netherlands, according to [12].

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA tentative level
0	Simple or weak identification	None	None	None	
1	DigiD	Online and requires a Social Security Number (or CSN after its introduction)	username and password	Tax declaration	2
2	DigiD + sms	Online and requires a Social Security Number (or CSN after its introduction)	username password + SMS (two factors authentication)	Tax declaration	3
3	eNIK (not implemented yet)	Physical presence during registration at the town hall	Authentication/signature certificate stored on the eNIK + password/PIN	Not implemented yet	4

Table 10: Summary of the Dutch authentication levels, and preliminary mapping according to the STORK-QAA tentative levels

The last column of the table indicates the mapping from the national Levels to the IDABC Levels (here adopted as STORK-QAA tentative levels), according to the "IDABC authentication levels report".

6.10 Portugal

The most significant e-IDM system in Portugal is based on the Citizen Card (Cartão do Cidadão), that is given to Portuguese citizens from the age of six and up. The Citizen Card was launched in 2007, and it is currently implemented in all districts. The roll-out will be concluded by the end of 2008.

The Citizen Card is distributed by the same institutions that provide the ID hard copy document, namely the Local Civil Registry and Citizen's Shops ("Lojas do Cidadão").

In the pilot, Portugal will provide a service of change of address for EU citizen. The service requires an authentication level 4 (associated nationally with the Personal Identity Card) or level 3 associated with PKI-based authentication solutions.

The following Table summarizes the situation for Portugal, according to [12].

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA tentative level
1	Other systems	Online	Username/password based on personal data such as the tax number and fiscal domicile;	Tax declarations, social security and customs	2
2	Justice		Advanced electronic signature in general issued by Multicert-Serviços de Certificação Electrónica, S.A.	Services enabling attorneys to file their documents	
3	eID (Citizen Card)	Physical presence at the Local Civil Registry or Citizen's Shops ("Lojas do Cidadão")	Smartcard (with an advanced electronic signature and authentication issued by the Portuguese State) and one-time password for phone authentication	Services that were accessible with the hard copy of the identity document..	4

Table 11: Summary of the Portuguese authentication levels, and preliminary mapping according to the STORK-QAA tentative levels.

The last column of the table indicates the mapping from the national Levels to the IDABC Levels (here adopted as STORK-QAA tentative levels), according to the "IDABC authentication levels report".

6.11 Slovenia

According to [12], Slovenia has adopted informally an authentication policy based on three levels. The following table summarizes the situation for Slovenia:

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA tentative levels
0	None	No registration	No authentication	Public information and services	
1		On-line registration and send-out of confirmation e-mail with username, initial password defined by the system and active URL to an address indicated by citizen	By assigned combination of a username and password chosen by user. Initial password is determined by the system. User can change the initial password upon registration with initial password.	Information/services of limited sensitivity	(1)
2		Physical identification at the registration authority for the acquisition of qualified certificate	Authentication/signature certificate + password	Information/services of high sensitivity and services requiring an electronic signature	(3)
3		Physical identification at the registration authority for the acquisition of qualified certificate	Authentication/signature certificate stored on SSCD+ password	Information/services of high sensitivity and services requiring an electronic signature	(4)

Table 12: Summary of the Slovenian authentication levels, and preliminary mapping according to the STORK-QAA tentative levels

In the last column of the table, we have indicated our proposal (numbers in brackets) for a mapping from the national Levels to the STORK-QAA tentative levels.

6.12 Spain

The most important of the existing eID token in Spain is the electronic national identity card "DNI electrónico" or "DNIe" that is a customized cryptographic smartcard whose uses and contents are regulated by law [17]

To generate this DNIe card, a person needs to be physically present at an office of the Police General Directorate where the DNIe is issued with a combination of identifiers:

- The card itself contains a general personal identification number known as DNI number (also known as NIF, CIF or NIE depending on nationality and/or other legal issues). This number is evidenced in other documents granted by the Administration such as the passport or the drivers licence. It is commonly used as authentication by knowledge mechanism.
- The chip of the document contains two types of certificates (X.509 v3): the authentication certificate and the signature certificate. These certificates are generated and granted according to legal specifications [18]

So, the DNIe card allows electronic authentication of the identity of a person in an irrefutable manner, and permit to eSign documents, granting them a legal validity identical to the one provided by the handwritten signature. These are the main reasons why the assurance level for the DNIe is considered the highest that can be achieved nowadays in Spain; and is equivalent to the proposed 4 level of IDABC.

