Security Issues in Cross-border Electronic Authentication

enisa
European Network and Information Security Agency

www.enisa.europa.eu

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. 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 the European institutions, the Member States and private business and industry actors.

Contact details:

For contacting ENISA or for enquiries on this study, please use the following details:
Sławomir Górniak and Ingo Naumann
Email: eid@enisa.europa.eu
Internet: http://www.enisa.europa.eu

This study has been prepared for ENISA by Dirk Hartmann and Stephan Körting, HJP Consulting GmbH.

Table of contents

1 Management summary

During the last few years Member States of the European Union have been increasingly issuing electronically readable identity documents (eID documents) to their citizens for different purposes and applications. These solutions are designed to be the most efficient and fitting with respect to national requirements and available or planned infrastructures. The goals of these systems are in general (if not in detail) identical for all Member States: managing identities, improving administrative efficiency, improving accessibility and user-friendliness, reducing abuse and fraud and, above all, reducing of costs.

European citizens who move freely through Member States face the problem that their eID documents from their home state do not allow access to the electronic services of another Member State in which they are currently present. Administrations face the problem that they cannot provide services to European citizens from other Member States with the same ease and efficiency as their national citizens.

Improving the interoperability of electronic identification and authentication systems is a European task and a task for all Member States. Considerable efforts have been made in several projects to face the challenges of pan-European interoperability of electronic authentication and to assess the feasibility of differing approaches.

This report assesses the security risks of electronic authentication in cross-border solutions. To visualize these risks, two different projects offering cross-border authentication have been exemplarily examined and evaluated.

NETC@RDS for eEHIC ID is a pan-European project supported by the EU eTEN programme. It aims at facilitating the medical treatment of European citizens by using an electronically readable European health insurance card.

STORK (Secure idenTity acrOss boRders linKed) is a large-scale pilot project in the ICT Policy Support programme that aims at simplifying administrative formalities by providing secure online access to public services across EU borders.

For each project, a high level IT security analysis was carried out and summarized. In compiling the results, generic critical success factors in the security of electronic cross-border authentication solutions were identified:

- establishing the legal and contractual framework
- identifying the citizen through credentials
- authenticating system participants across borders
- making online connections secure
- bridging technological differences
- establishing and agreeing on a common security policy.

By covering these factors appropriately in the concepts and specifications of a system to support electronic cross-border authentication, the national goals of eID solutions can be extended successfully to a pan-European solution.

2 Introduction

Many kinds of services use electronic authentication. The public services of government and health care providers are increasingly offering citizens electronic access to these services. These e-services are usually implemented on a national level with specific technologies, specific security concepts and specific business logic. In addition, these e-services are governed by the laws of the individual Member States, which range from data protection laws to dedicated regulations for the selected application. In most cases, these systems can only be accessed from within the Member State and by citizens of that state.

To European citizens who move freely through all Member States, this may be an undue restriction on their use of these services. So there is a need to extend these services beyond national borders and beyond the user group of national citizens. At the same time, European and national data protection laws and regulations must be respected and may not be undermined by any cross-border distribution of personal data.

When extending a domestic system across borders, the most obvious technical challenge may be the fact that separate IT systems with different technologies must be interfaced. Any problems arising from this are, however, usually limited to designing a proper technical and financially affordable solution. Differences in the business logic of national solutions pose greater difficulties.

Health care and educational systems, especially, differ greatly in the way that their services are provided, evaluated and billed. Establishing a business or dealing with taxes also differs greatly from Member State to Member State. In addition, amendments to the legal framework are often required in order to allow the distribution and processing of data by non-national institutions and organizations. At the very least, a contractual agreement with respect to the duties and rights of all participants and the restrictions under which data is stored and processed must be reached. This can be greatly facilitated by European legislation that can lay the foundation for the implementation of national laws to support such cross-border applications.

A foundation of any e-government or e-health service is trust in the authenticity of all participants and the data provided. Since most of these services handle confidential data, the confidentiality must be protected also in a cross-border scenario. Last but not least, a few services require high availability if the citizen is not to suffer undue consequences.

This establishes the need to discuss, evaluate and implement IT security in any cross-border application. By focussing on the electronic authentication of a citizen in a cross-border e-application, this study assesses the security risks and approaches to counter them by examining a generic model and a number of existing implementations in different business sectors – so that the core areas of risk can then be summarized and discussed with general recommendations on appropriate remedies.

3 Domestic v cross-border authentication

In order to better understand the issues involved in extending a system to allow cross-border access, the fundamental differences are shown in a generic model[1].

3.1 A generic model of domestic electronic authentication

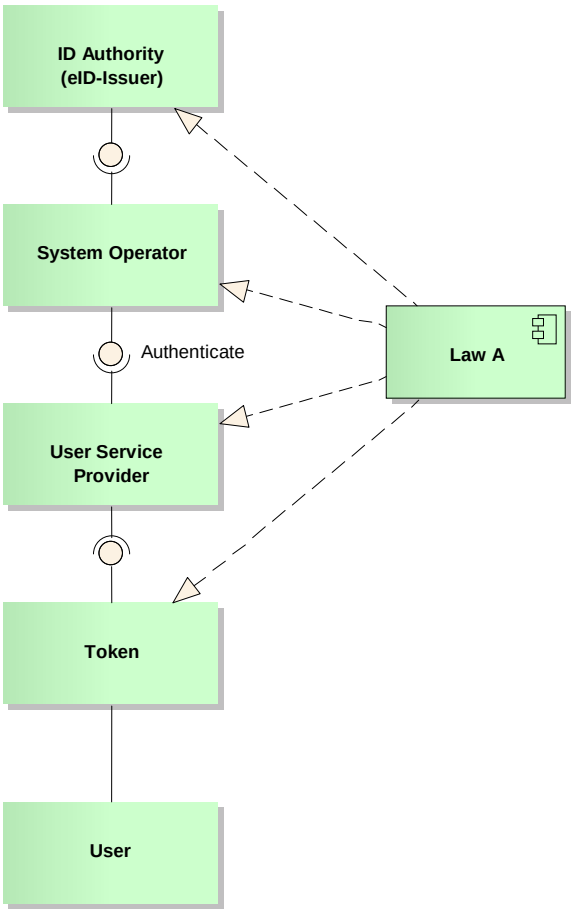


Figure 1: Domestic electronic authentication

In any system that involves electronic authentication, the **user** is assigned an electronic identity (eID). The scope of an eID may be limited to within the application (eg, a health insurance number or a civil register). This eID is assigned by some entity within the system, the **ID authority**.

The ID authority issues a **token.** A *token* is a device, eg, a smart card, which represents the user's identity. Examples are a health insurance card or a national ID card. The token may contain the person's indentity data and other data in electronically readable form.

A potentially separate participant[2] in the system is the **system operator** (eg, a health insurance company or a civil registration office). He operates the eID system and realizes any authentication processes with respect to the system's eID, usually in form of a centralized backend.

The **user service provider** (eg, a doctor or a vehicle registration office) interacts with the user and the user's token. He provides a service to the user that is linked to the application operated by the system operator.

---

[1] *The generic models presented were derived by the authors specifically for this report. They are based on several years of experience with different eID systems, their implementation and their interactions.*

[2] *For some systems the eID authority and the system operator may be the same entity.*

The laws, regulations or contracts governing the provision of this service require the user service provider to authenticate the user via the user's token against the system operator.

The entire system, its participants, components and processes are governed by the same set of laws and regulations (**Law A**). These laws range from general regulations on the handling of personal data (eg, based on the Data Protection Directive 95/46/EC [1]) to specific regulations regarding the application, the services or the token.

While the range of possible (and existing) technical solutions and variations in tokens and electronic authentications is vast, the general principle is the same for all such systems. All such systems:

- are homogenous with respect to technology;
- are governed by a single set of laws;
- 'know' all system participants, ie, they are closed to non-participants.

3.2 A generic model of cross-border electronic authentication

To utilize an application across borders or to utilize a service with a token provided from outside the user service provider's state, the domestic model must be enhanced.

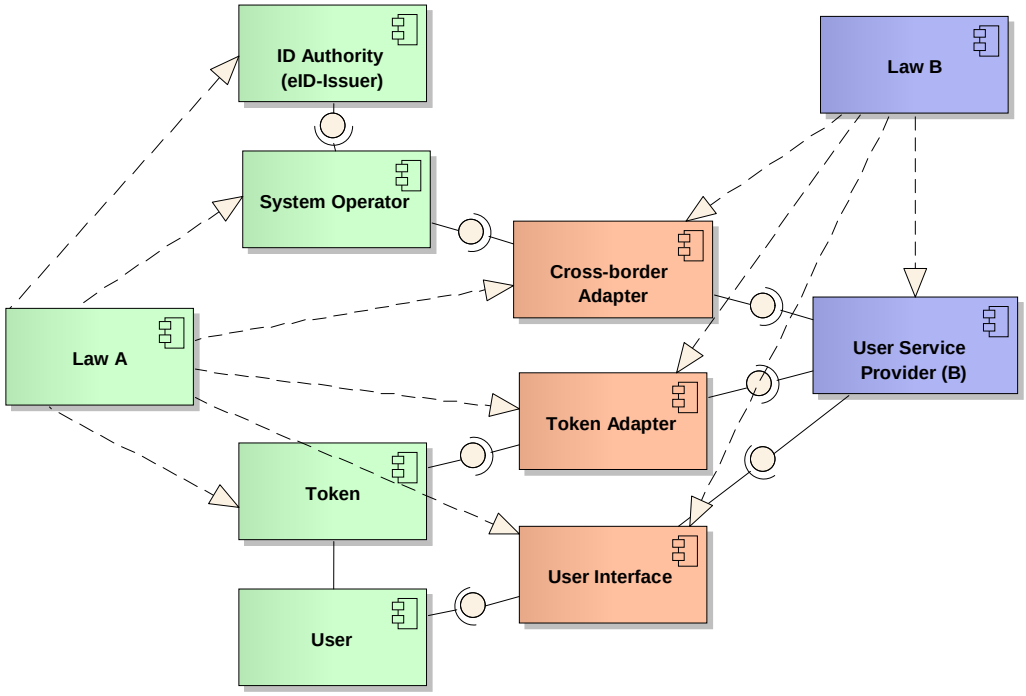


Figure 2: Generic model of cross-border authentication

The big difference in cross-border authentication compared to the domestic model is the fact that **user service provider (B)** is actually a user service provider from another system who is governed by different laws (**Law B**) and business rules than the domestic user service provider. In addition, the other system may use different technology which may be incompatible.

Even more important is the fact that the user service provider (B) is usually not known to the system operator in the sense that there is often no direct contractual agreement and no clear-cut legal regulations that govern their relationship. Even worse, the laws governing the operations of user service provider (B) and the system operator are different, which raises all kinds of problems from data protection to liability and insurance issues.

In order to achieve compatibility between the two systems to the point where a user of the first system may receive services from the second system, adapter components must be introduced into the systems.

The **cross-border adapter** has the task of actually proxying an electronic authentication request from the local service provider (B) across the border between countries and systems to the system operator. This task includes the translation of data formats and business rules wherever necessary. The cross-border adapter may be implemented in a number of ways, eg, using national proxy services, national portals or middleware. For each specific cross-border system, the best and most appropriate implementation must be found. This is not so much a question of technology, but of possible solutions as defined by law and contractual agreements within the systems.

The **token adapter** is the second component that is specific to the cross-border solution of the system. Its main task is interfacing a token from one country with the user service provider from another country. It is responsible for establishing the compatibility of the token with the user service provider's systems. Usually it may be considered to be an extension of the IT systems of the local service provider that are operated by him.

Comparing the generic model of a cross-border authentication system with the domestic system, some changes to the general principles of system design, which are relevant to any security evaluation, are evident. A cross-border system:

- is heterogeneous with respect to technology;
- is governed by two separate and at least partially disjunct sets of laws;
- does not 'know' all system participants, ie, it is potentially open to non-participants.

