enisa
European Network
and Information
Security Agency

National eIDs in pan-European e-Government Services

Mapping security services to authentication levels

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created as a response to security issues of the European Union. The Agency's Mission is essential to achieve a high and effective level of Network and Information Security within the European Union. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between European institutions, the Member States and industry players.

Contact details

For enquiries on this study please use the following details:
European Network and Information Security Agency
Technical Competence Department
Email: sta@enisa.europa.eu
Internet: http://www.enisa.europa.eu/act/it/eid

Supervisor of the study: Sławomir Górniak – ENISA
Authors: Stephan Körting, Diana Ombelli – HJP Consulting
ENISA staff involved in the project: Rodica Tirtea, Demosthenes Ikonomou

Acknowledgements

We particularly wish to thank all those working in the STORK project for their support during the compilation of this study.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Table of Contents

1 – Summary

Since the beginning of the 21st century, European Member States have been planning, developing and implementing new solutions to offer electronic services to citizens and businesses on a digital platform. The common denominators for these eGovernment services are improving administrative efficiency, accessibility and user-friendliness and, above all, reducing costs. However, different national legal frameworks, technologies and security policies have often led to slightly dissimilar implementations, thereby impeding progress towards the ideal of free movement of citizens within the European Union.

As it was not efficient or feasible to restart from scratch, policy makers and experts agreed on the desirability of finding solutions that would allow all stakeholders to work together across (digital) borders, while respecting the autonomy of the Member States. Several projects were then started in order to generate the required solutions. One of the directions taken by IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens) **[1]** defined a model, which included levels of authentication. Later those levels were mapped to the existing authentication solutions in the European Member States and some discrepancies were identified. Also, the discussion on security issues in cross-border electronic authentication recognised that some issues needed to be addressed. In the meantime, a number of countries cooperated to offer electronic services, which have been successfully activated and several pilots are still running.

This report reviews the authentication levels and their mapping to public electronic services in the eGovernment programme framework, which require an authentication of the user (security services). For instance, citizens are allowed to complete and send their tax declaration by electronic means, or use a smart card to identify themselves prior to receiving benefit from health care services. The draft of this report has been submitted to experts and their opinions have been included in the revised version.

The first part of this report gives a general overview of European efforts and particularly the activities of STORK (Secure idenTity acrOss boRders linked) **[2]** in relation to the levels and the mapping. Essential concepts in IT security are explained and the mappings are illustrated by everyday life examples.

The second part of the report details the issues that may be or have been encountered by applying the model to electronic services. The definition and separation of the levels, as well as the assessment and validity of the levels present some concerns, which need to be addressed in order to facilitate their application. The report includes recommendations and suggestions for a further fine-tuning of the model. These can be summed up as follows.

Authentication levels should be clearly defined without leaving any room for interpretation or ambiguity.

To make pan-European authentication levels acceptable and useable for service providers, a guideline should be developed on how to evaluate these levels in respect of the security demands of an offered electronic service.

A pan-European interoperable authentication solution will only be accepted by service providers and citizens if it is perceived as transparent and trustworthy. Therefore, any authentication levels and their mapping to national solutions must also fulfil these requirements.

Regular re-evaluation of levels and mappings is necessary for continued security. A procedure should be established to perform evaluations and mappings in a formal and transparent way.

2 – About the document

2.1 Glossary and abbreviations

Please note that the explanations provided in this glossary may only be considered normative within the scope of this report, because of differences in interpretation of terms within different contexts (e. g. the definition of confidentiality by STORK differs significantly from that found in ISO 27000 **[4]**). Beyond this background, the glossary attempts to explain the terms in a way that is easily understood without compromising the meaning. Due to this, explanations may be based on standards and existing glossaries, but have usually been edited, so as not to introduce additional terminology.

Authentication	a procedure to establish or confirm that someone or something is genuine (authentic)
Availability	a fundamental IT security value on ensuring that an asset is accessible and useable when needed by an authorised entity
CA	Certificate Authority
Certificate	an electronic document establishing a digital identity by combining the identity name or identifier with the public key of the identity, a validity period and an electronic signature by a third party
Certificate Authority	an trusted third party that issues digital certificates for use by other parties
Confidentiality	a fundamental IT security value associated with ensuring that information is accessible only to those authorised to have access
Credentials	a letter or certificate giving evidence of the bearer’s claimed identity or competence (including username/password and other electronic representations)
Credentials service provider	An entity which creates and delivers credentials
eGovernment	the use of Information & Communication Technologies (ICTs) to make public administrations more efficient and effective
eIDM	Electronic Identity Management
ICT	Information and Communication Technology
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens
Integrity	a fundamental IT security value associated with ensuring the protection of the accuracy and completeness of information
Interoperability	the ability of two or more systems to exchange information and to use the information that has been exchanged
IT	Information Technology
PEPPOL	Pan European Public Procurement OnLine

Registration Authority
(within the context of eIDM) an entity that vouches for the identity of an individual when this individual completes a qualifying process and which can revoke this electronic identity.

Revocation
The process initiated by the CA, which cancels the validity of a certificate.

Service
a set of related functions, governed by a policy, which are offered within a system. In the eGovernment context, the term ‘Service’ usually describes those functions which are offered by a public entity within the scope of one application

Service provider
an entity that offers and supplies a service to other system participants

SPOCS
Simple Procedures Online for Crossborder Services

STORK
Secure idenTity acrOss boRders linked

STORK QAA scheme
The 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

STORK QAA level
STORK Quality Authentication Assurance levels. These are four levels of authentication assurance, which facilitate the mapping of national authentication level and eID solutions on to each other

Token
a container for credentials, within the eIDM context, usually an electronic representation of the credentials (e.g. a certificate), with an optional hardware component serving as container for this electronic representation (e.g. a smart card)

2.2 Approach

The authors will firstly introduce the reader to the general topic of electronic identity management and its mechanisms, using real world examples. They will explain the key concepts needed to understand the necessity of having a European Union-wide common approach to quality and security for the providers and users of electronic services. The applicability of a known quality model will be reviewed. The second part will include an analysis of the model and recommendations for improving the model.

3 – e-Identity management in the European Union

3.1 Introduction to e-Identity management

There was a time when people were born in small communities. Travelling was exceptional and they usually lived in the same place their entire life. Therefore, they knew each other as complete generations by name and face, which facilitated all kinds of social and business interactions. Family ties, honour and fame enhanced trust among these people, allowing all services to be performed in good faith. Credit was granted at the grocery store and any family member could collect mail at the post office. Today, the communities we live in are huge and more often than in the past social or business interactions do not involve personal acquaintance. While it is still possible to receive the benefits of services delivered in good faith, authentication procedures have been formalised. Thus issuing a credit card requires the applicant's identity to be verified. Registered mail can be given only to the addressee or, by proxy, to anyone authorised by the addressee. The post office clerk is then supposed to verify the identity of the customer.

During the last three decades, the automation of all kind of business processes opened the doors to new opportunities and markets. Information was made available at previously unknown speed, even from the most remote locations. Information technology (IT) therefore became very attractive to governmental activities, which aimed to improve administrative efficiency, accessibility and user-friendliness and, above all, to reduce costs **[1]**. Citizens - actual people - became users.

Initially, the IT systems were built to serve users from the same (governmental) entity. From that moment, users could access digital information possessing basically the same value as its physical counterpart. But how could providers make sure that only authorised users access the data?

> *The procedure, which establishes or confirms that someone or something is genuine, is called authentication.*

Since computer driven systems are dehumanised, new techniques became necessary to perform the authentication of users. First they were taught to type a password. The electronic identity of the user was therefore composed of the user's name (or pseudonym) and his/her password (credentials[1]). The system could then 'recognise' the lawful users and reject the unauthorised users. However, no one could prevent the (informal) exchange of one other's user names and passwords, in order to access the data using someone else's credentials.

Technology moved quickly forwards, allowing remote connections to networks and databases. People could collect cash at every bank branch or enter a country by a port of his/her choice. Where new opportunities grow, there are always new threats from people who want to maximbenefits with minimal effort, using illegitimate means. In the past, threats were often countered after they had already occurred often enough to become noticeable, whereas today, preventive measures are taken in advance. Therefore, risks have to be evaluated, taking into account the likelihood that they will occur and the potential damage that may be caused. Finally, countermeasures have to be taken to prevent abuses. Over recent years, information technology has needed more and more security in order to protect data and trusted users.

[1] Please note that this section introduces some technical terms in an understandable, but informal way. For a more exact definition of these terms please refer to the glossary and existing standards.

Such a security assessment involves several steps. First of all, the value of the information is assessed and the group of people allowed access to it is defined (confidentiality)[2]. Then the reliability and accuracy of the information will be ascertained (integrity)[3] and last but not least, it is important to ensure that systems responsible for delivering, storing and processing information are accessible when needed (availability)[4]. Systems are considered more and more crucial and procedures are set up to make sure that confidentiality, integrity and availability are guaranteed over their entire life-cycle.

In the last decade, the number of electronic services offered by governmental entities or commercial companies has multiplied. Citizens are forced to remember their user name and dozens of passwords, due to different registration and authentication policies. One real life person has multiple e-identities to manage. Think of the large numbers and types of credentials you use every day to access all kind of online services, from social networks to banking systems. Nevertheless, this is conducive to privacy, as these e-identities and the linking ability of the supplied information is often in control of the user. On the other hand, governments need citizens' trusted identities to provide them and only them with the required services.

Electronic Identity Management (eIDM[5]) is a cornerstone of the implementation of the full range of eGovernment services, for both citizens and businesses across the European Union. As nowadays more governmental, personal and commercial transactions are conducted, electronic parties need to be sure of a person's or an organisation's identity, thus increasing the need for effective and appropriate authentication mechanisms.

The following scheme shows the steps involved in the registration and authentication of a citizen as a new user.

Registration phase	
ID proofing	The citizens provide their personal information to the registration authority (e. g. municipality or police).
Vouching of ID	The registration authority transmits the personal information to the credentials service provider, in other words the electronic identity will be set up.
Delivery	The credentials of the electronic identity are delivered to the citizens. This could also include a token (e. g. a smart card).
Electronic authentication phase	
Proof of possession	The citizen would like to access an online service using his/her electronic credentials. He/she enters the credentials into the system (e.g. by inserting the smart card in the reader connected to a PC), the electronic credentials on the card are read and transmitted from the service provider to the verifying party.
Assertion delivery	The verifying party confirms to the service provider that the citizen is trusted. The access is unlocked and the citizen can use the service.