Apart from the eID card, there are 11 other electronic identity types based on PKI certificates [19] and can be supported on different types of tokens: software, smartcards, cryptocards etc. These certificates are issued by public or private (commercial) IDPs that can be used in a large number of eGovernment applications for authentication services. The interoperability between these certificates (56 types issued by the 11 IDPs and DNIe) is guaranteed through the MAP multiPKI Validation Platform called @firma [20] that provides freely eSignature and eCertificate validation services to eGovernment services.

All these IDPs are subject to the eSignature law; but the issuing of these credentials can vary widely depending on the issuer certification practices, the certificate usage context and the registration mechanisms being applied for the issuing of tokens and/or credentials. So, the assurance level for these credentials can mainly vary between proposed level 3 and 4. A good example is Catalan Agency of Certification –CATCERT- that has published a conceptual framework for classification of evidences, which is being used by public administrations in Catalonia (see [9]) to indicate the reliability (integrity) of data.

The actual usage of authentication by means of electronic credentials has been boosted by the implantation of DNIe and the recently published law LISI, "Ley de Medidas de Impulso de la Sociedad de la Información"[21] that obliges companies to allow recognized certificates for authentication processes to access economically relevant services. So, should foresee that IDABC levels 3 and 4 will predominate in the Spanish arena in next years

Another recent law [22] is LAECSP "Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos" (law on electronic access to public services by citizens) which obliges locals governments to allow electronic access, under trusted conditions, to their administrations according to what any Administration may determine, mainly qualified electronic certificates. Thus, it is describing the authentication level 4 of IDABC.

On the other hand, the same law also envisages, but doesn't lay down, the use of weaker authentication methods previously agreed by both parts. This means that there would be coexistence of strong authentication with authentication by knowledge mechanisms like userid / password.

Recently, there has been a proposal on assurance levels for credentials depending on some conditions and had been established three levels: basic, medium, high.

The following table summarizes the above-mentioned situation for Spain.

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA Level
Basic - Level(1)	This level will admit any authentication mechanism: passwords, physical or logic tokens. If passwords are to be used basic quality assurance rules must be applied Authentication tokens either hardware, software or any other combination will have to take into account security issues: • Authentication factors or credentials are exclusively under user control • The user is conscious upon receiving the credential of the duties that must follows, particularly diligence custody and inform quickly after losing or compromised credentials. • Authentication factors or credentials will be change accordingly to the periodicity established in the Organization Policy regarding to the security level of the accessed system. • Authentication factors or credentials are to be discarded when the entity that them represents leaves the organization that stand for.	None or according to private entity information about user.	Authentication by Knowledge that takes place inserting a user name and a password or a digital certificate	Specific public or private services of relative importance such as e-mail services, banking or specific requests Note: this level can only be used by certain groups of applications and is not suitable for international usage.	This Spanish level is equivalent to Stork QAA level 1 or 2 depending on final implementation of the authentication method
Medium (Level 2)	If possible, password should be avoided. If they are to be used, strongest policies should be applied as for example quality of the password and frequently renewal. The usage of other authentication	Request must be issued online but Physical and in presence identity is required to obtain the user's	Advanced electronic signature Qualified Electronic Certificates (QEC). It is responsibility of the application	Specific public or private services of relative importance such as e-mail	This Spanish level is equivalent mainly to Stork QAA level 3 but it could