3.3 Challenges in cross-border authentication

Extending a domestic system to allow cross-border electronic authentication with a communication partner who is not native to the domestic system poses a number of challenges. All these challenges must be addressed and overcome to successfully achieve cross-border interoperability:

- There may be different types of credentials which link the user's identity to a token. *In this context biometric verification, such as fingerprints, may pose major*

problems with respect to technology and security.

- The reliability of the credentials may differ.
  This can pose the problem of maintaining different levels of credibility as well as raise legal issues.
- A wide range of different tokens appears:
  1. electronic and non-electronic tokens with different security levels
  2. tokens with different validities
  3. tokens from previous and/or related systems
  4. tokens which bear different datasets
  5. tokens issued by different system operators or on behalf of governments.

  Even within one domestic system, a number of different tokens may be in use, all of which may require to be supported in the cross-border scenario.
- Different technical infrastructure and equipment are in use.
  While this seems to be primarily a technological issue, the financial consequences involved in supporting these technologies may prove to be the largest problem.
- Different authentication protocols and procedures are in place.
  This is not only a technological problem, but may be a legal issue as well.
- Different sets of personal data come from different countries.
  This addresses technological aspects, such as formats or the use of identifiers.
- Acceptance and trust of personal data come from a foreign country.
  This addresses mostly legal aspects and aspects of trust but also the issue that a user service provider must accept the foreign system operator as an authentic authority.
- Manually checking the authenticity of a foreign token may be required.
  Procedures may have to be implemented that allow the manual verification of the token's authenticity before electronic authentication of the actual request.
- Checking the authorization of a foreign user service provider is required.
  Before answering an authentication request, the system operator must check that the user service provider generating the request is actually allowed to perform this authentication request.

3.4 Security Issues with cross-border authentication

International standards on evaluating information security and information security management systems are found in the ISO standards of the ISO 2700x family. These standards provide fundamental, but often rather general, security requirements. The German Bundesamt für Sicherheit in der Informationstechnik BSI (Federal Office for Information Technology Security) has published a set of German standards BSI 100-1 to BSI 100-4 ([17], [18], [19]). These are compatible to the ISO 2700x standards with the added advantage of practicability and more detailed instructions on how to evaluate security issues and how to set up an appropriate system of security management and

security measures.

The core of any security evaluation according to BSI 100-2 *IT-Grundschutz Methodology* [18] is the definition of assets that must be protected and the requirements for the protection of these assets. *Assets* refer to all the protection-worthy data as well as to the systems which process, store and transport this data. Each asset is assigned a protection requirement for the three basic protection values of confidentiality, integrity and availability.

Basic protection values according to ISO/IEC 27002 [27]	
Confidentiality	ensuring that information is accessible only to those authorised to have access
Integrity	safeguarding the accuracy and completeness of information and processing methods
Availability	ensuring that authorised users have access to information and associated assets when required

Table 1: Basic protection values (ISO/IEC 27002)

BSI 100-2 defines the requirements for protection in three categories:

Protection requirement categories[3]		
ENISA	**BSI-100-2**	**Description**
Low	Normal	The impact of any loss or damage is limited and calculable.
Medium	High	The impact of any loss or damage may be considerable.
High	Very High	The impact of any loss or damage can attain catastrophic proportions.

Table 2: Protection requirement categories

To assign requirements for protection to an asset, the following damage scenarios are evaluated:

- violation of laws, regulations or contracts
- impairment of informational self-determination
- physical injury
- impaired performance of duties
- negative internal or external effects, ie, the impairment of reputation and confidence

[3] *In a deviation from BSI 100-2, the protection requirement categories are named* low, medium *and* high *instead of* normal, high *and* very high. *This is done to establish consistency with other ENISA risk assessments.*

- financial consequences.

A single instance of loss or damage may impact several damage scenarios (eg, fraud usually violates laws or contracts and has financial consequences). As a general, directive BSI 100-2 assumes the maximum principle, ie, if several damage scenarios render different categories of protection requirement for any basic protection value, the highest category is accepted.

For each asset, the results of this analysis are collated in a single table such as the following:

Object name		**Personal data:** (*yes*/*no*)
Protection requirements		**Rationale**
Confidentiality	Medium	Publication of personal data may significantly harm the institution's public and international reputation.
Integrity	High	Widespread fraudulent use may cause ruinous financial obligations.
Availability	Low	Unavailability of e-authentication can be covered satisfactorily by offline verification for a few days.
Major damage scenarios:		
Integrity: sample threat 1		
Confidentiality: sample threat 2		

Table 3: Assessment of protection requirements (sample)

3.4.1 Protection requirements

The following assets are considered worthy of protection. While they are discussed here in the generic model, the reader must be aware that this can only be a starting point when it comes to the evaluation of a specific application.

It should be noted that the assessment of the protection requirements for each asset will differ wildly from application to application. For instance, in a pan-European system for maintaining medical patient's records electronically, the protection requirements regarding the integrity of a person's medical record to be used in medical treatment will obviously be 'very high', since incorrect data could lead to physical injury or even the death of that person.

In accordance to the previous statement, the protection requirements given here must be the **minimum values** for the scenario with the least impact (the common ground on all possible cross-border authentication systems). If a protection requirement is expected to

be higher than the minimum value in a significant number of implementation scenarios, it is stated to be 'at least' the minimum value[4].

3.4.1.1 Personal data

Data directly related to the identity of a person must be considered an asset that is worthy of protection in all cases. With personal data, the foremost concern is confidentiality, since the use of personal data is restricted, at least by the Data Protection Directive (95/46/EC).

The protection requirement category depends very much on the application and on the amount and type of personal data that is transmitted by the cross-border system. Obviously the name, address and date of birth of a person are less critical than any further personal data such as financial, criminal or medical records.

Personal data		**Personal data: yes**
Protection requirements		**Rationale**
Confidentiality	At least 'medium'	Due to the Data Protection Directive and the laws of Member States, any personal data is restricted in usage and distribution.
Integrity	At least 'low'	Impact of any loss of integrity is limited and calculable.
Availability	At least 'low'	Only has limited or no impact if system is not available for several days.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has effect on social or financial standing		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Integrity: falsification of person-related data has effect on social or financial standing		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 4: Protection requirements for personal data

[4] *Thus, if a protection requirement is stated to be 'at least medium', it cannot be set to 'low' in any scenario; as there is at least one scenario where it is 'medium', but there may be a number of scenarios where it must be considered to be 'high'.*

3.4.1.2 Application data

Depending on the type of application, the actual communication payload (beyond personal data) will be worthy of protection. This could be, for example, transaction numbers, status of services or card specific capabilities. At the minimum, this payload must be protected in order to ensure the integrity and authenticity of the data bases at the system operator and at the user service provider. In addition, an electronic authorisation to render a service (eg, a medical treatment) with the admission of and in compliance with the system operator may have a financial value.

Application data		**Personal data: no**
Protection requirements		**Rationale**
Confidentiality	At least 'low'	Impact of any loss of confidentiality is limited and calculable.
Integrity	At least 'low'	Impact of any loss of integrity is limited and calculable.
Availability	At least 'low'	Only has limited or no impact if system is not available for several days.
Major damage scenarios:		
Confidentiality: abuse of application data for non-system purposes		
Integrity: fraudulent use of system		
Integrity: impaired performance of duties due to false data		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		

Table 5: Protection requirements for application data

3.4.1.3 Token

The token usually contains application data as well as personal data. While its availability and confidentiality are mostly within the responsibility of its user (who is not regarded in the assessment of protection requirements), the token's integrity is fundamental to the functioning of any authentication system. Nevertheless confidentiality may also be considered a significant technical assignment, specifically if the token is used for multiple purposes or if regulations require that any access to the token's data requires authentication by the user service provider.

Token		**Personal data: yes**
Protection requirements		**Rationale**
Confidentiality	At least 'medium'	Due to the Data Protection Directive and the laws of Member States, any personal data is restricted in usage and distribution.
Integrity	At least 'low'	Impact of any loss of integrity is limited and calculable. The financial loss is acceptable to the institution.
Availability	At least 'low'	Only has limited or no impact if system is not available for several days.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has effect on social or financial standing		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Integrity: falsification of person-related data has effect on social or financial standing		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 6: Protection requirements for token

3.4.1.4 ID authority

The ID authoriy is the source of the electronic identity based on the person's personal data. An ID authority can be a health insurance register or a civil register which establishes the root of all personal data for the application.

ID authority		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	High	Disclosure of large amounts of personal data of registered persons would cause significant, nation-wide loss of reputation.
Integrity	High	If the integrity of the registers is corrupted, severe issues of liability may arise and trust in the system may be catastrophically compromised.
Availability	Medium	The acceptable downtime is up to 24 hours. Longer downtime may impair the reputation and the performance of duties significantly.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has effect on social or financial standing		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Integrity: falsification of person-related data has effect on social or financial standing		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 7: Protection requirements for ID authority

3.4.1.5 System operator

The system operator or, more precisely, the IT systems of the system operator are protection-worthy assets. The most prominent reason for this is the fact that the system operator hosts the personal data for all users of the system. Thus large-scale abuse of personal data is possible. The confidentiality of this data must be protected. The integrity of this data and of any additional application data must be ensured in order to allow the correct functioning of the system. Obviously the availability of such a system must be sufficiently high to allow timely processing of authentication requests by any local service provider.

System operator		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	At least 'medium'	Impact of the loss of confidentiality on a large amount of personal data sets is considerable.
Integrity	At least 'low'	Impact of any loss of integrity is limited and calculable.
Availability	At least 'low'	Only has limited or no impact if system is not available for several days.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has effect on social or financial standing		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Integrity: falsification of person-related data has effect on social or financial standing		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 8: Protection requirements for system operator

3.4.1.6 User service provider

The IT systems of the user service provider are necessary for his provisioning of services. As these IT systems process personal data as well as application data, the protection requirements for confidentiality and integrity are at least governed by the maximum principle. Depending on the specific application and the distribution density of local service providers, the protection requirements for availability may range from normal to very high.

User service provider		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	At least 'medium'	Due to the Data Protection Directive and the laws of Member States, any personal data is restricted in usage and distribution.
Integrity	At least 'medium'	Falsified tokens may cause significant financial damage to the system.
Availability	At least 'low'	Only has limited or no impact if system is not available for several days.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has effect on social or financial standing		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Integrity: falsification of person-related data has effect on social or financial standing		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 9: Protection requirements for user service provider

3.4.1.7 Cross-border adapter

The IT systems of the cross-border adapter are obviously the focus in any security evaluation of an electronic cross-border authentication process. As this component bridges not only two separate IT systems but also two separate sets of governing laws, a careful analysis of the security issues involved is strongly recommended for any specific application.

Following the maximum principle, these IT systems are assigned at least the highest protection requirements for personal data and application data. Depending on how the cross-border adapter is implemented in a specific system, it may be necessary to divide this asset into separate assets with different tasks and appropriate protection requirements.

Cross-border adapter		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	At least 'medium'	Due to the Data Protection Directive and the laws of Member States, any personal data is restricted in usage and distribution.
Integrity	At least 'low'	Impact of any loss of integrity is limited and calculable.
Availability	At least 'low'	Only has limited or no impact if system is not available for several days.
Major Damage Scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has effect on social or financial standing		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Integrity: falsification of person-related data has effect on social or financial standing		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 10: Protection requirements for cross-border adapter

3.4.1.8 Token adapter

The token adapter is the second component which is specific to the cross-border solution of the system. Its main task is interfacing a token from one country with the user service provider from another country. It may usually be considered an extension of the IT systems of the local service provider.

Cross-border adapter		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	At least 'medium'	Due to the Data Protection Directive and the laws in Member States, any personal data is restricted in usage and distribution.
Integrity	At least 'low'	Impact of any loss of integrity is limited and calculable.
Availability	At least 'low'	Only has limited or no impact if system is not available for several days.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has effect on social or financial standing		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Integrity: falsification of person-related data has effect on social of financial standing		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 11: Protection requirements for token adapter

Please note that the threats given in Table 11 are often resolved by reducing the token adapter to standardized hardware and software that is integrated in the user service provider's IT systems.