Table 1: Steps involved in the registration and authentication of a citizen

[2] To protect and preserve the confidentiality of information means to ensure that it is not made available or disclosed to unauthorised entities. In this context, entities include both individuals and processes. [5], [5]

[3] To preserve the integrity of information means to protect the accuracy and completeness of information and the methods that are used to process and manage it. [4], [5]

[4] Availability is a characteristic that applies to assets. An asset is available if it is accessible and usable when needed by an authorised entity. [4], [5]

[5] ENISA reports in this area are available at http://www.enisa.europa.eu/act/it/eid

While just about every eIDM solution contains these steps, organisational, functional and technological implementations differ widely.

Since the year 2000, huge efforts have been made to plan, develop and deploy solutions related to electronic identity management in European Union Member States and EEA countries. Although all governments have substantially identical goals, the way chosen to realise them varies considerably from country to country, because of national legislation, technology preferences and policy. In summary, there is no unique and comprehensive EU-wide eIDM legislation, with policies instead being set on national levels. If you consider that almost 12 millions European citizens are living permanently in another Member State and that there is a growing mobility of students and teaching staff (e.g. within the Erasmus programme), you see why setting up a European Union-wide policy in eIDM is an important step towards the idea of free movement of citizens within the EU. In 2006, a roadmap was created within the framework of the Modinis IDM project, called the eID roadmap **[8]**. This includes specific milestones and actions needed to realise the European Union's ambitions in respect of eIDM (cf. further details in section 3.3).

3.2 Current barriers to interoperability

It has quickly become obvious that a trade-off needs to be made between the freedom of Member States to introduce electronic identity solutions and the demand that citizens can use them independently from the source of their electronic ID (interoperability). Even on a national level, eGovernment applications have some issues accepting other electronic IDs from other applications. Extending this interoperability beyond national borders poses even more challenges.

Several types of barriers are currently limiting cross-border interoperability, mainly:
- Legal
- Technical

3.2.1 Legal barriers

National legislation regulates how to handle privacy issues, e.g. by imposing restrictions on the use of national identification numbers and other identifiers. The requirements for how to process those identifiers are defined by the individual Member States, the majority of which do not permit the usage of the identifiers outside their own jurisdiction, while some even limit the use within their borders. Electronic identity documents containing such information (so called certificates) therefore may have restrictions in respect of their cross-border usage **[1]**.

A comprehensive study of the current type of authentication certificates employed on eIDs is included in **[5]**, section 3.4.6 "Certificates and smart cards".

The European Union introduced several Directives, establishing an initial legal frame:

I. Directive on the protection of personal data 95/46/EC **[9]**
II. Directive 1999/93/EC on a Community framework for electronic signatures **[10]**
III. Directive 2006/123/EC on services in the internal market **[11]**
IV. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communication sector **[12]**

Since these existing European Union regulations offer scope for freedom in the implementation of e-identities, every Member State tends to implement one solution that is best fitted to their national legislation.

The security (and therefore the trustworthiness) involved in the authentication of an e-identity at a local, regional or national level can vary considerably. While a local entity could choose to assure someone's identity simply by asking the user to reply to an email, a regional or national entity may instead prefer to see the citizen in person, at least once. This also depends on the type of service provided. The delivery of tokens or credentials can again entail several security options, some of which could involve third parties. Those aspects create a complex security environment, where it is not clear how liability is handled when extending the range of an eID's usage. Which entity is liable for someone's eID? Table 1 in section 3.1 shows clearly that there are multiple parties involved in an individual's electronic identity. Can the Directive on electronic signatures be applied on the basis of similarity? As this is not a legal discussion paper, but a description of the current situation in eID interoperability, the question remains unresolved for the moment.

Finally, consider how different is the real world identity of actual people, where identity theft needs a huge effort to be achieved (think of impersonating someone by imitating his/her habits and looks). It may be possible for skilled criminals or imprudent users to compromise electronic identities, but luckily there are procedures that allow an electronic identity to be revoked.

3.2.2 Technical barriers

Some European Member States have not yet implemented national e-identity schemes, or may not even intend to do so in the near future. This leads to multiple local/regional e-identities, which are fairly often bound to single applications. Is the quality of one of those identities sufficient to be used in the context of a national cross-border application? Can the credentials of such an e-identity be trusted in a cross-border scenario? To what level of required security can this trust be extended?

In order to establish criteria, which can be used to compare the different technical solutions, a quality assessment approach is adopted. This is described in section 3.5.3.

3.3 European initiatives

What has been done in Europe to improve interoperability?

First of all, a basic consensus has been reached! EU Member States have agreed on objectives for optimising the means to be deployed for the electronic identification of citizens.

The first European initiative directly related to electronic identity management was the release in 2005 of a paper called Signposts towards eGovernment 2010 **[12]**, stating:

By 2010 all European citizens, businesses and administrations shall benefit from secure means of electronic identification (eID) that maximise user-convenience while respecting data protection regulations. Such means shall be made available under the responsibility of Member States but be recognised across the EU.

Later, the 2006 eGovernment action plan identified several key milestones to be achieved by 2010. These included the agreement of an eIDM road map, common interoperability specifications and monitoring of large-scale eIDM projects.

Interoperability should be achieved by introducing (among others) a model which is federated, that is respecting the autonomy of different administrations, and multi-level, allowing different levels of authentication.

From the application point of view, the Directive Services established in 2006 sets up "points of single contact" in each Member State. These are contact points for businesses, which can get clear and exhaustive information on administrative procedures and specific requirements. Businesses can complete the required procedures online, such as registration in commercial and professional registers, obtaining permits or licences, submitting notifications by filing requested information online and receiving decisions etc. This is achieved by a national e-government portal accessible via the internet **[14]**.

In January 2009 ENISA released a report reviewing the state of pan-European eIDM initiatives **[1]** considering the policy, infrastructural and application levels. The authors concluded that advances have been made in the European eIDM agenda. However, outcome and benefits from different initiatives will need to be combined to update the global vision for European electronic identity interoperability.

Additional historical and background information can be found in the ENISA Report on the State of pan-European eIDM initiatives **[1]**.

Five years after the Signpost paper, interoperability is still high on the Commission's to-do list. In May 2010, the European Commission launched a new programme, Europe's Digital Agenda, stating:

The Agenda outlines seven priority areas for action: creating a digital Single Market, greater interoperability, boosting internet trust and security, much faster internet access, more investment in research and development, enhancing digital literacy skills and inclusion, and applying information and communications technologies to address challenges facing society like climate change and the ageing population. **[15]**

Current activities directed towards greater interoperability are performed in the ICT Policy Support Programme under the Competitiveness and Innovation Framework Programme (CIP). ICT Policy Support Programme (ICT PSP) is a major component of the EU's Competitiveness and Innovation Framework Programme (CIP, 2007-2013). It aims at a wider uptake and best use of Information and Communication Technologies and digital content by citizens, governments and businesses, in particular SMEs. The main objective is to develop pan-European, ICT-based solutions and services, most notably in the areas of public interest.

It includes the following pilots:

- STORK: Secure idenTity acrOss boRders linKed[6]
- SPOCS: Simple Procedures Online for Crossborder Services[7]
- PEPPOL: Pan European Public Procurement OnLine (PEPPOL)[8]

While STORK is focusing on electronic identity, SPOCS and PEPPOL are mainly orientated to offer interoperable e-Government solutions for businesses.

In December 2006, the European Parliament and the Council adopted the Directive 2006/123/EC on the services of the internal market. The objective of the Services Directive is to release the untapped growth potential of services markets in Europe by removing legal and administrative barriers to trade in the services sector. In turn, Project SPOCS aims within the context of the Services Directive to provide seamless, cross-border electronic procedures for setting up a business in another EU country,. The project builds on solutions developed in Member States as they implement the Services Directive. SPOCS' goal is building the second generation Points of Single Contact through the availability of high impact electronic procedures. Therefore, its objective is cross-border interoperability based on existing systems. SPOCS has made public its draft specifications of a European interoperability layer for eGovernment services.

Furthermore SPOCS is expected to **[16]**:

- Develop a pan-European interoperability layer for accessing information and processing Service Provider Dossiers electronically and across borders in the context of the Services Directive
- Improve the competitiveness of European businesses and particularly SMEs by enabling all businesses – national and European - to benefit from the reduction of administrative burdens
- Enable all Member States to quickly adopt the solutions developed and scale them to all sectors impacted by the Services Directive

The objective of the PEPPOL project is to set up a pan-European pilot solution that, conjointly with existing national solutions, facilitates EU-wide interoperable public eProcurement. Although governments are the largest buyers in the European Union, they are not using the technological opportunities to manage procurement electronically. Lack of electronic data exchange standards prevents companies from participating without barriers in public procurement processes. In 2005, EU member states set ambitious objectives, declaring that "by 2010 all public administrations across Europe will have the capability of carrying out 100% of their procurement electronically and at least 50% of public procurement above the EU public procurement threshold will be carried out electronically." **[17]**. The broader vision of PEPPOL is that any company (incl. SMEs) in the EU will be able to communicate electronically with any EU governmental institution for all procurement processes. The final outcome of PEPPOL will be an interoperational environment built upon national systems and infrastructures supporting the full cycle of eProcurement activities.

In the following section we present the project STORK and its objectives.

[6] https://www.eid-stork.eu/
[7] http://www.eu-spocs.eu/
[8] http://www.peppol.eu/

3.4 STORK

The European eID project fact sheet states:

"Several barriers to free movement of workers still exist in the EU: for example, it is not easy to access public services while working or living in another country. The European Commission has launched a pilot project to remedy this situation with an EU-wide system for the recognition and authentication of electronic identity (eID via electronic cards or other means). It will enable businesses and citizens to securely use their national electronic identities and get help from public administrations in any Member State they live in or travel to." **[18]**

STORK (Secure idenTity acrOss boRders linKed) is a project within the ICT Policy Support Programme under the Competitiveness and Innovation Framework Programme (CIP). The timeframe of the STORK project is three years (2008-2011).

3.4.1 Goals

Stork aims to enable businesses, citizens and government employees to use their national electronic identities in any Member State. A survey conducted by the European Commission in 2007 showed that a majority (28 out of 32) of the European countries use an electronic ID scheme or plan to introduce one. While some countries have signed agreements on mutual recognition, eID systems differ from one Member State to another and interoperability across borders is almost nonexistent. Exceptions are some applications, especially in the area of customs and taxes where this has been successfully introduced with a point of single contact, but these are limited strictly to those applications.

3.4.2 Pilots

Until now, the achievements of STORK are mostly technical deliverables on various aspects related to the interoperability of eGovernment services, ranging from security specifications to systems architecture proposals.

STORK activities also include the implementation and test of the common specifications by means of pilot services. The objectives can be summarised as follows:

- Implementation and demonstration of interoperability services
- Operations between cooperating Member States in the context of the pilots, taking as a starting point the services that are already operational at national level
- Final implementation of an open, common interoperable service solution based on an initial common specification agreed amongst participants in the pilot. During the course of the pilot, the initial common specification will be further developed and gain a wider agreement, with a view to eventual scalability

The pilots refer to real life services, and include different Member States, different domains (G2B, G2C, G2G, B2B, B2C) and different existing eID solutions.