	mechanism should be recommended; for example personalized physical tokens, logic tokens	certificate.	owner to permit more or less rigid authentication methods. Usually, certificates are issued on software or hardware tokens.	services, banking medical, jobs, transportation or specific requests	also be 4 depending on final implementation of the authentication method is based on software or hardware certificates.
High (Level3)	Authenticator factors or credentials will be suspended alter a established inactivity period Use of passwords will not be allowed Personalized Physical devices are to be used Algorithm used in physical devices tokens must be accredited by Centro Criptológico Nacional Whenever possible certified product must be chosen This Spanish level is equivalent to Stork QAA level 4 depending on final implementation of the authentication method is based on software or hardware certificates.	Physical and in presence identity is required to obtain the user's certificate. According to a legal regulation	Qualified Electronic Signature Advanced Electronic Signatures based on Qualified Electronic Certificates (QEC) Level 4 only can be obtained using SSCD	Highly confidential and very personal services such as access to personal information stored by the Administration: work resume, medical history, tax payment, money transactions etc.	This Spanish level is equivalent to Stork QAA level 4

Table 13: Summary of the Spanish authentication levels, and preliminary mapping according to the STORK-QAA tentative levels

The last column of the table indicates the mapping from the national Levels to the IDABC Levels (here adopted as STORK-QAA Levels), according to the "IDABC authentication levels report"

6.13 Sweden

The solution adopted by Sweden is based on advanced certificates (both software and hardware based) in combination with revocation control (OCSP)[10]. Sweden recognizes the following two levels of authentications (called classes):

Class 1 (soft eID): Identification is performed via advanced electronic signatures with encryption keys protected in encrypted software (data file). The security requirements should correspond to the European standard ETSI TS 102 042 NCP.3.

Class 2 (hard eID): Advanced electronic signatures with encryption keys protected in hardware (microchip or equivalent). The security requirements should correspond to the European standard ETSI TS 102 042 NCP+

In the future, but there is no official timetable for that, a third class is planned to introduce qualified certificates.

Class 3 (qualified eID) Advanced electronic signatures are included as a requirement together with qualified certificates and secure arrangements for production of signatures in accordance with the Qualified Electronic Signatures Act in order to produce qualified electronic signatures in accordance with the Act's definition. The security requirements should correspond to the European standard ETSI TS 101 456.

Sweden also recognizes trust server certificates for public authorities. There is a major need to furnish authorities (and in the future also organisations and other legal entities) with tools for secure electronic exchange of information and secure handling of electronic documents. Time-stamp certificates and server certificates are such tools. There are technical standards for how these certificates are to be specified.

The following Table 14 syntheses the situation for Sweden.

[10] The OCSP (Online Certification Status Protocol) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 2560 and is on the Internet standards track.

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA tentative level
1	Soft identification	Physical presence face to face before or during registration at a bank or post office	advanced electronic signatures with encryption keys protected in encrypted software	National and regional public services as well as bank and industry services	(4)
2	Hard identification	Physical presence face to face before or during registration at a bank or post office.	Advanced electronic signatures with encryption keys protected in hardware (microchip or equivalent).	National and regional public services as well as bank and industry services	(4)
3	Qualified identification	Currently non adopted	Advanced electronic signatures+ qualified certificates and secure arrangements for production of signatures in accordance with the Qualified Electronic Signatures Act.	Currently non adopted	

Table 14: Summary of the Swedish authentication levels, and preliminary mapping according to the STORK-QAA tentative levels.

The last column of indicates the proposed mapping from the Swedish Levels to the STORK-QAA tentative levels (numbers in brackets).

6.14 UK

There is a significant discussion going on at the policy level within the UK, at the moment. UK will be refining its policy during the lifetime of the STORK project. This section reports on the examples that UK will deliver to the production Pilot for WP6.1. In the timeframe of STORK, UK will not be looking to change the processes described below.