3.4.1.9 User interface

The user interface is the third component which is specific to the cross-border solution for the system. Its main task is providing an end-user interface between the user and the user service provider. In systems where the user does not interact directly with an IT system, this component may be omitted.

User interface		**Personal data: yes**
Protection requirements		**Rationale**
Confidentiality	At least 'medium'	Due to the Data Protection Directive and the laws in Member States, any personal data is restricted in usage and distribution.
Integrity	At least 'low'	Impact of any loss of integrity is limited and calculable.
Availability	At least 'low'	Only has limited or no impact if system is not available for several days.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has effect on social or financial standing		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Integrity: falsification of person-related data has effect on social or financial standing		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 12: Protection requirements for user interface

3.4.2 Generic threats

The following technical security risks arise from studies of the generic model and must be coped with in every electronic cross-border authentication project:

- Different types of credentials and their reliability may lead to falsified personal data and fraudulent tokens.
- Tokens with different security levels differ in their trustworthiness.
- Dubious user service providers or cross-border adapters could withdraw, cache and misuse personal data.
- Different technical infrastructures elevate the number of security vulnerabilities due to different security levels.
- Different authentication protocols and procedures elevate the number of security vulnerabilities due to different security levels.
- Man-in-the-middle attacks, where an attacker inserts himself between the user's computer or terminal and somewhere on the network in an authentication

exchange and poses as the user service provider to the system operator and vice versa are potentially easier.

- Illegitimate tracking of the user's location or behaviour, where the attacker generates a person or card-specific profile from the locations of the related card or card readers, the times of use, etc.
- Attacks on the availability of the cross-border authentication process, eg, by creating large amounts of false authentication requests as a denial of service attack.
- The additional systems involved in the cross-border authentication process may not be trustworthy.

In addition to the technical issues, some legal problem areas are encountered in the generic model:

- National restrictions on the transfer of personal data across borders may differ, particularly with regard to national identification numbers or other identifiers, which may prohibit cross-border electronic authentication.
- National regulations may prohibit authentication across borders, eg, the usage or verification of the certificates in cross-border transactions.
- User service providers may try to obtain tokens or token data from sources other than directly from the user within a legitimate authentication process.
- The personal data may not be processed in an adequate, relevant and non-excessive way for the purposes for which they are collected and/or processed further, eg, more personal data is transferred than needed. Also the interpretation of what is adequate may differ from Member State to Member State.
- The Data Protection Directive (95/46/EC) may not be implemented fully in one or more of the Member States participating in a cross-border authentication process.
- The national interpretation of the Data Protection Directive (95/46/EC) and the national data protection laws may differ significantly between the Member States participating in the cross-border authentication process.
- The liability of user service providers for damages may differ significantly between Member States.
- There may be differences between the Member States in the legal obligations of user service providers to take out appropriate liability insurance.
- The liability of agencies involved in realizing the cross-border adapter may be complicated and may create a complex mesh of regulations concerning liability and waivers of liability.
- Incident handling may be complicated and hampered by questions on the applicability of national laws.

4 Case studies

4.1 NETC@RDS for eEHIC ID

4.1.1 System overview

The European Health Insurance Card (EHIC) facilitates access to health care services for insured European citizens during temporary stays abroad. This card should ensure that an individual obtains the same access to the public health care services as a national of the country being visited. As of today, the EHIC is mostly realized as a printed version of a national health insurance card (HIC) or as an electronic data set stored on a national electronic HIC.

The NETC@RDS project ([26], [28]) established an online service for the EHIC to authenticate a patient's health insurance chip card and/or a patient's entitlement to health insurance benefits abroad but inside the EU/EFTA for unplanned care. In the long run, the overall goal of this project is the complete integration of the existing and future national infrastructures for health insurance claims in order to improve the exchange of data.

The project is being run by by the NETC@RDS Consortium, which includes stakeholders from 15 European countries and which is co-founded by the EU. It started in September 2002 and has been in the implementation phase since June 2007. In a preceding evaluation phase, 85 pilots successfully were tested across 10 EU Member States and the first existing pan European eHealth connection was established.

The implantation phase will encompass 500 health care service points in 260 service units in 16 EU/EFTA Member States and Switzerland. The initial deployment of this infrastructure is regarded as a test-bed for the ongoing introduction of the e-EHIC.

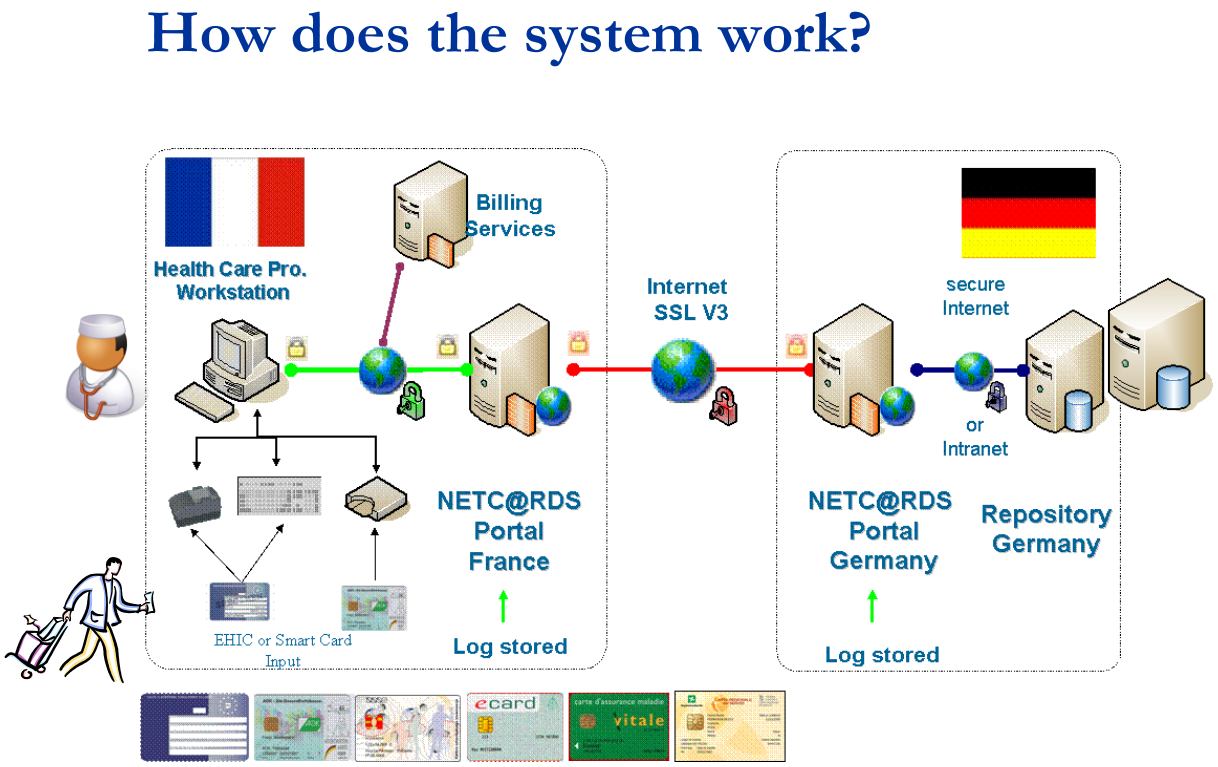


Figure 3: How the existing NETC@RDS system works[5]

The system will be used by national health care providers in hospitals and ambulatory facilities. They benefit from this service by electronically reading the e-EHIC dataset, either from a national health insurance card or by scanning the printed EHIC. This simplifies the existing manual paper-based process and delivers a precise insurance dataset for further processing.

Other groups which benefit from this service are the health insurance and the cross-border cost clearance organizations involved in the reimbursement process. In particular the reimbursement process is improved, because of reduced fraudulent or irrelevant claims, which reduces the complex health-costs claim procedures between the countries.

The NETC@RDS technical architecture [25] consists of secure network interconnections within and between Member States, linking national service portals and registries in each country with workstations within all service facilities.

Furthermore, cross-border mutual authentication is established every time a NETC@RDS user (typically a hospital clerk or a health practitioner) operates the online verification process of an e-EHIC dataset to verify entitlement to receive health care abroad in one of the NETC@RDS service units or points.

[5] *Courtesy of Mr Nader, Project Coordinator, NETC@RDS*

In today's solution, the NETC@RDS architecture features a direct communication between the individual national service portals as shown in Figure 3. The secure network interconnection between the 16 national portals relies on a common information security systems policy (ISSP), for which a common set of tools has been devoted to security audit at all the national portals. The ISSP describes the NETC@RDS information system security needs and requirements and provides the bases for a secure operational environment. To be allowed to access or connect its portal to other portals, each partner must respect it.

As foreseen in the ISSP, security audits must be conducted each year to verify compliance with the NETC@RDS ISSP. A suitable security audit procedure and tool has been constructed and approved. This audit procedure has been agreed and it is currently under implementation by all partners. It has already been successfully conducted by several partners.

With the introduction of the EESSI (Electronic Exchange of Social Security Information) service network [29], which will connect institutions at a European level through a central node, establishing the connection between the national service portals using the EESSI network is planned.

The planned solution using the EESSI service network has been targeted in this case study and will be discussed from here on.

The secure network interconnection between the national portals will be provided by integration within the EESSI service network. The related national health insurance networks will be connected by establishing national portals, which will connect with each other via the EESSI network. A cross-border electronic authentication request will be routed through this network.

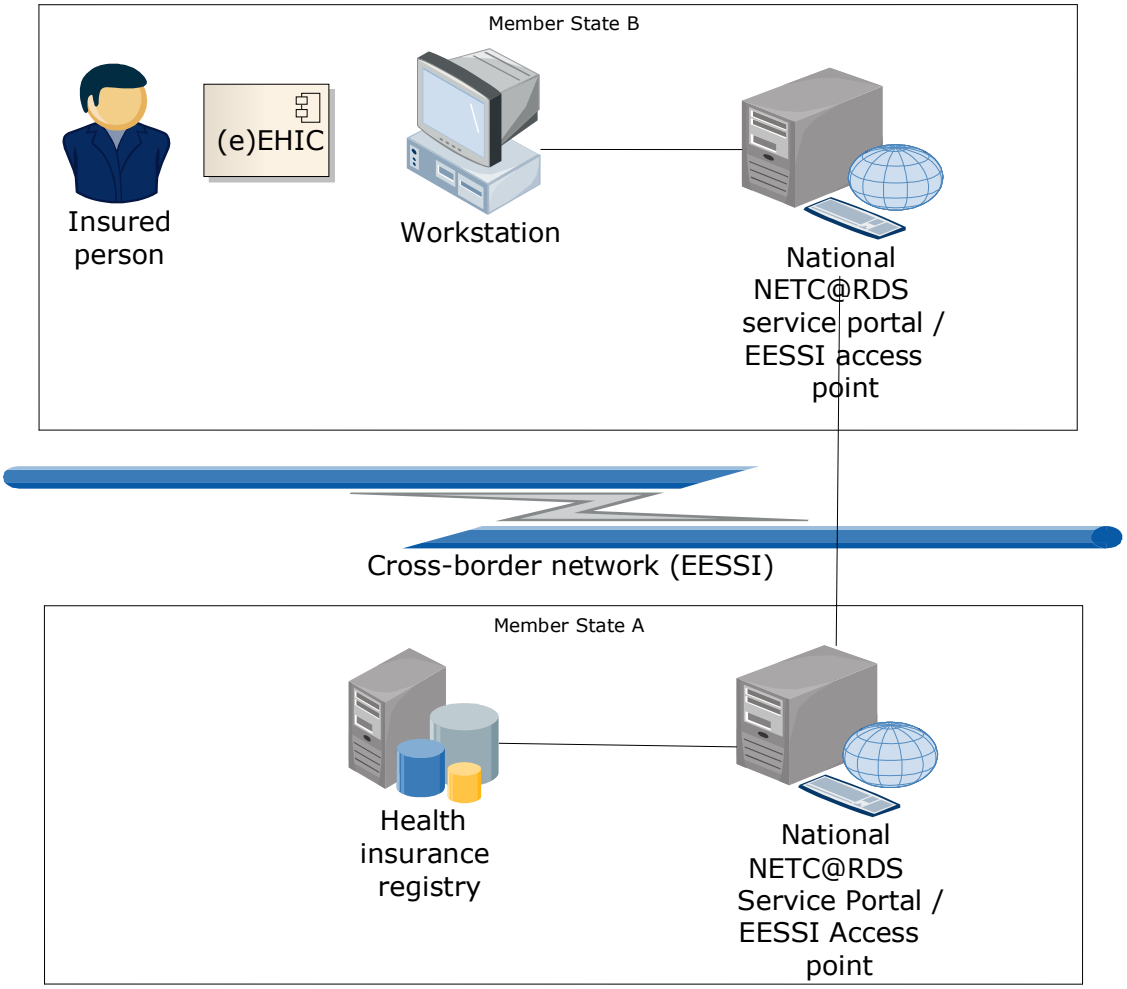


Figure 4: System overview

It is possible to use different types of an electronic national health insurance card or a non-electronic printed European Health Insurance Card with the system. Each type may bear a different insurance data set format. The type of card issued depends on the individual Member States. But no matter what type of card is presented at a workstation in a hospital or ambulatory facility, the technical infrastructure enables a check to be made as to whether the entitlement is deemed valid by the issuing institution.