- Pilot 1: Cross border authentication platform - for electronic services
- Pilot 2: Safer Chat - to promote safe use of the internet by children and young people
- Pilot 3: Student Mobility - to help people who want to study in different Member States
- Pilot 4: Electronic Delivery - to develop cross-border mechanisms for secure online delivery of documents
- Pilot 5: Change of Address - to assist people moving across EU borders
- Pilot 6: ECAS integration – integrating the European Commission Authentication System for Administration to Administration services

More information on those pilots can be found in **[19]**.

3.5 IT security Issues of pan-European eID management

European Union Member States have wide freedom in designing and deploying eID schemes. Recent surveys [5], [20], [21] and [22] show a heterogeneous display of solutions, involving different levels of security and privacy for the authentication of users.

Although the smart card industry, backed by the European Committee for standardisation (CEN), developed and published technical specifications for the European Citizen Card (CEN/TS 15480 series), a legal framework for the creation of a pan-European eID (card), based on common technical specifications and allowing 100% interoperability, is as yet missing.

Interoperability between government bodies' Information and Communication Technologies (ICT) systems requires them to be compatible in several ways [23]:

- Software and hardware systems need to be capable of exchanging information
- Secure infrastructure to transmit data is essential
- Systems have to have the same understanding of the data they share
- When data are in different languages, eGovernment systems need to be able to match the data to labels in their own language, and if necessary translate them before they can process them
- Organisations wishing to collaborate and to share data electronically may need to alter their internal structures to be able to do so efficiently. This is particularly the case for public bodies dealing with people or companies from other countries, whose qualifications or documents often do not exactly match those required from nationals, or whose appropriate documents may not exist at all. Processes have to be adapted, to ensure that non-nationals are not discriminated against in the internal market.

Therefore solutions need to be found to allow European service providers and users to deal with each other in a secure, reliable and trusted manner. The STORK approach defines abstract authentication levels based on characteristics of the processes involved (aka attributes) leading to a Quality Assurance of Authentication methodology, in order to assess the level of quality offered by a given authentication system.

3.5.1 IT security and standardisation

This section sets out to explain the basic concepts of IT security, which are needed to understand thoroughly the technical issues related to the secure interoperability of the Member States' authentication solutions, without going into too much technical detail.

Information security is defined as the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities [6] Information technology security (or IT security) aims at establishing information security, while using information storing or processing systems (IT systems).

When it comes to IT security, two fundamental principles are considered best practice by any acknowledged standard:

- On evaluating security requirements, the highest requirement or the highest perceived possible damage risk will prevail in assessing the total risk *(maximum principle)*
- On evaluating security measures, the least efficiently countered possible attack (or more exactly the least efficient measures against such an attack) will define the overall security reached *(minimum principle)*.

To illustrate the concept of the maximum principle on assessing security requirements, we will use a real world example. Think of an electronic health card, which stores personal information, insurance information and medical information for emergencies. Now imagine that someone would be able to manipulate that information.

- With manipulated personal information an impostor could gain illegitimate access to health services, which would be billed to the health insurance company, causing losses of perhaps several thousand Euros
- With manipulated insurance information the card holder could gain illegitimate access to health services, which would eventually not be covered by the health insurance, damaging the health service provider in terms of perhaps several thousand Euros
- With manipulated medical information, vital data on the card holder's condition could be suppressed. If, for instance, a critical medical condition was erased (the holder being a haemophiliac, allergic to a common medication or a diabetic), the card holder could actually die in an emergency if treated according to the available data.

Obviously, the highest possible damage is that to the health and life of a person (compared to limited monetary damages). Thus the integrity (and by corollary the trustworthiness) of the data on the health card must be protected against this level of risk[9].

Now let us look at the minimum principle used to assess security mechanisms, again taking a simple real world situation. Think of a bank's physical security (which is to some extent also evaluated when looking at IT security). Our special bank would have a very sophisticated and secure front door access mechanism for customers, capable of withstanding every known attack for long enough to initiate detection. At the rear of the bank there would be a back door for the staff, which is just a normal door without any enhanced security.

The back door would obviously be the weakest link, and would downgrade the overall security level of the bank. While this is clearly obvious in this example, IT security assessments too often show schemes that tend to depend overly on single technological security measures (e. g. a smart card), with security leaks in the organisational and operational setup.

Any single high-class security measure will be of little use, unless it is surrounded by equally effective measures.
Or to quote the well-known saying: a chain is only as strong as its weakest link.

Best practices in IT security can be found in ISO standards **[4]**, **[5]**, **[6]** as well as in standards provided by BSI **[24]**, **[25]** and NIST **[27]**, and **[28]**, and the Information Security Forum **[29]**.

3.5.2 Risk assessment

The security requirements of an IT system are identified through a methodical assessment of security risks **[26]**.

> *According to ENISA's risk analysis methodology [36], the final risk and its value are a function of the three elements, namely:*
> ***Risk = f(Asset, Vulnerability, Threat)***

Imagine that you have a library card. The procedure to borrow a book includes only the registration of your user identification number. In the event that the card is stolen or lost, everyone can use it, acting as an impostor. The probability that it would happen is therefore quite high and the consequences are social and financial. You will need to prove that you didn't borrow any books, as you don't have the card any more (did you report the theft/loss of the card?).

A risk assessment allows the determination of the extent of a potential threat and the risk associated with it **[31]**.
The risk assessment could then lead to a change of the security policy, introducing a second authentication element (PIN, photograph on the library card, etc.) in order to limit the risk of impostors borrowing books.

This risk assessment method has been applied in the IDABC Report 'Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms' to put forward a possible approach to managing risk and determining authentication assurance levels **[32]**.

[9] Since this is just an example, we assume that the health card stores all data in the same way and does not have different mechanisms for protecting data integrity.

The ENISA paper 'Security Issues in Cross Border Electronic Authentication' **[33]** proposes a model for assessing the security risks in the area in question. Two case studies illustrate the model. The authors come to several conclusions: the legal framework with respect to data protection and electronic transactions needs to be clear and on target; the reliability level of user credentials in Europe is varying. A strong recommendation is made in relation to a common (IT) security policy for all participants in the cross-border exchange, which would include deployed technologies (bridging possibly differences) and online connections.

3.5.3 STORK quality levels

Among the first works that explored the means for achieving the federated and multi-level model of pan-European interoperability of electronic identities were the "IDABC report on authentication interoperability" **[34]** and the "Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms"**[32]**. The goal of the first document was to present common specifications for interoperable identity management from the available national information and the resulting analysis and assessment of the gathered information. The specification aimed to provide a high level model of the functionalities that should be supported **[34]**. In the second report, a multilevel authentication policy was defined, which could be used to assess the security and reliability of any authentication solution, regardless the technology being used **[32]**.

Based on this report the STORK project released the paper D2.3 - Quality authenticator scheme.

STORK QAA (Quality Authentication Assurance) levels are layered according to the severity of the impact of damages that might arise from misappropriation of a personal identity. The more severe the likely consequences are, the more confidence in an asserted identity will be required from a service provider's perspective, in order to engage in a transaction. **[21]**

The main risk considered in the STORK approach is that someone uses a fake (or stolen) identity to perform online activities. In the previous section 3.5.2, 'impostor' indicated a possible situation of misappropriation of identity. The STORK Quality Authentication Assurance methodology estimates the consequences of this misappropriation and the gravity of the consequence is then linked to the required level of confidence. For instance, in the case of the library card, the consequences of misappropriation can be evaluated as medium (social and financial aspects are involved, which may be damaging, but not to the extent of threatening social or financial existence). Therefore, the user identification number is not sufficient to guarantee a sound authentication of the library user. Other identifiers need to be combined with the number and the card.

Impact levels are defined as "very low/negligible", "low", "substantial" and "heavy". Unfortunately, those attributes are neither defined in the same way as in the IDABC report, nor in a measurable way and therefore leave room for subjective interpretation.

In order to assess the quality of the authentication process, the STORK approach specifies relevant factors for each step within the process. Each option is then associated with one of four quality levels.

Requirements for the registration phase	Quality of the **identification** procedure	This takes into account aspects like the physical presence of the claimant, the quality of the assertions and their validation
	Quality of the **identity issuing** process	This considers the manner by which the credentials are created and delivered.
	Quality of the **entity** issuing the identity credential	Is the entity operating within a governmental agreement?
Requirements for the electronic authentication phase	**Type and robustness** of the identity credentials	Ranging from username/password to "hard" certificates.
	Security of the authentication mechanism	Protection offered by the authentication mechanisms against attacks.

Table 2: Overview of the aspects considered in the STORK QAA [21]

		Assurance level for electronic authentication phase (EA)			
		EA1	EA2	EA3	EA4
Assurance levels for registration phase (RP)	RP1	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1
	RP2	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 2	STORK QAA Level 2
	RP3	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 3
	RP4	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 4

Table 3: Computation of the overall QAA Level [21]

Examples of these levels are described in section 3.7.

3.6 Importance of the correct mapping to QAA levels

Service providers need to be confident in someone's eID in order to allow the user to perform the electronic transaction. The more severe the likely consequences of misappropriation of an eID are, the more confidence is needed. In the previous section, the methodology for the assessment of the level of confidence has been described (QAA). Now we come to the practical application of the methodology to the EU Member's eID schemes. This section explains the reasons why this has to be done.

Assigning the unified QAA levels to national eID schemes in general, and to national assurance levels particularly, is called mapping, which aims to:

- Use a unified approach and semantics to communicate among member states with respect to authentication processes
- Allow the direct comparison of the quality of authentication processes
- Increase trust
- Achieve interoperability
- Offer the same opportunities to equal QAA rated authentication processes
- Avoid subjective discrimination

However, the STORK document "D2.3 Quality authenticator scheme" states that for some countries there were technical difficulties assigning the appropriate QAA level. Moreover, some countries, such as Austria and Luxembourg, have only the highest authentication level available. By assigning this level to any offered electronic service, these countries would put pressure on other Member States to upgrade their schemes in order to access these services, even if the specific service would actually require only a lower level of security.

At the same time the mapping is as yet not formalised and binding. With the actual need to provide eServices to European citizens, new practices are being introduced which are based on bilateral and multilateral informal agreements. Some of these practices are described in chapter 3.8 (on page 20f.), as well as various initial experiences that were gathered in the application of QAA levels to security services.

3.6.1 Trust

Citizens and service providers must be able to place their trust in a secure and reliable exchange of information.