At a very high level, the UK Government policy recognizes four assurance levels for both *registration* and *authentication*, which can be summarised as follows:

Registration

Level	Process
0	Obtain a user ID and Password in an online environment. User ID is system generated and password is selected by the user. User ID is displayed on the UI. Email address is captured for reset but it is not verified.
1 / 2 Depending on Implementation	Obtain a user ID and Password in an online environment. User ID is system generated and password is selected by the user. User ID is displayed on the UI. Email address is captured for reset but it is not verified. The user then selects a service to enrol in an online service. The user will provide known facts for the service. These known facts are matched with the known facts held by the service provider. If they match a one time activation code is sent by post to the address held in the Service Provider. The user then authenticates with their User ID and Password and enters the activation PIN for the service. They can then use the service.
2	As above but the user can provide 5 shared secrets to be used as credentials.
3	Face to face interview with an accredited registration Authority. Proof of Identity documents required. Soft Digital Certificate is issued. Only a qualified certificate if the registration authority is tScheme accredited. Certificate holds no identity Attributes.

Authentication

Level	Process
0	User ID and Password generated through the level 0 registration process. Not linked to any real world identity.
1	User ID and Password generated through the online level 1 or 2 registration process. Linked to a real world identity.
2	The UK Government Supports (or will) the following authentication mechanisms. 1. User ID, password and shared secrets all registered through the online level 2 registration process. 2. Digital Certificate issued through the face to face level 2 registration process. 3. Soft Certificate lives in the users browser. Certificate protected via a PIN. 4. Chip and PIN Authentication using challenge and response. The user types a unique identifier into a portal. The portal presents the user with a challenge (8 digit number). The user places their card into a hand held card reader and enters their PIN. The user enters the challenge and the card reader presents a response to the user. The user then types the response into the portal. 5. One time password tokens. Process is as with chip and PIN authentication but there is a token rather than a card and reader.
3	Currently the UK Government Gateway does not support level 3 authentication

When allocating registration and authentication levels to a transaction, e-Government service providers need to determine how much they need to know about the real-world identity of the client. In general, informal or lower value transactions will attract the lower levels of registration and authentication. Higher value or legally significant transactions will attract more stringent registration and authentication requirements.

There are broadly four categories of real-world identification; these are given below with their implied registration and authentication levels:

- Level 0: no confidence that the individual is who they claim to be
- Level 1: on the balance of probabilities, the individual is who they claim to be
- Level 2: there is substantial assurance
- Level 3: the identity is verified beyond reasonable doubt.

In Level 0 (Anonymous or pseudonymous), neither the real-world identity of the client nor an electronic identity in an associated credential is required to complete the transaction. In the latter case, the client provides a pseudonym (registration level: 0, authentication level: 0).

In Level 1(Anonymous or pseudonymous with electronic identity**)**, the real-world identity of the client is not required to complete the transaction, but the electronic identity enables the service provider to recognise the client in repeat transactions (registration level: 0, authentication level: 1, 2 or 3).

In Level 2 (Anonymous or pseudonymous with electronic identity and traceable), the real-world identity of the client is not required to complete the transaction, but the electronic identity enables the service provider to recognise the client in repeat transactions and it could be used to retrieve the real-world identity via the RA, if required (registration level: 1, 2 or 3, authentication level: 1, 2 or 3).

Finally in Level 3 (Real-world identity established), the real-world identity of the client needs to be established to some degree of confidence before the transaction can be performed (registration level: 1, 2 or 3, authentication level: 1, 2 or 3).

As a rule, service provision should operate on a principle of maximum anonymity consistent with necessary functionality. The table below sets out the likely combinations of registration and authentication levels that will be assigned to transactions. For example, there would seem to be little point for a transaction to need level 3 registration (extensive verification of real-world identity) and level 0 authentication (essentially unrestricted electronic access). Further guidance on the relationship between levels and assignment of a consistent set can be found in the overarching security framework.

		Authentication level			
		0	1	2	3
Registration level	0	✓	✓	✓	✓
	1	×	✓	✓	✓
	2	×	×	✓	✓
	3	×	×	×	✓

× unlikely combination

✓ likely combination

The following Table 15 synthesises the UK situation.