4.1.2 Scenario: Going to a doctor while on vacation in another European country

One of the most important purposes of an eEHIC is to prove the entitlement of a European citizen outside his or her home Member State when requesting healthcare services. This

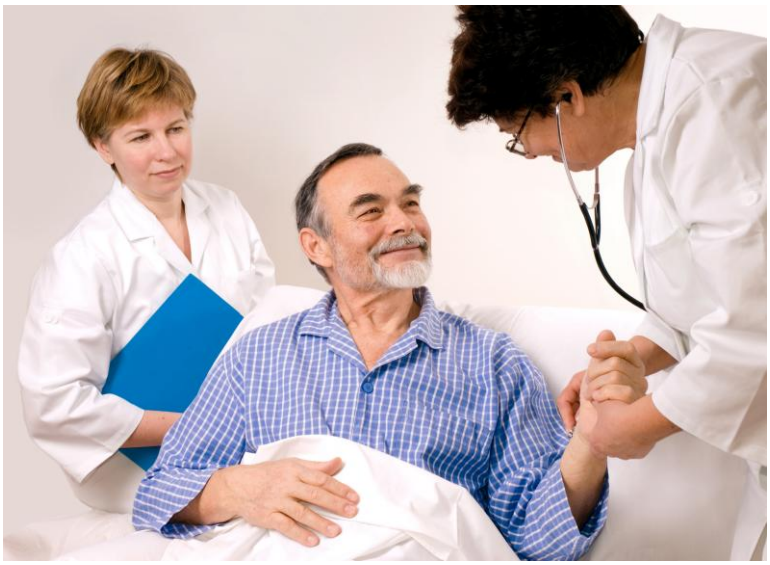
can be described as follows:

A French citizen is on vacation in Germany and needs to use unplanned healthcare services, ie, the visitor goes to a German doctor because of sickness or maternity. For her entitlement, she uses her electronic national Health Insurance Card (or an EHIC) and provides it at the front desk at the doctor's facility. The card, containing the eEHIC dataset, is read by a smart card reader connected to the front desk workstation.

This workstation connects to the national German NETC@RDS service portal via an online connection and tries to verify the dataset. To this end, it is necessary to authenticate the German doctor to this portal. The German NETC@RDS service portal then contacts the French NETC@RDS service portal, which in turn contacts the French health insurance company for verification of the dataset and for authorization of the entitlement. This verification of entitlement contains the actual electronic authentication as a first step. The result of this verification is the decision (yes/no) about the entitlement of the patient, which is transmitted back to the front desk workstation of the German doctor.

4.1.3 Mapping the generic model to the NETC@RDS implementation

To access the security issues for cross-border electronic authentication, the NETC@RDS technical infrastructure using the EESSI service network was mapped to the generic model from chapter 3.2. The NETC@RDS model, including this mapping, is displayed in Figure 5.



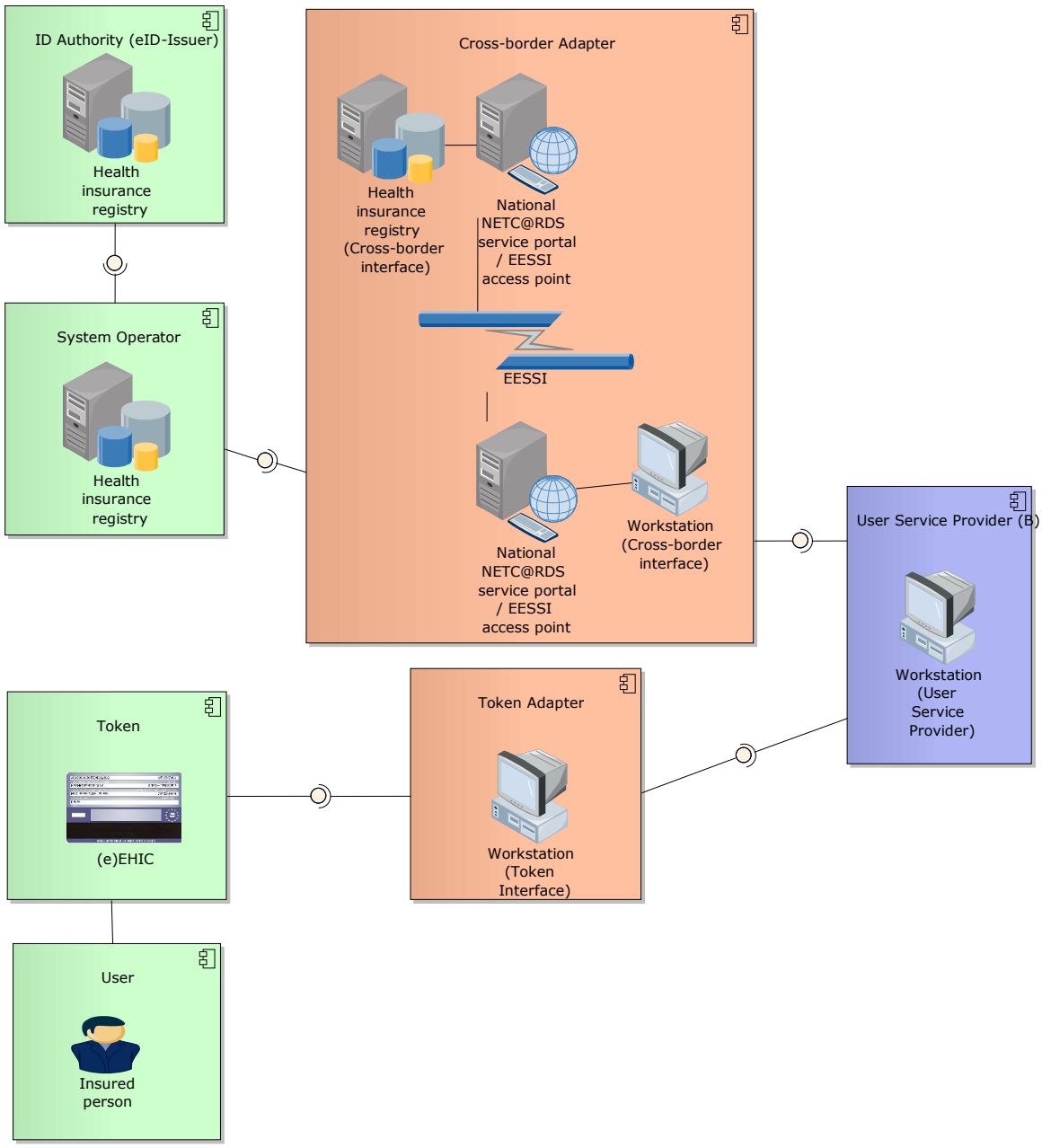


Figure 5: Mapping of NETC@RDS components to the generic model

Mapping the generic model to NETC@RDS provides the following relations: The insured person residing outside his or her home Member State, who is requesting health services, is the generic model's user. This user is entitled to obtain these services according to regulation 1408/71 [30]. The eEHIC maps to the token. The minimum set of data held on

the token is prescribed in Administrative Decision No 189 of 18th June 2003 [5].

The workstation within a hospital or ambulatory facility represents primarily the user service provider of the generic model. This workstation also reads the EHIC dataset from the token. This part of the workstation's hardware and software realizes the token adapter.

That part of the NETC@RDS workstation which interfaces with the NETC@RDS service portal must be considered to be a first subcomponent of the cross-border adapter.

The generic model's cross-border adapter extends to the NETC@RDS service portals and EESSI network and infrastructure. It also includes that part of the health insurance registry which is responsible for catering to requests from the NETC@RDS service portal. The remaining parts of the health insurance registry map to the generic model's system operator. The health insurance registry is also regarded as the identity authority. In this area, the related national laws and regulations apply as well as the security policy of the health insurance company.

By following this approach, the NETC@RDS project would be following European Regulations 883/2004 on the coordination of social security systems [4], which is expected to be applicable by May 2010. Additionally, national laws and regulations are applicable to each portal.

4.1.4 Protection requirements

The NETC@RDS project is evolving over time through the introduction of new technologies and services as these become widely available throughout Europe. This entails the need to frequently re-evaluate security threats and the measures implemented to counter them. This case study is based on the next evolutionary step of NETC@RDS as was current at the time of writing.

In this scenario the national service portals will communicate with each other securely via the EESSI network. In this function, it is assumed that each national portal authenticates its domestic communication partners as persons or institutions who are authorized to request an electronic authentication. The national service portals and health insurance registers in other countries are not required to electronically authenticate the requesting health professional or institution as entitled to perform an authentication request, but can and must rely on the functioning of the first country's national service portal.

4.1.4.1 Personal data

The personal data used and transmitted in the NETC@RDS electronic authentication process is defined in the CEN Workshop Agreement CWA 15974 (May 2009) [25]. According to this document, the EHIC data comprises the following mandatory information:

- surname of the card holder ('Name' on the face of the EHIC card),
- forename of the card holder ('Given names' on the face of the EHIC card),
- personal identification number of the card holder,
- date of birth of the card holder,

- expiry date of the card,
- ISO code of the Member State issuing the card (with the exception that UK, rather than GB, is used for the United Kingdom),
- identification number and acronym of the competent institution,
- logical number of the card (including a card issuer identifier),
- identification of the paper form that is replaced by the card.

Three optional extensions of this data set are permitted:

- The character string data, such as the name of the card holder, can be held several times, with each instance being a transliteration of the string into a different character set.
- The gender of the card holder may be included.
- The card issuer may include the address and telephone numbers of the card holder.

The EHIC data set is transmitted to the health insurance registry (the system operator) during authentication.

Personal data		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	Medium	A loss of confidentiality might have a significant negative effect on the reputation of the system and its participants.
Integrity	Medium	Loss of integrity may impair the performance of duties to the point where some of the individuals affected would consider it intolerable (eg, because of substantial upfront payments for medical services).
Availability	Medium	The acceptable downtime is up to 24 hours. Longer downtime may impair the reputation of the system and the performance of duties significantly.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes[6]		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Availability: impaired performance of duties		
Availability: negative effects on system reputation due to unavailability of service		

Table 13: Protection requirements for personal data

4.1.4.2 Application data

In addition to the EHIC data set, other information is transmitted during the authentication of an entitlement. This data comprises identification data on the health care professional and his institution (the user service provider), return codes and additional entitlement data.