> *Without confidence in the trustworthiness of services or the genuineness of users any e-ID platform scheme is bound to fail.*

In fact service providers will not feel that they can offer their services via this platform and users will refrain from the use of any offered services that are perceived to be untrustworthy.

Standardised quality measures and correct mapping of the different QAA levels will improve the confidence of the service providers and the citizens.

3.6.2 Liability

Liability is a legal matter, which can be addressed by applying the current national or EU legislation, or by making new agreements on a European level, if necessary. There are several issues to deal with. For instance:

- Who is liable for issuing and/or revoking someone's electronic identity? The Registration Authority or the provider of the token and/or the certificate?
- Who is liable in case of an error situation?
- Who can guarantee that the mapped QAA level is correct?
- How will the maintenance of the mapping be dealt with, particularly in the event of a risk re-assessment and related upgrade of the security measures? This is particularly important when we look at technological advances in security attacks, which may invalidate an existing security mechanism.

National legal rules can vary from country to country with different accents on security, data protection and privacy.

Looking at the European legal framework, the applicable regulations have been already mentioned:

I. Directive on the protection of personal data 95/46/EC **[9]**
II. Directive 1999/93/EC on a Community framework for electronic signatures **[10]**
III. Directive 2006/123/EC on services in the internal market **[11]**
IV. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communication sector **[12]**

Some of these legal acts (e.g. Directive on the protection of personal data) are currently under review or are part of the telecoms package. The new telecoms rules will now need to be transposed into national laws of the 27 Member States by May 2011.

The Directive on the protection of personal data states principles for data quality, e.g. article 6d: "Member States shall provide that personal data must be: accurate and, where necessary, kept up to date."

The Directive on electronic signatures includes provisions on liability (art. 6) and on international aspects (art. 7), which could apply to cross-border authentication processes. However, STORK report D2.2 [5] brings to light the crucial question of whether the certificate is qualified or not. Differences in liability have been identified and would need some additional legal investigation. It must be considered also that the Directive on digital signatures explicitly targets electronic digital signatures and not the use of comparable mechanisms for authenticating users. This Directive is currently under revision.

The Directive on Services [11] mentions that 'Issues such as liability for providing incorrect or misleading information should be determined by Member States'. This Directive introduces the concept of a single point of contact, which allows the exchange of information between providers and recipients. Also found here (art 7.3) is one of the required information quality attributes, that information must be up to date.

> *It seems that the current legal framework may not be sufficient to deal with the new challenges and with issues related to cross-border authentication.*

This becomes particularly apparent when Member States' national legal rules have different approaches regarding security, data protection and privacy.

3.7 Exemplary business cases for mapping security services to authentication levels

The STORK project mentions some possible business cases for cross-border authentication on its platform: starting a company, getting your tax refund, or obtaining your university papers without physical presence. The access to these services would be granted through your personal data, using the national eID, which intuitively would be considered to be a high-level authentication method (QAA 4). However, other levels of authentication are technically possible. Are the business cases applicable to these levels as well?

This section will show the practical application of the concepts of security level and the importance of the mapping. A couple of cross-border business cases will make clear the different needs of security. Each case is compiled according to the following structure:

- Description of the situation
- Risk assessment
- Mapping to QAA level

3.7.1 Case 1: Border-crossing public transportation (QAA Level 1)

Imagine living in a town close to the national border. You might be employed by a company and/or for leisure purposes (seeing friends, shopping, cultural events) travel to the other side of the border. You are an environmentally friendly citizen who makes use of public transportation and the public transportation company across the border offers digital services to its users. People can access customised timetables, get updated information about changes (perhaps even utilising mobile phone connectivity) and subscribe to a newsletter.

Risk assessment: there is little motivation to access this kind of information using a fake eID, therefore the risk is unlikely to happen. The impact of the risk is negligible, as it is in any case public information. Even the possibility of accessing another citizen's preferred timetables and similar information would not usually cause any damage to this citizen[10].

Mapping: This brings this scenario to QAA level 1.

[10] Citizens with a perceived high risk of suffering personal attack or kidnapping might be damaged by behaviour based attacks. They are not considered in this example, since such a citizen will subject his public life to a security based evaluation and therefore be unlikely to use this service.

Caveat: While this theoretical scenario works, in reality the citizen will simply register directly with the transportation company by providing the necessary (unchecked) data and – perhaps – an email address or phone number.

Therefore there is little practical need to have a trans-national platform to authenticate users of this kind of service. Nevertheless, it may be considered to be more comfortable for the user to access this information via a single point of contact, together with other electronic services.

3.7.2 Case 2: Utility services (e.g. electricity, water) (QAA Level 2 or 3)

More and more European citizens have permanent holiday accommodation: an apartment, a house or any other estate in a nice environment, most likely in another EU Member State. Companies have offices in other Member States, which may be used only when needed and are therefore not permanently staffed.

A constant worry has been to make sure that basic supplies of electricity and water are guaranteed throughout the year. Physical bills need to be paid on time or, a late payment fee is charged. Fortunately, this now belongs in the past. The local supplier has decided to take a step towards user-friendliness and switch its administrative handling from paper to electronic statements and bills. The consumer reads the meter (physically before leaving or even remotely if the technology allows it) and sends the information electronically to the supplier, which produces e-statements and e-bills. The consumer then receives an electronic notification.

Risk assessment: an impostor could change the tariff to one less favourable or even unsubscribe the provision of services. Secure identification of the owner is therefore appropriate to this example. The risk is moderate and the impact is low to medium.

Mapping: QAA level 2 or 3.

This level of authentication has practical use, improving the services to the citizens in a real cross-border environment. However, how many EU Member States can provide fitting QAA level 2/3 authentication credentials? While any higher QAA level authentication would be acceptable as well, by default, QAA level 4 credentials might be considered security overkill with respect to the effort and cost involved. Just think about initial and recurring costs for the issuance and revocation of certificates for qualified signatures and the infrastructure required to utilise them. Citizens would have to contribute to those costs annually (prices vary depending on CA).

3.7.3 Case 3: Marriage between citizens of two different nationalities (QAA Level 4)

This is a real life case about two people in love who intend to stay together for a long time. They want to marry. One of them is living in his home country, the other is living in the same country, but is a national of another European Member State. The couple need to present themselves in person to the civil registrar of the second state in order to to obtain the necessary marriage documents.

Risk assessment: As marriage would influence the civil status information component of their personal data – and potentially open opportunities for abuse of social benefits - the couple need to be identified in a secure way. The risk is likely to happen and the impact is high.

Mapping: QAA level 4.

Here an electronic cross-border transaction must be considered to be extremely useful to these European citizens, since it would save them the time, trouble and the cost of a trip to the other Member State.

3.8 Current practice

Since mapping rules are not yet formally established, but the need to provide eServices to European citizens is a reality, new practices are being introduced. Through bi- and multilateral cooperation, the cross-border application of electronic identification is possible.

The Company Registration Portal (CReP)[11] of the Estonian Ministry of Justice grants access to Estonian citizens by ID-card, Mobil-ID or via bank-link. Portuguese, Finnish and Belgian citizens can access the CReP by their respective national ID-card and Lithuanian citizens can use their national Mobile-ID.

In May 2009, an Estonian company was created online for the very first time using a Finnish ID card. The Estonian Centre of Registers and Information Systems stated "The newly-created company has two Estonian and three Finnish founders who all used the ID-card of their respective country in creating the company that is located in Tallinn and deals with the wholesaling of electronic and telecommunications appliances and their parts."**[35]**

On the Iberian Peninsula, there is mutual eID recognition between Portugal and Spain. A holder of a Spanish DNI (Documento Nacional de Identidad)[12] can open a business in Portugal online, for example.

Finland, one of the first EU countries to introduce the electronic identity card, took several initiatives in the area of eGovernment. In 2005, mobile digital signatures for eGovernment services were introduced, using mobile phone SIM cards as the carrier of the signature.

Various services are now provided to Finnish citizens possessing a digital certificate and, in addition, Finland is to apply SPOC technology to support EAC-enabled e-Passports. In fact, international EAC certificate requests will be handled directly between SPOC's. By the end of 2010, the Finnish Population Register Centre SPOC is scheduled to be up and running.

A method for assessing certificates based on private key carriers, security levels of cryptographic algorithms, the quality of the certification service and an independent quality assurance standard has been set up by Estonia.

In relation to the application of QAA levels models, it seems that issues are raised about the application of QAA level 4 on services, which may not actually require such a high level of trust. The pilot "Safer Chat", which promotes safe internet communication for children and young people by requiring an authentication to join a chat, is designed with QAA level 4. This automatically excludes quite a number of Member States from participating because they don't have QAA level 4 (cf. situation of QAA levels in the EU on p. 31-32). At the same time, QAA level 3 or even QAA level 2 may be considered to be safe enough for such a service, since they require the citizen's data to be cross-checked against a trustworthy database and provide the credentials in a way that is fairly secure against eavesdropping or stealing.

Moreover, the first issues relating to QAA level 4 overkill now appear to be emerging. This happens because the participants in STORK pilots have national ID cards with electronic authentication, the highest level possible. Member States that wish to join those pilots and provide only lower levels of authentication, are now urging a revision of the need for an authentication level 4. At the same time, Member States are aware that other levels are needed to meet the requirements for authentication relating to such activities as business services.

As the number of countries with a national ID card with electronic authentication capabilities is increasing (see Figure 1 and Table 3), it would be appropriate to define common rules, which would extend the application field and geographic area of the cross-border electronic identification to all of Europe.