Authentication level	Description	Registration of identity	Authentication method	Applications	Proposed STORK-QAA tentative level
0	Anonymous	Obtain a user ID and Password in an online environment. User ID is system generated and password is selected by the user. User ID is displayed on the interface. Email address is captured for reset but it is not verified	User ID and Password (but they are not linked to any real world identity)	(to be provided)	(1)
1	Probable Identity	As Level 0 or the user will provide known facts for the service. These known facts are matched with the known facts held by the service provider. If they match a one time activation code is sent by post to the address held in the Service Provider. The user then authenticates with their User ID and Password and enters the activation PIN for the service.	User ID and Password generated through the online level 1 or 2 registration process.	(to be provided)	2
2	Assured identity	As Level 1 or the user can provide 5 shared secrets to be used as	User ID, password and shared secrets all registered through the online level 2 registration process. or	(to be provided)	3

		credentials	Digital Certificate issued through the face to face level 2 registration process or Soft Certificate lives in the users browser. or Certificate protected via a PIN. or Chip and PIN Authentication using challenge and response. or One time password tokens. Process is as with chip and PIN authentication but there is a token rather than a card and reader		
3	Undoubted identity	As Level 2 or Face to face interview with an accredited registration Authority. Proof of Identity documents required. Soft Digital Certificate is issued.	Currently non supported		

Table 15: Summary of the English authentication levels, and preliminary mapping according to the IDABC Levels

In the last column, we have reported the IDABC Levels. According to the "IDABC authentication levels report" [1] only level 1 (self-chosen username and password in order to access the Government gateway) and 3 (soft qualified signature certificates from the British Chamber of Commerce and Equifax) are implemented.

6.15 Overview of the STORK-QAA Scheme for the member states

Based on the inventory made in the previous sections, the table below provides a preliminary mapping between the authentication assurance levels of the member states and the STORK-QAA tentative levels. It must be stressed that the mapping is preliminary and tentative; for example, it also does not include the legal aspects, which will be analyzed and considered inWP2.2. The final version of the mapping will appear in deliverable D2.3.

	STORK-QAA tentative Level 1	STORK-QAA tentative Level 2	STORK-QAA tentative Level 3	STORK-QAA tentative Level 4
Austria				Level 1
Belgium	Level 1	Level 2	Level 3	Level 4
Estonia		Level 1 (with username and passwords 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)
Luxemburg				Level 1, Level 2
The Netherlands		Level 1	Level 2	
Portugal		Level 1		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 16: Resume of the preliminary mapping, for each member states, between the national levels and the STORK-QAA tentative levels.

7 Conclusions and Open Issues

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. A common framework is required to reach interoperability in authentication.

This deliverable provides an overview of today's eID solutions offered by the member states and of their corresponding assurance levels; it also highlights the differences of interpretation between the nations that might cause difficulties. Nevertheless, the research performed in this deliverable shows that all the member states fundamentally recognise compatible categories of eID assurance, which informally can be expressed as follows:

- eID is a courtesy only;
- eID is required, authentication of the ID has la ow assurance;
- eID is required, authentication of the ID has a medium assurance;
- eID is essential, authentication of the ID has a high insurance

On this base, the deliverable investigates on a classification scheme that the member state can use to classify their solutions with respect to common authentication assurance levels for pan European authentication interoperability framework. As a proposal, this deliverable adopts the scheme that has been described in a previous IDABC work (see [1]) and that proposes a multi-level authentication mechanism for a pan European eID Interoperability.

By basing its framework onto [1], STORK aims for an approach that is less technology based and more on processes. As advised by some member states, this deliverable agrees that technology references must be taken as much as possible as examples and as least as possible as normative statements. Therefore, the preliminary proposal for a STORK-QAA level framework recognizes (as the IDABC does) four levels of assurance (called STORK-QAA levels) which are based both on organizational and on technical properties of the authentication process (composed by registration and electronic authentication sub-processes).