[6] *The EHIC dataset is not generally encrypted.*

Application data		Personal data: no
Protection requirements		**Rationale**
Confidentiality	Low	Impact of any loss of confidentiality is limited and calculable.
Integrity	Medium	Loss of authenticity (falsified entitlements) may cause significant financial damage.
Availability	Medium	The acceptable downtime is up to 24 hours. Longer downtime may impair the reputation of the system and the performance of duties significantly.
Major damage scenarios:		
Confidentiality: abuse of application data for non-system purposes[7]		
Integrity: fraudulent use of system		
Integrity: impaired performance of duties due to false data		
Availability: impaired performance of duties		

Table 14: Protection requirements for application data

4.1.4.3 eEHIC (token)

The eEHIC contains the holder's personal data. This data is defined to be freely readable. An authentication mechanism for the eEHIC may be implemented optionally, but this must not hinder free access to the eEHIC dataset. The mandatory EHIC dataset is also printed on the surface of the eEHIC. The eEHIC is under the control of the user, and it is assumed that the user consents to having the data read by handing the eEHIC to somebody.

[7] *Messages are mostly communicated via secured connections but this is, in part, not mandatory.*

eEHIC		Personal data: yes
Protection Requirements		**Rationale**
Confidentiality	Medium	A loss of confidentiality might have a significant negative effect on the reputation of the system and its participants.
Integrity	Medium	Falsified eEHICs may cause significant financial damage to the system.
Availability	Low	Only has limited or no impact if the eEHIC is not available for several days[8].
Major damage scenarios:		
Integrity: identity theft[9]		
Integrity: impaired performance of duties due to false data[10]		

Table 15: Protection requirements for token

The personal data on the eEHIC is considered to be under the control of the identified person and therefore to have a comparatively low impact on the right of informational self-determination. Because of this the security measures of the eEHIC with respect to confidentiality must only satisfy a 'low' requirement for protection.

4.1.4.4 Health insurance organization (ID authority)

The ID authoriy is typically the health insurance organization where the person is insured. Within this organization the person's electronic identity is provided based on his registration data.

[8] *While the individual user may suffer some damage, this is calculable and limited. Obviously this addresses only the individual failure of an eEHIC and not the substantial damage that may be caused by a failure of a series of whole eEHICs.*

[9] *Minimal security is achieved by printing the EHIC dataset on the card body, which may be verified against the insured person's identity documents.*

[10] *In the sense that if data on the chip is corrupted, it may be copied from the printed surface of the eEHIC.*

ID authority		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	High	Disclosure of large amounts of the personal data of insured persons would cause significant, nation-wide loss of reputation.
Integrity	High	If the integrity of the registers is corrupted, severe liability issues may arise and the public trust in the system may be catastrophically compromised.
Availability	Medium	The acceptable downtime is up to 24 hours. Longer downtime may impair the reputation and the performance of duties significantly.
Major Damage Scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has effect on social or financial standing		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Integrity: falsification of person-related data has effect on social or financial standing		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 16: Protection requirements for ID authority

4.1.4.5 Health insurance register (system operator)

The health insurance register or the IT systems of the health insurance company hosts the personal data for a large number of users of the system. Thus, large scale abuse of personal data is possible. The confidentiality of this data must be protected. The integrity and availability of this data and of any additional application data must be ensured in order to allow the correct functioning of the system.

Nevertheless these aspects are beyond the scope of a risk assessment for cross-border authentication, since the health insurance company is also required to maintain the required levels of security in its regular domestic and non-electronic cross-border operations. One main concern of the health insurance company, as a stakeholder and participant in the NETC@RDS system, must be that the introduction of this system must not compromise the company's established security levels.

Health insurance register		**Personal data: yes**
Protection requirements		**Rationale**
Confidentiality	High	Disclosure of large amounts of the personal data of insured persons would cause significant, nation-wide loss of reputation.
Integrity	Medium	Loss of integrity in the database of insured persons may cause significant financial damage and considerable impairment in the performance of duties.
Availability	Medium	The maximum downtime is less than one day.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		

Table 17: Protection requirements for system operator

4.1.4.6 Workstation (user service provider)

The workstation at the medical institution has the primary function of allowing the medical institution to provide and account for services within its own national health care system. This functionality must not be compromised by extending the workstation's tasks to accommodate the NETC@RDS system.

The evaluation of security threats and protection requirements is limited to the functionality of the workstation that concerns the processing and storing of data related to the NETC@RDS system. The primary function of the workstation may pose other (higher) requirements.

Workstation		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	Medium	Due to the Data Protection Directive and the laws of Member States, any personal data is restricted in usage and distribution.
Integrity	Low	Any consequences of a loss of integrity will be limited and calculable[11].
Availability	Low	Unavailability of the workstation for a few days will have limited consequences only.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes[12]		
Integrity: identity theft[13]		
Integrity: impaired performance of duties due to false data		

Table 18: Protection requirements for user service provider

4.1.4.7 Workstation (cross-border adapter)

Software and potentially hardware must be added to the (domestic) workstation in the health care institution and the associated local IT systems in order to allow cross-border authentication within the scope of the NETC@RDS system.

These components are considered part of the cross-border adapter and are governed by the related local laws and contracts.

It is assumed that communication with the national service portal is effected via a secure connection that requires mutual authentication.

---

[11] This assumes a 'regular' medical institution within the national health care system. For an institution that specializes on providing services to foreign patients, the resulting damage from a loss of integrity may be considerable.

[12] The medical institution is legally required to observe data protection regulations, but should be contractually or legally required to adopt appropriate security measures.

[13] This is limited to the discretion of the health professional in identifying the patient as the legitimate owner of the eEHIC. Identity theft that is assisted by a health care professional (eg, for fraudulent billing purposes) is not countered.

Workstation (cross-border adapter)		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	Medium	Personal data is transmitted to external systems. Disclosure of this data to unauthorized external systems will violate laws and regulations as well as impair the individual's right to informational self-determination.
Integrity	Low	Impact of any loss of integrity is limited and calculable[14].
Availability	Low	Only limited or no impact if system is not available for several days.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		

Table 19: Protection requirements for cross-border adapter

4.1.4.8 National service portal (cross-border adapter)

The national service portal is the national focal point for all NETC@RDS cross-border activities. It is the interface between the national network and the European EESSI network.

One main task of this portal is the authentication of health professionals and medical institutions to authorize the authentication request to the foreign health insurance registry. The national service portal passes authentication requests from domestic medical institutions across the border and receives authentication requests from abroad to be passed to the domestic health insurance registers.

[14] *A request may have to be resent or aborted for the manual alternative.*

National service portal		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	Medium	Due to the Data Protection Directive and the laws of Member States, any personal data is restricted in usage and distribution.
Integrity	Medium	Allowing false authentications opens the door to large-scale abuse.
Availability	Medium	The service portal may not be unavailable for more than 24 hours.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes[15]		
Integrity: identity theft		
Integrity: falsification of the authorization data of system participants may cause a severe breach of security		
Availability: impaired performance of duties		

Table 20: Protection requirements for cross-border adapter

4.1.4.9 EESSI

As a secure network, the EESSI[16] (Electronic Exchange of Social Security Information, not to be mistaken for the European Electronic Signature Standardization Initiative) [29] is part of the cross-border adapter.

The EESSI project (formerly PROTECTUS) will allow the pan-European electronic exchange of data regarding social security between Member States.

The main features of the agreed EESSI architecture are:

- use of s-Testa (which is an IDABC-driven secure *Trans European Services for Telematics between Administrations* network) as the backbone,
- minimum of one and maximum of five access points per Member State,
- online transaction facilities for posting the electronic European Health Insurance Card,

[15] *There is a substantial potential for organizational misuse, since the service portal acts as a communication node through which all information is passed.*

[16] *See also: http://ec.europa.eu/idabc/en/document/7189/*

- compulsory use of a central node,
- flexible use by Member States of a Commission-developed reference implementation (RI) which will be made available free of charge to Member States.

In this way, EESSI will provide a secure network between national service portals, including their authentication. The NETC@RDS project aims to include the services developed for electronic data exchange in the EESSI network in compliance with the new European Regulation 883/2004.

EESSI		**Personal data: yes**
Protection requirements		**Rationale**
Confidentiality	High	Large-scale unlawful disclosure of the personal data of European citizens through the European social security network may have a disastrous pan-European effect on the reputation of and confidence in the electronic social security network and the institutions it represents.
Integrity	High	If the integrity of the access to authorization registers is corrupted, severe liability issues may arise and the confidentiality of system may be catastrophically compromised.
Availability	Medium	As a pan-European communication node for social security electronic interchange, the acceptable downtime will be less than 24 hours.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has effect on social or financial standing		
Integrity: identity theft		
Availability: impaired performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 21: Protection requirements for EESSI

4.1.4.10 Workstation (token adapter)

The token adapter is the additional hardware and software in the workstation at the hospital or ambulatory institution that implements the physical and logical aspects of communicating with the eEHIC. These components are only considered to be the token adapter if they are not part of the IT system that supports the domestic health insurance card.

Workstation (token adapter)		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	Medium	Due to the Data Protection Directive and the laws of Member States, any personal data is restricted in usage and distribution.
Integrity	Low	Impact of any loss of integrity is limited and calculable[17].
Availability	Low	Only has limited or no impact if system is not available for several days[18].
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Integrity: identity theft		

Table 22: Protection requirements for workstation (token adapter)

4.1.5 Conclusive risk assessment

Because of the rather imperfect way the EHIC is used today (with health professionals having low confidence in the authenticity of insurance claims by patients and cumbersome administrative billing processes), electronic authentication may be expected to boost efficiency and lower the administrative cost of processing claims.

With the integration of EESSI as a pan-European secure network, the NETC@RDS project is gaining stability and security and adoption by Member States is becoming easier compared to direct bilateral connections. Still some areas of risk remain to be discussed[19].

4.1.5.1 Authenticity of the eEHIC

The trustworthiness of the EHIC dataset provided by the NETC@RDS application relies on the acceptance of national health insurance cards as a security token shown by the insured patient at the point of health care delivery. If supported by the national HIC and the health care provider's IT systems, the card will be authenticated on-line based on the specific

[17] Accepting that the authenticity of the eEHIC is not required to be validated, the use of a falsified or stolen eEHIC must be considered as having no impact, if the authentication with the Health insurance register fails or has little impact, or if the authentication passes and services are provided and billed to the health insurance company.

[18] This assumes that the health care institution does not specialize in providing services to European visitors.

[19] The risk analysis raised a multitude of risks and an appropriate number of security measures to counter these in the NETC@RDS system were found. The risks discussed here address only the most relevant issues.

national protocol of the card issuing system.

A fundamental security threat in the design of the NETC@RDS system is the decision that the e-EHIC itself need not necessarily be authenticated as the token. While the specifications provide for an optional electronic authentication of the national health insurance card hosting the EHIC dataset, this has little impact on security since the operator at the medical institution may not be able to electronically access this token and, even then, may still decide whether or not to use this authentication mechanism. Possible exploits, based on accepting the eEHIC on sight, include fraudulent use of copied eEHICs to receive health care services and play-back attacks where a health care provider uses eEHIC data sets to create fake incidents that are billed to the health insurance companies.

This security risk is inherent in the system design due to the necessity of supporting all kinds of EHIC technologies. There is neither a requirement to implement any authentication mechanism at all in a national health card, nor is there a requirement to support all known authentication mechanisms at all health care providers. Any solution to this risk lies in the common responsibility of Member States and would require their agreement on one solution. It cannot be met effectively by NETC@RDS since it is beyond NETC@RDS' normative authority.

Such an agreement between the Member States might favour electronic authentication of the eEHIC by simplifying or accelerating the billing process. The full utilization of the benefits of an eEHIC authentication process may thus be an incentive to Member States to implement these mechanisms without exerting undue pressure on Member States by continuing to support the hereditary, albeit more cumbersome, tokens and processes.

4.1.5.2 Entrusting personal data to a foreign system

A general problem of processing personal data in cross-border scenarios is the risk of entrusting this personal data to an institution that is not governed by the same set of laws and, more specifically, not by the same regulations on data protection. National law may even prohibit the electronic transmission of personal data across borders in general, and amendments to national laws and regulations may be required to allow participation in the NETC@RDS eEHIC scheme for electronic authentication.

The disclosure of the personal data of insured persons on a large scale may cause severe damage to public trust in the national health insurance system.