[11] https://ettevotjaportaal.rik.ee/index.py?chlang=eng
[12] National Identity Card

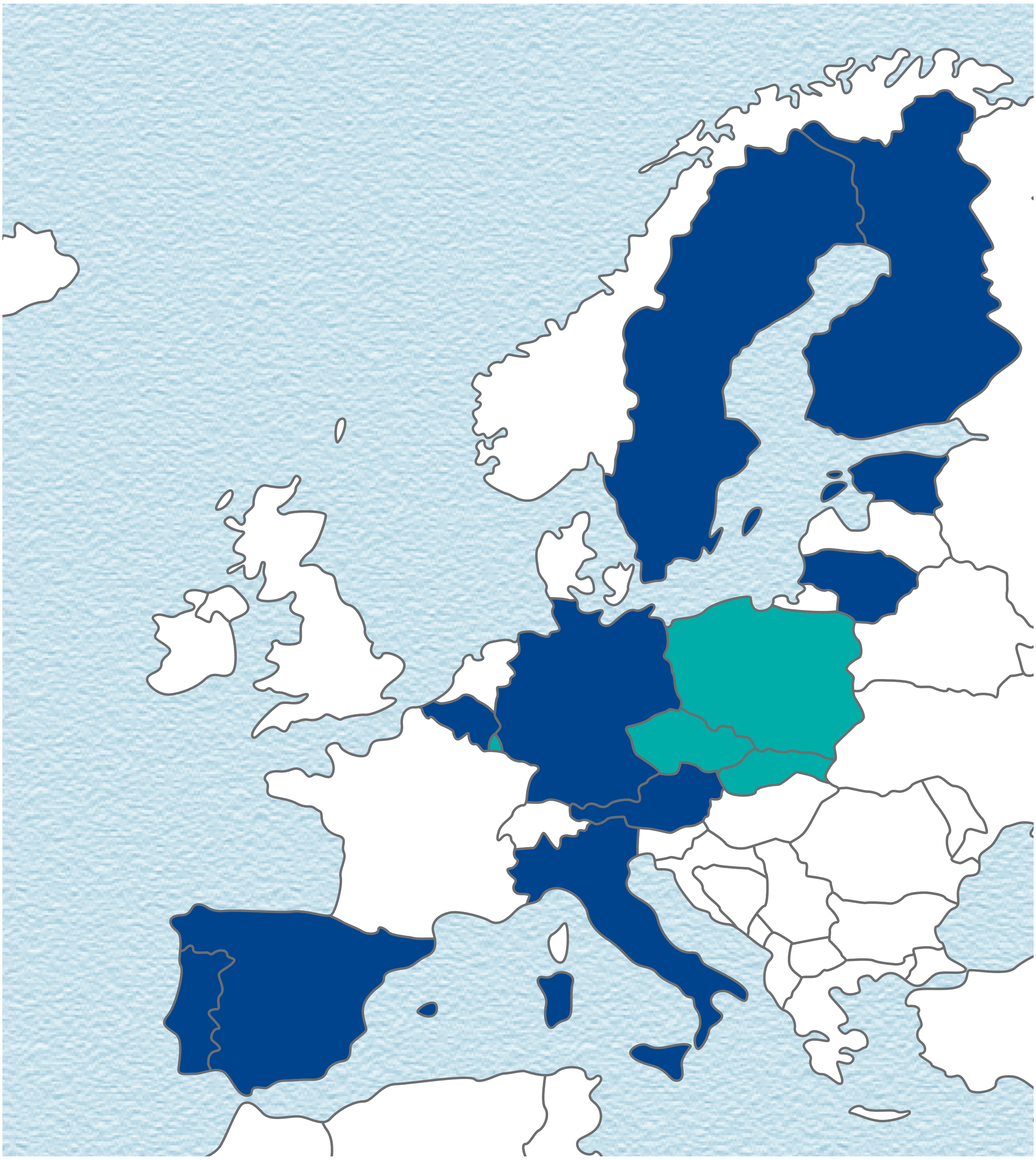

Figure 1: Overview of eID implementation

Member state	Deployed since	Introduction in	Remarks
Austria	2004		Only for electronic authentication.
Belgium	2003		
Czech Republic		2012	
Estonia	2002		
Finland	2004		
Germany	2010		
Italy	2004		Partial deployment
Lithuania	2009		
Luxembourg		2011	
Poland		2011	
Portugal	2007		
Slovakia		2012	
Spain	2006		
Sweden	2005		

Table 4: National ID cards with electronic authentication capabilities in the EU

4 – Mapping security services to authentication levels

With the aforesaid in mind, we will now take a closer look at the actual process of mapping security services to authentication levels. Through such a mapping the different solutions throughout the Member States will become comparable to the point where a national authentication solution can be trusted in a cross-border scenario.

4.1 For a given measure of trust

Any authentication aims at establishing trust between a claimant, stating his identity, and what STORK calls a "relying party", i.e. someone who needs to trust in the claimed identity. Unfortunately, trust is not an absolute value and it is actually fairly difficult to measure. So how much trust does a relying party need?

If we look at authentications in our daily life, there is actually a quite simple approach. A stranger ringing at our door will only be trusted after providing some information that supposedly makes him trustworthy. We will not allow him to enter our residence, unless he presents a good reason and possibly some third party authentication. Someone who is tasked with registering our usage of electricity and needs access to the electricity meter may present a plastic card from the electricity provider, incorporating his photo. If we let him in, this is due to the amount of trust that we place in the presentation of these credentials. A more careful person may call the electricity provider to check whether this stranger is a genuine employee. Nonetheless, we will not usually require any official ID document in order to check his identity. In the end, this is low-level trust, since we would not even allow this person to move unsupervised within our residence.

Taking another example, if we go shopping, we will usually be anonymous to the store staff. As long as we pay cash and take the purchases away, this will remain so. If we pay electronically, we identify ourselves as customers of a specific bank (via name and account number). In order to prove this to the member of store staff, we present our bank card, which, will be sufficient for most purchases. But the staff member may request some additional ID if the price of the purchase exceeds a given amount. So we show our national ID card, our passport or our driver's licence.

This is where the question of trust gets tricky. Each storeowner may decide individually the threshold at which this additional ID is required, by evaluating the perceived risks and efforts. Obviously, each additional identification process costs valuable staff selling time. Also the customer may not like this display of distrust and decide not to purchase. On the other hand, if the bank card is not valid or is stolen, the store will be the loser.

Some stores – especially big chains – will perform very careful calculations, taking into account not only absolute values, but also relative values such as the prevalence of crime in the vicinity of each individual store. Other stores may simply define a value based on the maximum amount of money they are willing to risk on the trustworthiness of their customers.

So each storeowner defines three levels of trust he requires. On the lowest, the customer may stay anonymous as long as he pays cash. On an intermediate level, some authentication (by possession of a bank card) will be required to allow the use of the electronic payment service. And for electronic payment exceeding a given amount of money, additional ID documents will be required. A well-known customer may be spared this (an alternative authentication mechanism based on the store staff "knowing" the customer).

Interestingly enough, the presentation of an official ID document increases the trust placed in an authentication process significantly, although experience shows that credit cards displaying the customer's photograph are often accepted without additional ID. So at least for a face-to-face transaction, most trust will be placed in linking any official looking document to the claimant via the photograph. The trustworthiness of the document itself seems to be less important on this real-life level.

So we are quite used to applying different levels of trust in everyday situations without even thinking about it too much.

When applying this approach to electronic authentication we quickly face a number of difficulties:

- We now need formally defined levels of trustworthiness, since the authentication is not performed by ourselves, but by IT systems
- To make things worse, the claimant does not show up in person at all, so we can only rely on the electronic information provided. Finding the claimant in the case of any inconsistency may prove to be a major challenge
- Electronic attacks can be automated. This means that even small damages may very quickly add up to substantial amounts, without requiring an attacker to invest similarly high levels of effort.

As a provider of electronic services, we have to rely on the implemented authentication mechanisms – and only on those – in order to place our trust in the identity of the claimant. If we do not control this authentication mechanism directly, it is of utmost importance that it is reliable and at least sufficient to meet our requirements with respect to trustworthiness.

4.2 A closer look at QAA levels

This section examines how the QAA levels are defined and how these definitions are suited to the task.

STORK defines four QAA levels ranging from 1 to 4, with QAA level 1 being the minimal assurance level and QAA level 4 being the highest. The QAA level of an authentication solution is based on five factors, which focus on the quality of the registration phase (establishing the electronic identity in the first place) and on the quality of the electronic authentication (validating this electronic identity in the actual use). These factors are described in Table 2 on page 17.

For each of these factors, technical requirements are stated (as so called quality levels), which must be met in order to qualify for a specific QAA level.

> *The QAA level of an authentication solution is established as the lowest quality level that is reached by any single factor.*

This minimum principle is widely considered best practice when it comes to assessing security measures.

To the provider of the authentication process, this implies that all factors must be given equal attention so as to assure an even QAA level. For example, it is of little use (with respect to IT security in a border-crossing or application independent scenario) to provide smart-card based certificates (quality level 3 for “type and robustness of the credential”) if these are issued by an organisation with no government supervision or accreditation (quality level 1 for “entity issuing credentials”), since for any such solution the QAA level could not exceed 1 anyway.

4.3 QAA levels and the service provider

QAA levels are intended as an “exchange rate” between different national assurance levels, in some ways similar to the ECU before the advent of the EURO. A service provider should be able to easily match the authentication needs of his system to a QAA level that would be expected from any citizen in any Member State as a minimum authentication level.

From a service provider’s point of view, the technical security measures are not really the prime concern. Potential damages and their probabilities are much more important for a number of reasons:

1. The service provider is well aware of the value of the service he offers and of the (often quantifiable) value of the information he processes, stores and provides for the user.
2. The security goals and overall requirements will be well known to the service provider as part of his business continuity management.
3. Technical security measures, on the other hand, are usually beyond the service provider’s business scope, so the task of evaluating them is difficult or even virtually impossible.

4. The service provider can only measure the effectiveness of security measures through the perceived damages that he or the users of his service suffer. It is quite easy for a service provider to define what amount and kind of damages can be deemed acceptable and what damages are unacceptable to the service and its users.

Potential damages are stated as impacts in the QAA level definition without further explanation:

QAA Level	Impact of erroneous authentication
1	Very low or negligible
2	Low impact
3	Substantial impact
4	Heavy impact

Table 5: Damage impact mapping to QAA levels

These values are open to interpretation by any reader. Without any clear qualification of the potential damages or the involved risks, selecting an appropriate QAA level may be based on two simple (and usually wrong) approaches:

- The highest QAA level is selected by default. This is costly and limits the use of the service to those citizens who have access to that QAA level and who are willing to go to the trouble of using it.
- The QAA level is selected by comparing the mechanisms to those which are used locally. While this might work in a lot of cases, there are still cross-border concerns that may require higher levels of security.

***Recommendation:** The definition of QAA levels should be extended to include not only the required technical or organisational security measures, but also the risks and potential damages that are addressed at this level of authentication quality.*

***Recommendation:** A short and easy-to-use guideline for service providers should be developed on how to evaluate the required QAA levels for a service by an appropriate European Community agency. Such a guideline should be orientated to the potential damages and their likelihood and not to the technical security measures required to counter the corresponding risks.*

While the development of such a service provider-centric redefinition or assessment of QAA levels is beyond the scope and mandate of this report, some general ideas will be provided on how such a guideline could be created.

A service provider-centric assessment guide should consider the QAA levels from the service provider's point of view. To him, it is much more important to know what is achieved by utilising a specific QAA level than to know how this is achieved.

The application of a national authentication level is usually quite easy for a service provider. Often enough, this will be regulated by a national eGovernment policy and a service provider will not always be required to perform an in-depth security analysis.

For the cross-border scenario, the service provider must be able to assess his security requirements for the authentication process, including the quality of the identity that is authenticated and consequently map it to the appropriate QAA level.

So the first section of the assessment guide might provide some guidance on how to assess these security requirements. This could be done in the form of a questionnaire, where the answers should be provided in a way that is quantified and decisive.