The preliminary STORK-QAA level framework, as follow-up on the IDABC framework, provides a set of definition of registration requirements and a set of definitions of authentication requirements for solutions to be used at each of the four assurance levels (cf. [1]). As a kick-off for the work in deliverable 2.3:, this deliverable suggests also a preliminary mapping from the national authentication assurance levels into the tentative STORK-QAA levels.

More research is needed for future pan European service provisioning. Legislation may bring additional constraints, but also the service providers might require more granularities in the assurance levels. The legal aspects will be addressed in deliverable D2.2 of WP 2, whilst WP 6 will indicate whether more granularity is desired by the service providers. Together with this deliverable, the legal aspects and the service providers requirements (if any) will result in the eventual STORK Authentication Framework, which is scheduled for deliverable D2.3.

The consortium is currently discussing open issues like, for example, what are the attributes that compose an identity, and how to measure the quality of an identity attribute (data with quality can be useful in case of low level of authentication). These open issues are going to be addressed in the overall quality authentication assurance framework in deliverable D2.3. The consortium is also preparing a WP glossary, which will be published in a separate document that will be used by all the WP deliverables.

References

[1] 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).

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

[3] STORK: Secure Identity Across Borders Linked. ICT-PSP/2007/1 project proposal, 2007

[4] H. Leitold, personal communication (by mail of the 02 September 2008)

[5] IDABC – European e-Government Service, eID Interoperability of PEGS: Analysis of Assessment of Similarities and Differences – Impact on eID interoperability, November 2007 (http://ec.europa.eu/idabc/en/document/6484/5938)

[6] M. Stern, personal communication (by email of 18 September 2008)

[7] W. Arvid, personal communication (by email of the 19 September 2008)

[8] T. Schneider, personal communication (by email of the 18 September 2008)

[9] Ignacio Alamillo and José Manuel López, Marco Conceptual de Clasificación de Evidencias, CATCERT, vv1.0

[10] Central Sponsor for Information Insurance (CSIA), Registration and Authentication: e-Government Strategy Framework Policy and Guidelines, vv 3.0, September 2002 (http://www.cabinetoffice.gov.uk/csia/publications.aspx)

[11] T. Martens, personal communication (by mail of the 22 September 2008)

[12] IDABC European e-Government Service, Multilevel authentication mechanism: Summary of the existing national and other authentication schemes. November 2007 (http://ec.europa.eu/idabc/en/document/6484/5938)

[13] R.V. van Wielink, Complexity and Granularity of User Privacy Preferences in Context-Aware Systems, Bachelor Assignment Telematics, University of Twente, 2007

[14] Grandison, T., & Sloman, M. (2000) A survey of trust in internet applications. IEEE Communications Surveys and Tutorials, 4(4), pp 2–16.

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

[16] PRIS v2.1, A general Security Frame of Reference (http://www.synergies-publiques.fr).

[17] Royal Decree 1553/2005, of December 23, ruling the national identity card and its eSignature certificates. http://www.dnielectronico.es/marco_legal/RD_1553_2005.html

[18] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf And the (eSignature) Ley 59/2003, de 19 de diciembre, de firma electrónica. http://www.mityc.es/NR/rdonlyres/62297ED5-20DF-426B-B2DD-9A76996527A0/0/15LEY59_2003.pdf

[19] IDABC – European e-Government Service, eID Interoperability for PEGS NATIONAL PROFILE SPAIN November 2007 http://ec.europa.eu/idabc/servlets/Doc?id=31527

[20] @firma more detailed information at: http://www.csi.map.es/csi/pg5a12.htm and http://www.dnielectronico.es/seccion_aapp/platform.html

[21] Boletín Oficial del Estado 29/12 año 2007, número 312. Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/22440

[22] Ley Para el Acceso Electrónico de los Ciudadanos a los Servicios Públicos. BOE 23-06-07 http://www.map.es/iniciativas/mejora_de_la_administracion_general_del_estado/moderniza/Administracion_Electronica/parrafo/05/document_es/A27150-27166.pdf