Council Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems [4] laid the foundation for the regulations that will govern the electronic exchange of electronic data regarding social security, including health care services:

> (40) The use of data-processing services for exchanging data between institutions requires provisions guaranteeing that the documents exchanged or issued by electronic means are accepted as equivalent to paper documents. Such exchanges are to be carried out in accordance with the Community provisions on the protection of natural persons with regard to the processing and free movement of personal data.

Even assuming the transference of the Community provisions on data protection to national laws in each Member State, Member States with stricter data protection regulations may have to evaluate the related data protection laws of the other Member States to evaluate the compatibility of the corresponding regulations.

Aggravating this problem is the fact that, in general, the health insurance companies will not have direct contractual agreements with each health care provider in another European country. This limits the possibilities for including non-disclosure clauses with penalties in contracts, as is common in other (commercial) cross-border agreements.

Nevertheless this remains a problem in the domain of laws, regulations and contracts and therefore it should be resolved within this domain. In order not to unduly interfere with national laws and data protection schemes, it may be easiest to agree on the strictest and most constraining regulations as part of summary contracts between the health care system participants (where applicable).

Within NETC@RDS, health insurance organizations which are providing the NETC@RDS service to their (insured) customers have signed a multilateral agreement (the so-called NETC@RDS General Agreement). This contract contains a commitment to *organisational* and technical safety measures to prevent unauthorized access and to fulfil all applicable regulations on data protection.

4.1.5.3 Authenticating health professionals

A European Health Professional Card is envisioned in European Directive 2005/36/EC [2] with the primary intention of facilitating the free movement of health professionals in Europe. The HPRO CARD project [32] established a working group in 2007. While two work packages are concerned with the strong authentication of health professionals and the interoperability of different (national) authentication systems, it may be expected that it will take several years before the European Health Professional Card will be in widespread use in Europe in the form of an electronic smart card with strong authentication.

Until such a time, the health insurance companies' difficulty of establishing sufficient trust in the identity of a health professional or a health care institution across borders remains. The approach of using the national service portal as a 'trusted third party', that vouches for the health professional's identity, is practical and in principle sound. Nevertheless it raises issues of liability[20].

The question on how to enable the National Service Portal to authenticate the health professional with sufficient confidence also remains. This is entirely within the domain of the relevant Member State, so that varying levels of confidence and security may be expected throughout the European Community. While some Member States use electronic health professional cards, other Member States do not as yet use any token-based authentication mechanism.

---

[20] *Is the national service portal accountable for damages caused by an imposter health professional who was accepted by it?*

One possible remedy to this dilemma is the creation and implementation of an IT security policy (ISSP) as done by NETC@RDS. Such a security policy could also state expectations with respect to the service availability of the national service portals.

In addition, a recommendation on the minimal security required in national networks could be given or – depending on the extent of the authority of the normative agency – could even be made a prerequisite for the participation of Member States in the system.

4.2 STORK

4.2.1 System overview

Within EU Member States, the administrative formalities of daily life are being increasingly simplified by online access to public services. The introduction of national electronic identities, ie, the introduction of national eID cards (eID[21]), as a gateway to personal information greatly facilitates the use of eGovernment services. The identity of citizens, business employees and civil servants can be electronically proven by the use of such an eID.

The goal of the STORK (Secure idenTity acrOss boRders linKed) project [33] is to establish the cross-border recognition and authentication of eIDs issued by other EU Member States. This will simplify administrative formalities across EU borders. To this end the STORK project develops rules and specifications to assist the mutual recognition of eIDs, taking into account existing infrastructures and specifications. Furthermore, pilot applications, implementing and utilizing cross-border authentication in real-life environments will be realized. Pilot #1 will demonstrate the operation of cross-border electronic authentication in several Member States. The project also interacts with other European eID projects to maximize the field of applications.

STORK runs under the ICT Policy Support Programme of the Competitiveness and Innovation Framework Programme (CIP). As of mid-2009, 14 States and 29 consortium partners composed of public and private sector organisations were participating in the project. It started in June 2008 and will run for three years.

The project's technical infrastructure [24] consists of:

- national identity providers linked with national pan-European proxy services (PEPS) [8],
- system operators of the eID system, connected to their PEPS at national level,
- workstations, including specific software for online access by citizens.

In this architecture the cross-border electronic authentication requests will be bundled in

[21] *In STORK terminology, eID describes not only the electronic identity but also and foremost the electronic identity document, eg, the national ID card.*

the national PEPS and forwarded to the citizen's home Member State PEPS for authentication with the national system operator.

This infrastructure will ensure interoperability with existing national eID systems. In general, STORK will be kept as technologically transparent as possible and will utilize open standards wherever possible.

STORK pilot #1 will demonstrate the operation of cross-border electronic authentication in several Member States by implementing a demonstrator. The authentication process can be realized using different approaches. The discussion that follows in this document is limited to evaluating the PEPS approach.

4.2.2 Scenario: Cross-border authentication using the proxy service approach

A Spanish citizen staying in Belgium starts using a Belgian eGovernment service (eg, for registering the change of his address in Belgium) via his workstation. The selected eGovernment service requests authentication of the citizen's identity and offers an option for the authentication of non-Belgians. The eGovernment service sends a request for authentication with the required level to the Belgian PEPS. This offers the Spanish citizen a list of qualified Member States which support the required electronic authentication. After the citizen selects 'Spain' the Belgian PEPS sends the request for authentication to the Spanish PEPS.

This asks the user which eID he intends to use, presenting the citizen with a list of suitable eIDs. After its selection, the eID is validated by a specific interactive process through the Spanish PEPS system. Should validation fail, the citizen will be notified directly. Should validation be successful, an assertion will be sent by the Spanish PEPS to the Belgian PEPS which validates and converts the assertion. Then the converted assertion is sent to the Belgian eGovernment service. Thus, the citizen is sufficiently authenticated to proceed to use the service.

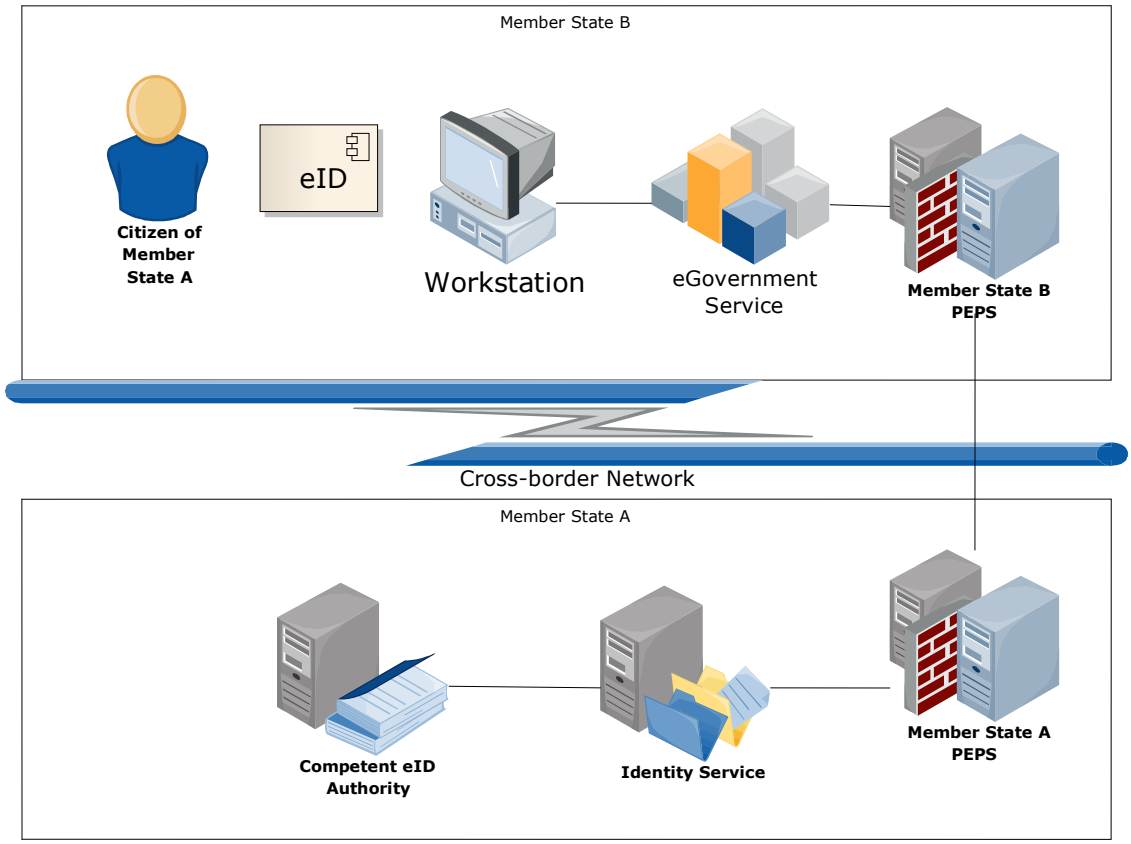


Figure 6: STORK system overview

4.2.3 Mapping the generic model to the implementation

To illustrate the security issues in cross-border electronic authentication, the STORK infrastructure is mapped to the generic model from chapter 3.2.

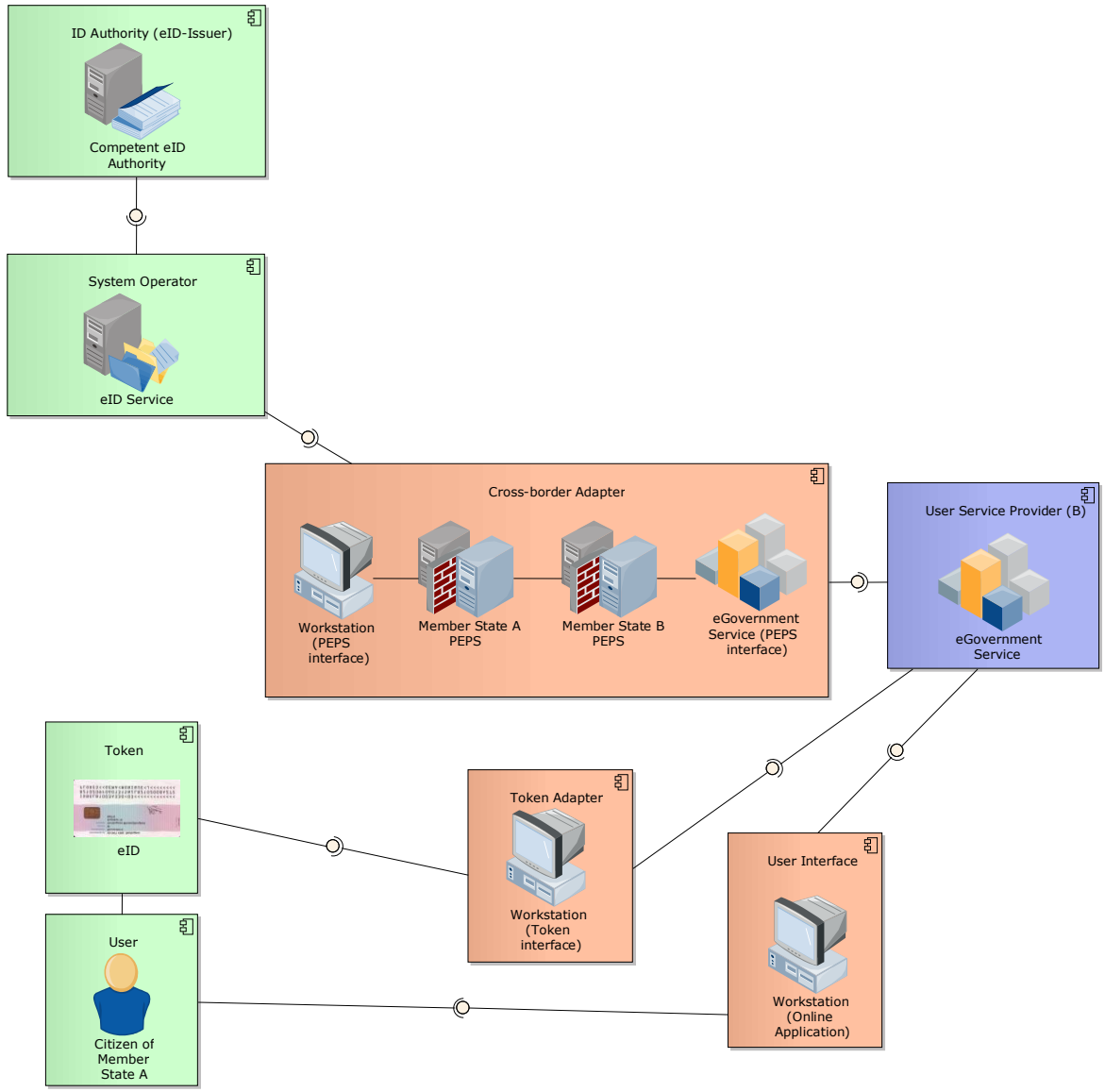


Figure 7: Mapping of STORK components to the generic model

The citizen of Member State B who requests an eGovernment service from Member State A is the generic model's user. This online service is in accordance with Service Directive 2006/123/EC on services in the internal market [3]. Such a service can require electronic authentication utilizing a citizen's eID. The eID (ie, the electronic ID document in this case) acts as the generic model's token. Depending on the issuing Member State, the eID is equipped with specific security features. It is subject to the relevant laws of the issuing state.