Questions in such a questionnaire should focus on issues, which can be answered from within the knowledge domain of the service provided. The questions should be formulated in such a way that the service provider is able to provide quantified answers, e.g.:

- What consequences with respect to data privacy can be expected if a user's identity is stolen and used to access the service?
- What financial damage can result to the service provider if services are requested and provided based on a false identity?
- What damages can affect the user if the service is requested and provided based on his illegitimately used identity?
- What legal obligations does the authentication mechanism of the service have to fulfil when the service is used across borders?

The quantified results will then be categorised in such a way that each category can be mapped to one specific QAA level. By applying the maximum principle and summing up the results of the questionnaire, it should be possible to provide very quickly a reliable assessment of what minimum QAA level is required by a specific service. This approach would also normalise required QAA levels for services throughout the different Member States, since a service provider would not default to the QAA level provided by his local eID solution.

Utilising existing and accepted standards for IT security management systems (e.g. ISO 27001 or BSI 100) in the definition and evaluation of such a questionnaire will greatly facilitate this process and help to alleviate problems of ambiguity or interpretation. Eventually it may even be considered appropriate to supply assessment guides, which would be adapted to different security management standards prevalent in the European Member States. This would greatly facilitate the reuse of existing IT security assessments as a basis for the QAA level assessment.

A second non-technical section of this assessment guide could concern legal issues, such as questions of liability. Even if these are not (yet) regulated and formalised within the scope of the STORK project, these issues are of very high concern to any service provider and to any user of an electronic service.

4.4 Separation of QAA levels

QAA levels are separated by the definition of required security measures. The impact of these security measures and their applicability to the requirements of any specific service remains vague. So why are there four separate levels at all?

The selection of four levels is based on the suggestion of IDABC, who propose four Authentication Assurance Levels. It is widely agreed that more QAA levels would tend to obscure the issue and potentially alienate users.

Let us take a look at the QAA levels that are most clearly defined.

Level 1 (the minimal level) simply requires the citizen to supply some information which is not checked (with the exception of a possible email address). Based on this – actually pseudonymous – information, the citizen is provided with a password or PIN, without the requirement for any special security (like sending the password by physical mail in order to establish at least the address of the claimant).

In principle, this QAA level is useful for services that only need to recognise a returning user and that might send out non-sensitive information to that user.

Level 4 (the maximal level) is quite the opposite. Based on the directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, the authentication mechanisms are focused on qualified certificates and qualified signatures. The signatures are regarded as legally equivalent to hand-written signatures.

Principally, a service provider might require QAA level 4 if the corresponding manual process would require a legally binding hand-written signature or if the manual process would necessarily involve the citizen's presence and his identification based on an official ID document. This is usually the case if the damage potential is considered very high or even disastrous to citizen or service provider[13].

Even with the adoption of a minimal and a maximal level as relatively fixed designs, there remains the problem of the in-between levels. While there is obviously quite some room between the pseudonym and the identity which is established beyond dispute and any doubt, the differentiation between further levels is at best vague.

> ***Recommendation:*** *The distinction between QAA levels 2 and 3 should be carefully evaluated. If no strict distinction (apart from technical measures) can be found, QAA levels 2 and 3 should be united as one medium level. If a distinction can be found, there is a need to develop a short and easy-to-use guideline to how to evaluate the required QAA levels for an application. Such a guideline should be orientated to the potential damages and not to the technical security measures required to counter the corresponding risks.*

4.5 The definition of mappings

The QAA level of an authentication solution is based on five factors, which focus on the quality of the registration phase and on the quality of the electronic authentication. The QAA levels are defined based on the technical quality of five different factors:

- The identification procedure
- The credential issuing process
- The entity issuing the credential
- The type and the robustness of the credential
- The security of the authentication mechanism

Each factor is then provided with a set of minimal requirements for each assurance level.

4.5.1 Quality of the identification procedure

This factor is established via three independent aspects:

- The physical presence of the claimant at some time in the identification process
- The quality of assertions about the claimant's identity
- The quality of validation of these assertions

4.5.2 Quality of the credential issuing process

This factor measures the quality of verification of the recipient's identity during delivery of the identity token or credential.

The different quality levels are described with somewhat unclear expressions and examples. Without a clear definition of terms like "light-weight verification" the assessment of a verification process which is not stated in the examples will be arbitrary and depend on the assessing body's interpretation.

[13] Please be aware that the damage potential is not limited to a single incident. A damage scenario that appears very likely in huge numbers may be considered to be of disastrous damage potential even though each single incident would be considered minor. On the other hand even a single incident may be considered to be unbearable, e. g. if this incident would cause the death of a citizen.

In addition, the examples provided to illustrate the quality level definitions are not decisive enough to make up for the fuzzy descriptions.

For example, the verification of the recipient by means of a qualified signature, according to the terms of directive 1999/93/EC (which is equivalent to a legally binding signature), should comply with the highest level of quality, instead of just level 3. If the given example involves a soft credential, which lowers the total QAA level to a maximum of 3, this should not affect the quality level of this factor. Let us look at a (as of today hypothetical) automated delivery kiosk that delivers a qualified signature hardware token if the applicant identifies himself by providing his old qualified signature token and by electronically signing a receipt form with a qualified signature. Going just by the examples, such a highly secure system would have to be considered to be quality assurance level 3 only.

4.5.3 Quality of the entity issuing the identity credentials

This factor measures the extent of government involvement in the credential issuing entity. It may range from "none", through "with government agreement" and "with government accreditation or supervision" to "qualified" according to annex II of the Directive 1999/93/EC".

The medium quality levels are rather awkward to handle, since "government agreement" and "government supervision" lack clear meaning and are ambiguous[14]. These terms must be clarified to the point that a quality level can be determined beyond any reasonable doubt.

In addition, there is the question of identifying the credential issuing entity. A lot of credentials are produced and issued by a multitude of participants. A national ID card may be produced and personalised by two separate private companies, the electronic certificates to be stored on it usually come from a CA (yet another company) and the responsible entity for the issuance of the ID card may be the national Ministry of Interior. In such a scenario it is not quite clear who must be considered to be the credential issuing entity.

Finally, the importance of retaining registration information for a specific period of time is stressed. Yet neither the existence of such a retention system nor the retention period is currently formally evaluated within the quality levels for this factor.

4.5.4 Type and robustness of the credential

STORK focuses its work on a number of selected token types, ranging from "username/password" to "qualified hard certificates". Each of these types is assigned to one of four quality levels.

Since the type of the token limits the maximal security that can be possibly reached by it, this is a good first approach. Nevertheless, there is some room for argument in accepting each type of token automatically at its highest possible level, without regard for any security mechanisms or their strength. In addition, the types of tokens are not clearly defined (e.g. a soft certificate is a key which is stored on a medium, a hard certificate is a medium which stores a protected key).

Soft certificates, qualified soft certificates and (unqualified) hard certificates are considered to be of the same quality level 3. But a soft certificate may be extremely vulnerable if it is stored in a low-security area (e. g. on a web server without strong security mechanisms) and if its password is of low quality. No qualification of the mechanism or strength of the cryptography is required, which means that the (unqualified) soft or hard certificate does not have to withstand even a simple brute-force attack[15]. In the end this means that the QAA level 3 is available with credentials which are actually ineffective.

[14] E. g. the German Bundesnetzagentur supervises every telecommunication provider in Germany, although this should not automatically qualify every SIM-card in a German cell phone as quality level 3 with respect to the credential issuing identity.
[15] A brute-force attack is a computerised attack which attempts to gain access to a secret by trying a multitude of possible combinations.

***Recommendation:** the robustness (meaning the security requirements of the token itself including cryptographic strength, password quality and storage security) should be explicitly covered in the quality level definitions.*

Finally, STORK raises the aspect of credential freshness. This refers to the question, how up-to-date any credential information is and is paired with the need to identify credentials that may seem valid but have lost their credibility (e.g. because the credential owner has died). The increase in quality of an authentication with up-to-date credentials is acknowledged, but not (yet) reflected in the definition of quality levels.

4.5.5 Security of the authentication mechanism

STORK lists a number of perceived attacks against the authentication mechanism. The quality levels are defined as authentication mechanisms offering protection against these attacks:

1	Offering little or no protection
2	Offering some protection
3	Offering protection against most attacks
4	Offering protection against all attacks and comparable to CC EAL4+ or higher

Table 6: STORK levels of protection

These definitions seem to be quite obvious at first sight. A second glance shows them to be much too vague to be of any use as a normative scale. Even levels 1 and 2 are difficult to distinguish, since the distinction between "little" protection and "some" protection is completely arbitrary and depends on the subjective scale of the assessor.

In addition, the definition of the third quality level opens a huge security gap, since the lack of any adequate protection against even one perceived attack may cause severe damages and decrease the system's credibility to the point of uselessness.

Recommendation: the quality levels for the factor "Security of the authentication mechanism" should be redefined to state clearly and unambiguously the intention of the authors.

4.5.6 Summary of the analysis of the STORK quality levels

STORK defines QAA levels based on the strengths or weaknesses of the authentication process, including the registration process which establishes the identity in the first place. This is a valid and commendable approach to establish different levels of authentication processes. While the intention of the approach and the associated quality levels are fundamentally sound, the actual definition of these quality levels is not sufficient to act as normative declaration or assessment. If the assessment of authentication processes is based only on the definition of quality levels as described in D2.3 "Quality authenticator scheme", the results are in many cases not clear enough to warrant trust in these authentication processes by a service provider.

The clarification of terms and the strict separation of quality levels are of utmost importance in order to establish the STORK QAA levels as common denominators in interchanging authentication levels across national levels of different Member States. Without clearly and unambiguously defined QAA levels that are cleanly separated from each other, little trust can be placed in the QAA levels which are assigned to other Member States' authentication processes, so that service providers will tend simply to require the highest QAA level, since that is the only level which is based on a clear and accepted standard.

***Recommendation:** The quality levels should be exactly and more elaborately defined. Ambiguous terms must be clarified or adapted in order to provide the QAA levels as a normative and clear-cut baseline, which allows assessment of quality of national authentication levels across borders. It should be possible to easily measure or assess the attributes of defined quality levels.*

4.5.7 Validity duration of quality levels

Security is not an absolute value. It changes over time as attacks on security improve with scientific and technological progress. Therefore, a security mechanism that was considered highly secure at one time may be considered almost useless some years later. Banknotes that were virtually impossible to forge 50 years ago would present little challenge to today's forger.

With respect to IT security, the evolution of threats and countermeasures is much faster. Just think of antivirus software, which is updated on a daily basis to counter new threats. Attacks on cryptographic security measures are improving with new analytical methods and ever more powerful computers. Ciphers, which were considered safe ten years ago because cracking them would require years of computing time, are deciphered today within minutes.