The citizen's workstation showing the online application represents the user interface and, as far as interfacing the eID is concerned, the token adapter. The part of the workstation that interfaces with the PEPS is considered a subcomponent of the generic cross-border adapter.

The eGovernment service corresponds to the user service provider in the generic model.

The generic model's cross-border adapter consists of:

- the workstation's PEPS interface
- the PEPS systems in both countries
- the PEPS interface with the eGovernment Service
- the PEPS interface with the eID service.

The eID service, which is responsible for processing the requests from the PEPS system, maps to the generic model's system operator.

The competent eID authority maps to the generic identity authority. While this may often be a civil register, the organization representing the competent eID authority is defined by the type of eID selected for authentication.

4.2.4 Protection requirements

STORK is at an intermediate stage. The first deliverables are publicly available; these pertain to an interim report on the eID process flows [24], a scheme as to how Member States can classify their authentication processes to quality levels [23] and can map into each other [21], as well as a report on legal interoperability [22]. This case study is based on these documents and the STORK approach with local PEPS on a national level.

One of the major challenges of the STORK project is to develop a common framework for the mutual recognition of national electronic identities between participating Member States. Each Member States has its own eID solution for authentication. A common framework must ensure that the Member States recognize each other's solutions and must handle the different qualities and characteristics of each authentication scheme. Therefore a scheme of assurance levels was developed to be used among Member States. This scheme is called STORK QAA (quality authentication assurance). It supports four levels of authentication assurance and facilitates the mapping of authentication levels and eID solutions onto each other.

The following assets are taken from the mapping of the generic model to the STORK components. These assets must be considered as trustworthy in a cross-border electronic authentication.

4.2.4.1 Personal data

The identity of a person must be considered as an asset that must be highly protected. The protection of personal data must ensure the anonymity of the citizen as far as possible within the authentication process. In particular, the Data Protection Directive (95/46/EC), the right to informational self-determination and the national laws of Member State apply.

Personal data		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	Medium	A loss of confidentiality might have a significant negative effect on the reputation of the system and may violate the Data Protection Directive, the right to informational self-determination and the laws of Member States.
Integrity	Medium	The loss of the integrity of personal data may lead to fraudulent identities within legal transactions causing considerable financial loss or a significant impairment of the individual's right to informational self-determination[22].
Availability	Medium	Having personal data not available for longer than 24 hours may lead to considerable negative consequences for the citizen[23].
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has effect on social or financial standing		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Integrity: falsification of person-related data has effect on social or financial standing		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 23: Protection requirements for personal data

4.2.4.2 Application data

In order to process an authentication request, other information is transmitted. This data

[22] Depending on the nature of the application, the requirements for the confidentiality and integrity of the identity data will often be 'High', since they often contain or allow access to sensitive personal information (eg, financial or medical data).

[23] For example, by missing important deadlines

comprises the assertion exchanged by the PEPS systems, communication data during the electronic authentication and return codes.

Application data		**Personal data: no**
Protection requirements		**Rationale**
Confidentiality	Low	The impact of any loss of confidentiality is limited.
Integrity	Medium	The loss of integrity may lead to fraudulent or false authentications with severe impact on the citizen's social or financial standing.
Availability	Medium	Having the application data not available for longer than 24 hours may lead to considerable negative consequences for the citizen.
Major damage scenarios:		
Confidentiality: abuse of application data for non-system purposes		
Integrity: fraudulent use of system		
Integrity: impaired performance of duties due to false data		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		

Table 24: Protection requirements for application data

4.2.4.3 eID (token)

The eID contains personal data. This data is regarded as confidential and is secured by a large range of security features depending on the issuing Member State [9]. The eID is under the control of the citizen, and it is assumed that the citizen consents to having the data read during authentication.

This case study assumes that the eID is a national ID card or comparable document which does not contain personal data that is considered extremely critical with respect to its confidentiality (eg, a medical record possibly stating the holder has an HIV infection).

eID		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	Low	The eID is under the control of the user and the user consents to the data being read.
Integrity	Medium	The loss of the eID's integrity may lead to fraudulent identities causing financial damage and giving the system a negative reputation.
Availability	Low	Only has limited or no impact if the token is not available for several days.[24]

Table 25: Protection requirements for eID

4.2.4.4 Civil register (ID authority)

The ID authoriy is typically a civil register which establishes the person's identity on the basis of evidence such as a birth certificate or equivalent documentation. It issues the national ID card used for electronic authentication.

[24] This assumes that administrative procedures would eventually allow the identification of the citizen by other means.

ID authority		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	High	Disclosure of large amounts of the personal data of insured persons would cause significant, nation-wide loss of reputation.
Integrity	High	If the integrity of the registers is corrupted, severe liability issues may arise and trust in the system may be catastrophically compromised.
Availability	Medium	The acceptable downtime is up to 24 hours. Longer downtimes may impair the reputation and the performance of duties significantly.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has an effect on social or financial standing		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Integrity: falsification of person-related data has an effect on social or financial standing		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 26: Protection requirements for ID authority

4.2.4.5 eID service (system operator)

The eID service is responsible for processing authentication requests from the PEPS. The system interacts directly with the citizen (via the user interface) for validation of his or her identity. This interaction is specific to the Member State concerned.

This eID Service validates the authentication request and has access to all the personal data of the citizens concerned (eg, to a civil register). A large scale abuse of personal data is a potential risk and the confidentiality and integrity of personal data must be highly protected. Only correct data allows the proper functioning of the system and ensures the confidence of and acceptance by citizens. The availability of this system must be at least at the same level as the PEPS in order to allow the processing of requests for authentication.

eID service		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	High	A loss of confidentiality may allow large-scale abuse of personal data. This might have a catastrophic negative effect on the reputation of the system.
Integrity	High	Large-scale loss of integrity may render the entire eID service inoperable for a prolonged duration.
Availability	Medium	The acceptable downtime is up to 24 hours. Longer downtime may impair the reputation and the performance of duties significantly.

Table 27: Protection requirements for the eID service

4.2.4.6 Workstation (token adapter)

The token adapter is the additional hardware and software in the end user's workstation that implements the physical and logical aspects of communicating with the eID. For example, this might be a smart card reader and the appropriate software.

Workstation (token adapter)		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	Medium	Due to the Data Protection Directive and the laws of Member States, any personal data is restricted in usage and distribution.
Integrity	Low	Impact of any loss of integrity is limited and calculable.
Availability	Low	Only has limited or no impact if system is not available for several days.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		

Table 28: Protection requirements for workstation (token adapter)

4.2.4.7 eGovernment service (user service provider)

The IT systems of the eGovernment service are necessary for providing the online services. These IT systems process application data as well as personal data. This data is

received from the PEPS in the form of an assertion.

eGovernment service		**Personal data: yes**
Protection requirements		**Rationale**
Confidentiality	High	A loss of confidentiality may allow large-scale abuse of personal data. This might have a significant negative effect on the reputation of the system.
Integrity	Medium	The loss of integrity may lead to fraudulent transactions and violation of Member State laws.
Availability	Medium[25]	The acceptable downtime is up to 24 hours. Longer downtime may impair the reputation and the performance of duties significantly.

Table 29: Protection requirements for eGovernment service

4.2.4.8 Member State PEPS (cross-border adapter)

The national Member State PEPS are the central component in establishing cross-border electronic authentication. For handling an authentication request, two instances of a Member State PEPS are required, one from each state participating in the authentication. It is assumed that the PEPS are considered to be the services described in IDABC *Common specifications for eID interoperability in the eGovernment context* [20]. From the European perspective, the Member State PEPS is regarded as the local PEPS. Each Member State PEPS is governed by its related national laws.

The Member State PEPS concentrates the authentication requests at a national level and forwards them to the target Member State PEPS. Therefore, the communication between the PEPS systems should be secured by using SSL/TLS connections. The exchange of personal data and authentication data and assertions should use the SAML format [7]. Based on this format, the assertion can be validated and, if necessary, converted by the PEPS.

These systems must fulfil the highest requirements for protection. They process personal and application data. The availability of the cross-border electronic authentication service of a Member State depends on the availability of the local PEPS.

[25] *Depending on the specific eGovernment service, this may differ.*

Member State PEPS		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	High	Large-scale unlawful disclosure of the personal data of European citizens may lead to a Europe-wide loss of reputation and confidence in the whole system.
Integrity	High	Loss of integrity allows large-scale false authentications and fraudulent transactions. This may render the Member State PEPS and, by corollary, all cross-border transactions of the Member State's eID services and eGovernment services inoperable.
Availability	Medium	The acceptable downtime is up to 24 hours. Longer downtime may impair the reputation and the performance of duties significantly.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has effect on social or financial standing		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Integrity: falsification of person-related data has effect on social or financial standing		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 30: Protection requirements for PEPS

4.2.4.9 Workstation (PEPS interface)

The interface between the workstation and the PEPS system is considered to be part of the generic model's cross-border adapter. It is used to communicate both with the PEPS of Member State A and with the PEPS of Member State B. It is realized using web technology. This interface serves to discover the eID country of origin from the PEPS of Member State B and to provide credentials to the eID Service via the PEPS of Member State A.

Workstation PEPS interface		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	High	Due to the Data Protection Directive and the laws of Member States, any personal data is restricted in usage and distribution.
Integrity	High	The loss of integrity may lead to identity theft causing potentially considerable effects on the social or financial standing of the citizen.
Availability	High	The acceptable downtime is up to 24 hours. Longer downtime may impair the reputation and the performance of duties significantly.
Major damage scenarios:		
Integrity: impaired performance of duties due to false data		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		

Table 31: Protection requirements for workstation PEPS interface

4.2.4.10 eGovernment service (PEPS interface)

The interface between the eGovernment service and the PEPS is considered to be part of the cross-border adapter. The interface links the eGovernment service with the PEPS of Member State B. It is used to transfer the request for authentication to the PEPS of Member State B and to receive the assertion from the PEPS of Member State A.

eGovernment service (PEPS interface)		Personal data: yes
Protection requirements		**Rationale**
Confidentiality	High	Large scale unlawful disclosure of citizens' personal data may lead to national loss of reputation and confidence in the whole system.
Integrity	High	Loss of integrity allows large-scale false authentications and fraudulent transactions. This may render the eGovernment services inoperable.
Availability	High	The acceptable downtime is up to 24 hours. Longer downtime may impair the reputation and the performance of duties significantly.
Major damage scenarios:		
Confidentiality: abuse of personal data for non-system purposes		
Confidentiality: misuse of person-related data has effect on social or financial standing		
Integrity: identity theft		
Integrity: impaired performance of duties due to false data		
Integrity: falsification of person-related data has effect on social on financial standing		
Availability: impaired performance of duties		
Availability: increased cost of performance of duties		
Availability: unavailability of service has effects on social or financial standing of individual		

Table 32: Protection requirements for eGovernment service (PEPS interface)

4.2.5 Conclusive risk assessment

By providing quality levels for the authentication of the eIDs of each Member State, STORK lays a foundation for the mutual assessment of trust and security by Member States that wish to establish cross-border authentication. The eGovernment service only needs to decide upon the required level of authentication in order to see which eID from which Member State can satisfy the demand. Provided Member States support authentication via STORK with a number of available eIDs, this may lead fairly quickly to a large number of interoperable eGovernment services that can be used freely by European citizens.