Easier and cheaper access to ever more powerful technology tilts the balance continuously in favour of the attackers. While the cost for 1 million computing instructions per second (MIPS) was around US$190 million in the year 1960, the same amount of computing power was available in 1980 for about US$100,000 and in the year 2000 the cost was down to less than US$10[16].

With the increase in cheap computing power, passwords are subjected to attacks that continually require them to be made longer and longer.

For just the same reason, cryptographic key lengths are increased on a regular basis. While in 1998 a qualified signature[17] could be produced with a key length of 768 bits, this value was only accepted until 2001. In 2010 the required minimal key length is 1728 bits. With respect to STORK quality levels this implies that a token supporting QAA level 4 in 1998 would have no longer qualified for this QAA level in 2002.

As a result of this race between attackers and defenders, any IT security measures must be evaluated every few years to assure that the required security level is still reached. This also means that the quality levels defining the STORK QAA levels need to be adapted again and again. The advent of new attacks may require the introduction of completely new security measures, while technological progress will require existing mechanisms to be strengthened in order to withstand more powerful attacks.

Experience shows that a forecast on the security and continued effectiveness of a cryptographic mechanism and key length cannot be reliable for more than a few years. In a pan-European setting this requires a conservative approach that allows a (comparatively) fast reaction to new research results and increased computing power. Following the German approach16 on acceptable qualified digital signature technologies, such an evaluation might be performed every three years.

***Recommendation:** The security measures required to reach a specific quality level should be re-evaluated at least every three years by the authority responsible for the QAA framework. The level of security measures should be designed to be sufficient for at least twice that time span[18].*

[16] The calculation is normalised for the value of US$ in the year 1998, based on data from H. Moravic, 1998 [36].

[17] Based on the German regulations for the qualified signature using the RSA algorithm (Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen; Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen); 06. Januar 2010 and the appropriate document from 1998).

[18] This means that a QAA quality level defined in 2010 should be considered sufficiently secure to be still used in 2016 (anticipating the development in computing power and analytical procedures). If in 2013 the required security measures are increased, these will need to suffice until 2019, but an identification service that was assessed in 2011 will still be valid until 2016.

Recommendation: The assignment of QAA levels to a specific security service should have a limited duration requiring re-assessments in regular intervals (e. g. every three years).

4.6 The application of mappings to national security services

4.6.1 Why is the correct mapping so important?

By mapping national security services to QAA levels, a quantified level of trustworthiness in a specific national authentication mechanism is declared. This level of trustworthiness is the only information available to a service provider in another country.

Local laws and regulations govern the service provider and information entrusted to him must be processed, stored and/or distributed according to these rulings and to the business rules governing the provided service. Among all these rules are some that define under which conditions a service may be used. The electronic authentication of the user must comply with these rules.

On the national level, the service provider usually evaluates the different available authentication solutions (there are only a very limited number in any country) and selects the one solution that satisfies the security requirements with the least possible cost and effort involved.

For the cross-border situation, the service provider has to decide whether to use a platform such as that proposed by STORK. If he does, he defines a QAA level that must be fulfilled in order to allow access to the provided services. From this point on he has no direct control over the quality of the authentication process used to access his provided service! He must trust that the authentication service in the other country actually satisfies all criteria for the declared QAA level.

Obviously this trust must be earned. A mapping of security services to QAA levels which even potentially seems to be opaque, arbitrary or unreliable, cannot be accepted by the service provider, who must then look for alternative cross-border options, which may be more limited but at least seem trustworthy to the service provider. If no other cross-border options seem viable and trustworthy, the service provider is required to reject any cross-border authentication to satisfy his legal constrictions, even though such a measure would not be aligned to the Signposts towards eGovernment 2010 **[12]**

4.6.2 Application of the quality authenticator scheme to the national authentication levels

Applying the QAA levels to the national authentication services poses a considerable practical challenge. Member States obviously do not wish their high level solutions to be "downgraded" in comparison, especially if the factors used for the mapping may contain a different evaluation from the national solution. Also a lot of solutions provide more than the minimal set required for one QAA level, without actually complying with the next level.

For such cases, it is important to understand that in mapping the national authentication level the minimum principle applies, while the maximum principle is used for selecting the QAA level required by an e-government service. Therefore the national authentication level may be mapped to one QAA level, and national services using this national level would demand the next higher QAA level in a pan-European context, in order to be satisfied with the authentication's security.

In D2.3 STORK proposes a mapping of national authentication levels to QAA levels. This is based on an inventory of all Member States' authentication solutions described in STORK deliverable D2.1.

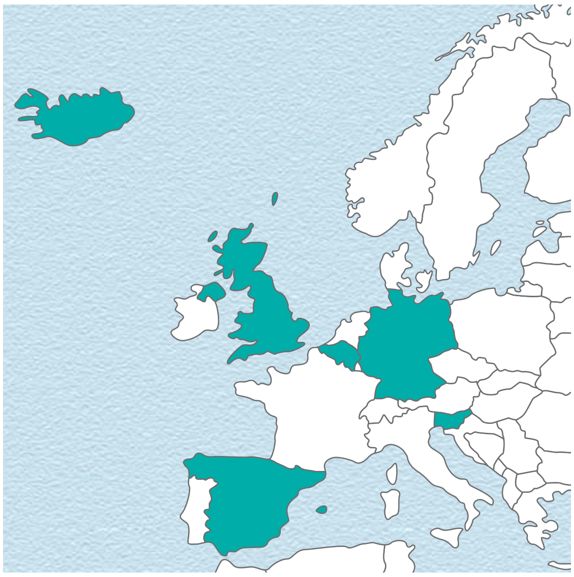

Figure 2: Countries with QAA level 1

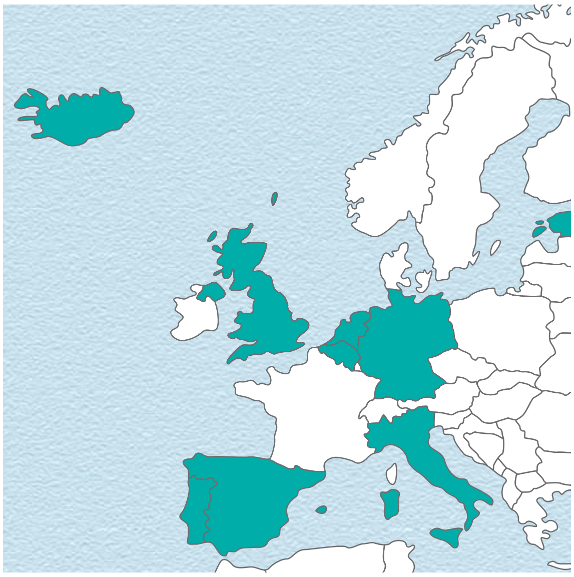

Figure 3: Countries with QAA level 2

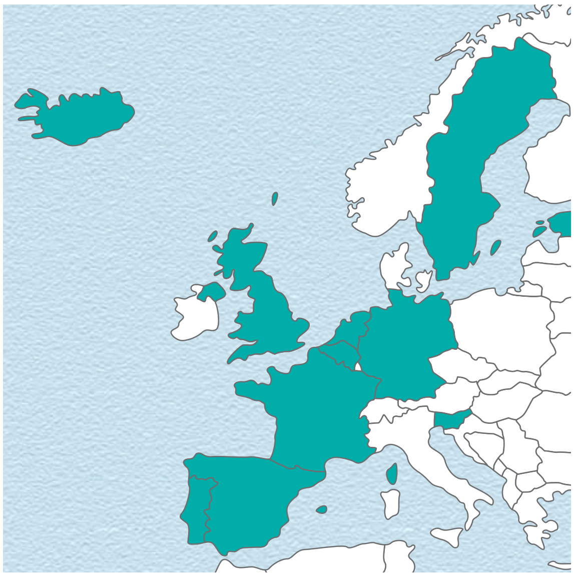

Figure 4: Countries with QAA level 3

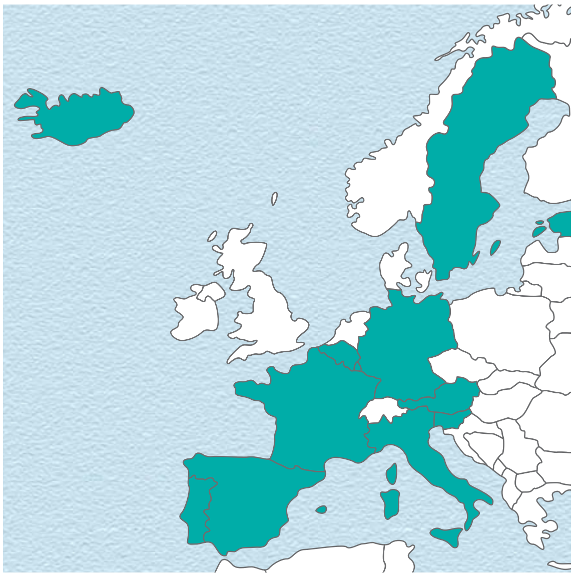

Figure 5: Countries with QAA level 4

In order to validate this mapping, additional information would be required that is not available to the authors of this report. From the information contained in D2.1, at least some doubt with respect to the correctness of the mapping should be voiced, although it must be stressed that this document seems to contain the summary of the survey results, so that additional undisclosed information may well counter this impression.

To provide just one example: for the French national level "strong" a QAA level 4 is proposed, although this uses hardware that is CC EAL3+ instead of CC EAL4+ as required for QAA level 4.

Recommendation: *Any documentation mapping the national authentication levels to the QAA levels should clearly state the mechanism used to fulfil each of the five factors.*

4.6.3 Compliance, supervision and re-evaluation

From the viewpoints of citizens and service providers, the core issues of cross-border authentication lie with the ease of use and with the trust in the remote system. Since the perception of security and data privacy and the corresponding laws and regulations vary slightly from Member State to Member State, citizens and service providers may be more reluctant to place any implicit trust in the "foreign" systems. Without discussing legal implications in depth, it is quite obvious that service providers are often restricted by local law with respect to processing and distributing sensitive information, especially if this information is person-related and considered to be within the realm of informational self-determination. Thus service providers may not only wish to be assured of the trustworthiness of an authentication process, but may be required by law to assess this trustworthiness.

Obviously, it is not feasible for a service provider to assess each national security service in the EU. The possible solution is to place trust in the QAA levels and their mappings to national security services. To do this, these mappings must be applied in a way that leaves no room for doubt as to whether a mapping is actually applied correctly.

This could be done, for instance, by controlling the mappings of QAA levels to national security levels by an independent IT security authority, which is accepted by all Member States.