4.2.5.1 Linkage between the eID and the holder

The misuse of eIDs in eGovernment services might have serious consequences for their holders. Hence, it is essential to ensure that the token can only used within the authentication process by the rightful holder. To this end, various mechanisms for

presenting credentials are in place.

The STORK project supports different types of credentials within the electronic authentication process. They range from username/passwords over TAN lists to qualified hard certificates with PINs. The username/password credentials are the weakest credentials; they might easily be compromised by guessing, social engineering and replay attacks.

4.2.5.2 End-user workstations

One of the most vulnerable entities is the end-user's workstation. A broad range of attacks can compromise a workstation's integrity and can lead to severe damages to the end-user.

To mitigate these risks, the user should be recommended to protect the workstation with free or commercially available security software packages. Mechanisms should be used to protect the integrity of any software (eg, Java applets or ActiveX components) which is provided to the workstation by STORK, the PEPS and the eID Service.

It should be noted that the workstation is under the control of the user and can be intentionally misused to compromise and abuse data or to attack other systems (eg, with denial of service attacks). To counter these risks, it is recommended that transactions and network traffic be monitored, specifically to record the user's IP address and to display it to the user as a deterrent.

5 Conclusion

To conclude the case studies, there are a number of core risks that must be addressed and countered by a successful and secure implementation of any electronic cross-border authentication process.

Data protection

Data privacy must be protected in any approach to electronic authentication, be it domestic or cross-border, because of the human right to informational self-determination as set forth in Article 8 of the European Convention on Human Rights [35] and interpreted in the Data Protection Directive. Each Member State implements this directive in its national law. The added challenge of a cross-border solution lies with the differences between different implementations by the participating states.

It is recommended that an approach on how to respect European and national data protection laws and regulations within any electronic cross-border authentication system be clarified at the earliest with a clear and explicit concept.

Legal framework

First and foremost, any cross-border activity is governed by the different laws and regulations of the participating states. These laws often prohibit either specific transactions or data exchanges. In particular, data protection laws may limit the processing and distribution of person-related data to the point where an efficient and effective cross-border transaction may not seem possible at all. Here the approach should be to respect the restrictive law and find a technical solution that is satisfactory.

To develop a successful cross-border interface between national IT systems, it is recommended that the legal requirements and restrictions be targeted as early as possible. This is necessary, since states must be able to initiate necessary adjustments to laws and regulations, and because a promising system design must reflect the requirements and restrictions.

Credentials of the user

Any electronic cross-border authentication process bears the risk of identity theft. Without a trustworthy authority (eg, a civil servant) to establish that the user's identity matches that of the eID token, another approach must be used to make sure that the eID token is used by its rightful holder and that the request for authentication is really in accordance with the will of that holder.

To this end, some credentials should be presented by the user. In principle, there are a number of options to implement such a mechanism:

- The eID token allows access only after the user presents his credentials to it (eg, by sending a PIN to a smart card for authentication).
- Biometric features of the user are captured and verified either by the eID token or by the system operator.

- The user has to present credentials to the system operator via the online connection.
- In cases where a properly authorized operator interacts with the user, this operator may manually validate the user's identity and vouch for it to the system.

All of these mechanisms have specific advantages and disadvantages, so that the optimal mechanism depends on the security demands of the specific application. As a general rule, one can say that the more severe the consequences of identity theft or abuse could be, the more important is strong user authentication. For applications where identity theft may be critical to the user, credentials should consist of a combination of possession (of the eID token) and knowledge (of a PIN or password), possibly enhanced by the use of biometric verification.

An added challenge in cross-border authentication lies in national differences in the selection and implementation of user credentials and in the resulting different levels of reliability.

Authenticating system participants

The foremost obligation of cross-border authentication is mutually establishing the identities of the user and the user service provider beyond any reasonable doubt. To this end, a chain of trust must be established through all participants in the cross-border authentication process. Such a chain of trust is feasible, but obviously the complexity of any solution increases with the number of entities involved in this chain.

The system operator faces the difficulty of establishing sufficient trust in the identity of a user service provider across borders. The same problem presents itself to the user service provider with respect to the authenticity of a system operator. The approach of using a national portal as a 'trusted third party', that vouches for the participant's identity (as used in STORK and NETC@RDS), is practical and in principle sound. Nevertheless it raises issues of liability with respect to the national portals.

Also, there remains the question of the reliability and confidence with which a national portal authenticates its participants. This is entirely in the domain of the relevant Member State, so that varying levels of confidence and security may be expected throughout the European Community. For each participant, this poses the problem of evaluating each national solution with respect to the confidence that can be placed in the strength of its registration and authentication mechanisms.

A common IT security policy for all participants in the cross-border exchange may be a remedy to this, since then a defined and common level of security could be assumed by any participant.

Securing online connections

While establishing a secure online connection poses no technological problem today and while there are a number of viable and proven solutions available, it is still necessary for any cross-border system to ensure secure communications.

As seen in the case studies, there are different approaches. These either rely on secured

publicly-accessible internet connections or they integrate with dedicated secure cross-border networks. However, each approach must ensure the confidentiality and integrity of the data exchanged. Therefore authentication of the participants within the communication must be ensured, and the communication itself must be secured by sufficiently strong encryption.

Another aspect is the availability of these connections, which must be at least at the same level as the highest required availability of the participants.

Bridging technological differences

For many applications there will be different hereditary national systems in operation that use different and incompatible technologies. At first view, this is purely a technology problem, which can be countered comparatively easy by proper engineering and – what is often more difficult to find – adequate funding. On second view, a multitude of security problems is raised, most of them resulting from combining systems with incompatible security policies and divergent levels of security for different components[26].

The need for a security policy

Even if the national systems are in principle compatible, the development of a security policy for (application-specific) electronic cross-border transactions is strongly recommended. This security policy must be agreed upon by participating states and may have an effect on their national laws and regulations. Only in this way will each participating state know exactly what security threats are to be countered at what component in the systems.

In view of the heterogenic nature of hereditary national systems, no assumptions may be made with respect to a common and obvious approach to IT security measures. People who are used to a specific technology and a corresponding security approach tend to assume that this approach is 'natural' and obvious.

[26] *For example, a system that is based on a magnetic stripe token will anchor security in the backend system, while a smart card system may use the token itself as the security anchor. Making these systems compatible requires a lot more than adding additional card reading devices.*

6 Glossary

actor	the initiator of an interaction
application	The different sets of functionalities of smartcards are called 'applications'.[27]
certificate	an electronic document that establishes a digital identity by combining the identity name or identifier with the public key of the identity, a validity period and an electronic signature of a third party
certificate authority	a trusted third party that issues digital certificates for use by other parties
EESSI	Electronic Exchange of Social Security Information
PEPS	pan-European proxy services
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.
scenario	a description of a use-case within a given situation, describing the distribution and interaction of the tasks between the participating components
situation	the combination of circumstances at a given moment
STORK QAA level	STORK quality authentication assurance levels are four levels of authentication assurance that facilitate the mapping of national authentication levels and eID solutions onto each other
use-case	a description of the interaction between a primary actor and the system itself, represented as a sequence of simple steps

[27] Rankl, Wolfgang; Effing, Wolfgang: *Handbuch der Chipkarten*, Carl Hanser Verlag , ISBN: 3-446-22036-4; English translation: *Smard Card Handbook*, John Wiley & Sons, ISBN: 0-470-85668-8

7 References

Any references that are not explicitly cited within the report have been used as background information, but cannot be pinpointed easily to a specific text passage.

[1] European Union: Directive 1995/46/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
[2] European Union: Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications
[3] European Union: Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market
[4] European Union: Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems
[5] European Union: Administrative Commission of the European Communities on Social Security for Migrant Workers – Decision No 189 of 18 June 2003
[6] European Union: Administrative Commission of the European Communities on Social Security for Migrant Workers – Decision No 190 of 18 June 2003
[7] ENISA, 2008: *Mapping IDABC Authentication Assurance Levels to SAML v2.0 – Gap analysis and recommendations*
[8] ENISA, 2009: *Report on the state of pan-European eIDM initiatives*
[9] ENISA, 2009: *Privacy Features of European eID Card Specifications*
[10] ICAO: DOC 9303 Part 1 Volume 1, *Passports with Machine Readable Data Stored in Optical Character Recognition Format*
[11] ICAO: DOC 9303 Part 1 Volume 2, *Specifications for Electronically Enabled Passports with Biometric Identification Capability*
[12] ICAO: *PKD Regulations for the ICAO Public Key Directory*
[13] ICAO: *Memorandum of Understanding regarding Participation and Cost Sharing in the electronic Machine Readable Travel Documents ICAO Public Key Directory (ICAO PKD)*
[14] ICAO: *PKD Procedures for the ICAO Public Key Directory*
[15] ICAO: *ICAO PKD Terms and Conditions*
[16] Hartmann, Körting, Käthler, 2009: *A Primer on the ICAO Public Key Directory*
[17] Bundesamt für Sicherheit in der Informationstechnik: *BSI Standard 100-1 Infomation Security Management Systems (ISMS)*
[18] Bundesamt für Sicherheit in der Informationstechnik: *BSI Standard 100-2 IT-Grundschutz Methodology*
[19] Bundesamt für Sicherheit in der Informationstechnik: *BSI Standard 100-3 Risk Analysis based on IT-Grundschutz*
[20] IDABC: *Common specifications for eID interoperability in the eGovernment context*, http://ec.europa.eu/idabc/en/document/6484/5938
[21] ICT-PSP STORK: D2.1 - *Framework Mapping of Technical/Organisational Issues to a Quality Scheme*, http://www.eid-stork.eu/index.php?option=com_processes&Itemid=60&act=streamDocument&did=579
[22] ICT-PSP STORK: D2.2 – *Report on Legal Interoperability*, http://www.eid-stork.eu/index.php?option=com_processes&Itemid=60&act=streamDocument&did=578

[23] ICT-PSP STORK: D2.3 - *Quality authenticator scheme*, http://www.eid-stork.eu/index.php?option=com_processes&Itemid=60&act=streamDocument&did=577
[24] ICT-PSP STORK: D4.1 *Interim Report on eID Process Flows*, http://www.eid-stork.eu/index.php?option=com_processes&Itemid=60&act=streamDocument&did=576
[25] CEN: CWA 15974:2009 (E) *Interoperability of the electronic European Health Insurance Cards* (WS/eEHIC)
[26] Marjan Sušelj, Roberto Zuffada, 2005: *Netc@rds for e-EHIC - a Step towards the Introduction of the European Health Insurance Card*
[27] ISO/IEC 27002 *Information technology - Security techniques - Code of practice for information security management*
[28] NETC@RDS: Web site http://www.netcards-project.com
[29] IDABC: EESSI (Electronic Exchange of Social Security Information) website, http://ec.europa.eu/idabc/en/document/7189/
[30] European Union: Council Regulation (EC) No 1408/71 of 14 June 1971 on the application of social security schemes to employed persons, to self-employed persons and to members of their families moving within the Community
[31] European Community: Decision No. 189 of 18 June 2003 of the Administrative Commission of the European Communities on Social Security for Migrant Workers
[32] HPRO Card: Website http://hprocard.eu
[33] STORK: Website http://www.eid-stork.eu/
[34] ICAO: ICAO PKD Interface Specifications
[35] Council of Europe: *The European Convention on Human Rights and its five Protocols*, Rome 4 November 1950