STORK mentions the necessity to have such a supervising authority, which controls and acknowledges the correct application of the mappings of national security services to QAA levels. Obviously such a QAA authority should be equipped with the IT security knowledge necessary to assess a national security service.

For any real-world application beyond limited pilots, this authority should be neutral and sufficiently empowered to enforce any assessment of national security services. A formal assessment procedure, which would be based on the quality authenticator scheme, would help to assure citizens and service level providers of the trustworthiness of the cross-border authentication.

Regular audits by the QAA authority should be required for any national security service, in order to assure the continued compliance of the national security service. In addition, this is necessary to assess if any updates to security measures have been correctly implemented.

It may be a useful approach to issue compliance certificates to national security services with an appropriate logo to show the service's compliance to a specific QAA level.

Alternatively, national authorities may regulate assessment of national security services. This would require an EU directive similar to the eSignature-Directive, which regulates liability issues by placing liability with the certification service provider. An appropriate eID directive would need to clarify liability questions.
Recommendation: It should be decided on a political level whether the mapping of national security levels to QAA levels shall be performed by a European authority or whether this should be left to the individual Member States. Depending on this decision, liability issues and the (possibly mandatory) acceptance of QAA level mappings between Member States must be regulated.

> ***Recommendation:*** *It should be decided on a political level whether the mapping of national security levels to QAA levels shall be performed by a European authority or whether this should be left to the individual Member States. Depending on this decision, liability issues and the (possibly mandatory) acceptance of QAA level mappings between Member States must be regulated.*

5 – Recommendations

In this section the recommendations given throughout the report are summarised for easier reference and overview.

- It seems that the current legal framework may not be sufficient to deal with the new challenges and with issues related to cross-border authentication (section 3.6.2, p. 18)

- The definition of QAA levels should be extended to include not only the required technical or organisational security measures, but also the risks and potential damages that are addressed at this level of authentication quality (section 4.3, p. 25)

- A short and easy-to-use guideline for service providers should be developed on how to evaluate the required QAA levels for a service by an appropriate European Community agency. Such a guideline should be orientated to the potential damages and their likelihood and not to the technical security measures required to counter the corresponding risks (section 4.3, p. 25)

- The distinction between the QAA levels 2 and 3 should be carefully evaluated. If no strict distinction (apart from technical measures) can be found, the QAA levels 2 and 3 should be combined into one medium level. If a distinction can be found, there is a need to develop a short and easy-to-use guideline on how to evaluate the required QAA levels for an application. Such a guideline should be orientated to the potential damages and not to the technical security measures required to counter the corresponding risks (section 4.4, p. 27)

- The robustness (meaning the security requirements of the token itself, including cryptographic strength, password quality and storage security) should be explicitly covered in the quality level definitions (section 4.5.4, p. 29)

- The quality levels for the factor "Security of the Authentication Mechanism" should be redefined to clearly and unambiguously state the intention of the authors (section 4.5.5, p. 30)

- The quality levels should be exactly and more elaborately defined. Ambiguous terms must be clarified or adapted in order to provide the QAA levels as a normative and clear-cut baseline, which allows assessing the quality of national authentication levels across borders. It should be possible to easily measure or assess the attributes of defined quality levels (section 4.5.6, p. 30)

- The security measures required to reach a specific quality level should be re-evaluated at least every three years by the authority responsible for the QAA framework. The level of security measures should be designed to be sufficient for at least twice that time span[19] (section 4.5.7, p. 31)

- The assignment of QAA levels to a specific security service should have a limited duration, requiring re-assessments in regular intervals (e. g. every three years) (section 4.5.7, p. 31)

- Any documentation mapping the national authentication levels to the QAA levels should clearly state the mechanism utilised to fulfil each of the five factors (section 4.6.2, p. 32)

- It should be decided on a political level whether the mapping of national security levels to QAA levels shall be performed by a European authority or whether this should be left to the individual Member States. Depending on this decision, liability issues and the (possibly mandatory) acceptance of QAA level mappings between Member States must be regulated (section 4.6.3, p. 34)

[19] This means that a QAA quality level defined in 2010 should be considered sufficiently secure to be still used in 2016 (anticipating the development in computing power and analytical procedures). If in 2013 the required security measures are increased, these will need to suffice until 2019, but an identification service that was assessed in 2011 will still be valid until 2016.

6 – Conclusion

eGovernment services are becoming more and more prevalent within European Member States. Considering the concept of free movement of citizens within the European Union and the fact that almost 12 million European citizens are living permanently in other Member States, the necessity to establish an interoperability between the different national eID solutions has become obvious and, in the course of recent years, more prominent.

Apart from a multitude of application-specific solutions, which are based on bilateral or multilateral agreements, a number of pan-European solutions were planned and introduced in the form of pilots. Most notable among these are STORK, PEPPOL and SPOCS while IDABC defined a model for levels of authentication. These were mapped later to existing authentication solutions in the Member States. This report reviews these authentication levels and their mapping to security services.

In the course of this review some issues and discrepancies are identified and addressed by providing recommendations. Summarily the following core issues have been identified.

The legal frameworks, which govern the provision of electronic services across European borders, are not aligned to the point where service providers and citizens can easily assess the implications of a cross-border deployment, especially in respect of data privacy and issues of liability. A European community framework, which is comparable to the one established for electronic signatures by the EU directive 1999/93, is not (yet) in place.

The definition of methods of authentication as proposed by STORK (QAA levels) provides a good first approach to the assessment of authentication processes, with the goal of making them comparable. Nonetheless, these definitions should be clarified to remove any ambiguity and room for interpretation, as well as extended to include all significant factors identified by STORK. This would lead to a real interoperability of all European authentication methods.

Mapping authentication levels to security services proves to be a challenge for the service providers, since the QAA levels are categorised on the basis of the technical measures established with the authentication process. This may lead to a reluctance of service providers to actually utilise this pan-European approach. To alleviate this problem, a categorisation of QAA levels from a service provider-centric point of view should be included. This report suggests a possible approach.

In the face of ever increasing computing power and new technological innovations, no security measure can be considered to be valid indefinitely. As of today, mechanisms and an organisational framework are missing, which would define and govern the initial assessment and the periodic re-evaluation of national authentication solutions and their mapping to QAA levels. The formalisation of these aspects would increase the mutual levels of trust.

In conclusion, it can be said that the technological barriers to establish cross-border interoperability of eGovernment solutions and services are overcome in principle, even though some more work will be required in fine-tuning the comparison standard. On the other hand, the lack of a binding legal framework at the European level seriously hampers the fast and widespread prevalence of cross-border enabled eGovernment services, even though current cooperation between some Member States seems to provide sufficient grounds to begin providing basic electronic services across European borders. However, more legal and technical work needs to be done in order to offer every EU citizen an equal chance to access eGovernment services across Europe, guaranteeing privacy and an appropriate service level.

Annex

References

[1] Website: http://ec.europa.eu/idabc/

[2] Website: https://www.eid-stork.eu/

[3] ENISA, Report on the state of pan-European eIDM initiatives, 2009, www.enisa.europa.eu/act/it/eid/eidm-report

[4] ISO 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary

[5] ISO 27001 Information technology - Security techniques - Information security management systems - Requirements

[6] ISO 27002 Information technology - Security techniques - Code of practice for information security management

[7] ICT-PSP STORK, D2.2 – Report on Legal Interoperability, 2009, http://www.eid-stork.eu/index.php?option=com_processes&Itemid=60&act=streamDocument&did=578

[8] European Commission, Information Society and Media Directorate-General, eGovernment Unit, A Roadmap for a pan-European eIDM Framework by 2010, 2006 http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf

[9] European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[10] European Union, Directive 1999/93/EC on a Community framework for electronic signatures, 1999, http://europa.eu/legislation_summaries/information_society/l24118_en.htm

[11] European Union, Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, 2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0123:EN:HTML

[12] European Union, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communication sector, 2002, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

[13] European Commission eGovernment Unit, Signpost towards eGovernment 2010, 2005, http://ec.europa.eu/information_society/activities/egovernment/docs/minconf2005/signposts2005.pdf

[14] SPOCS Website: http://www.eu-spocs.eu/

[15] European commission, Digital Agenda: Commission outlines action plan to boost Europe's prosperity and well-being (Press release) IP/10/581, 2010, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/581

[16] SPOCS Website: http://www.eu-spocs.eu/index.php?option=com_content&view=article&id=1&Itemid=42

[17] Website: http://www.epractice.eu/en/library/281737

[18] Website: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4147

[19] ICT-PSP STORK, D6.0 Pilots Scope, 2009, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=575

[20] ICT-PSP STORK, D2.1 - Framework Mapping of Technical/Organisational Issues to a Quality Scheme, 2008, http://www.eid-stork.eu/index.php?option=com_processes&Itemid=60&act=streamDocument&did=579

[21] ICT-PSP STORK, D2.3 - Quality authenticator scheme, 2009, http://www.eid-stork.eu/index.php?option=com_processes&Itemid=60&act=streamDocument&did=577

[22] ENISA, Privacy Features of European eID Card Specifications, 2009, http://www.enisa.europa.eu/act/it/eid/eid-cards-en/at_download/fullReport

[23] Website: http://ec.europa.eu/information_society/activities/egovernment/policy/key_enablers/interoperability/index_en.htm

[24] Bundesamt für Sicherheit in der Informationstechnik, BSI Standard 100-1 Information Security Management Systems (ISMS)

[25] Bundesamt für Sicherheit in der Informationstechnik, BSI Standard 100-2 IT-Grundschutz Methodology

[26] Bundesamt für Sicherheit in der Informationstechnik, BSI Standard 100-3 Risk Analysis based on IT-Grundschutz

[27] NIST, 800-100 Information Security Handbook: A Guide for Managers, 2006,

[28] NIST, 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems, 1996,

[29] Information Security Forum, Standard of Good Practice for Information Security, https://www.isfsecuritystandard.com/SOGP07/index.htm

[30] ISO/IEC Guide 73:2009 Risk Management - Vocabulary

[31] NIST, Risk Management Guide for Information Technology Systems, NIST 800-30, 2002,

[32] IDABC, Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms, 2007, www.vaestorekisterikeskus.fi/.../Proposal_for_a_multi_level_authentication_mechanism_and_a_mapping_of_existing_authentication_mechanisms.pdf

[33] ENISA, Security Issues in Cross-border Electronic Authentication, 2010, http://www.enisa.europa.eu/act/it/eid/xborderauth/at_download/fullReport

[34] IDABC, Common specifications for eID interoperability in the eGovernment context, 2007, http://ec.europa.eu/idabc/en/document/6484/5938

[35] Website: http://www.rik.ee/39309

[36] ENISA, Flying 2.0 Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology, 2010

enisa
European Network
and Information
Security Agency

PO Box 1309   71001 Heraklion   Greece
Tel: +30 2810 391 280   Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu