



HJP CONSULTING.

Study commissioned by ENISA




ENISA Study:
“Risk assessment on security issues
of cross-border electronic authentication”
Summary

HJP Consulting GmbH, Markus Hartmann
for Security Document World Conference, London
10 February 2010





We are Smart Card Architects

Our services

-  We plan
-  We procure
-  We approve

We focus on eHealth and eID systems

-  Consultancy and project management
-  Specification, testing and GlobalTester tools

Worldwide references

-  Europe: Germany, UK, France, Switzerland ...
-  Middle East: U.A.E, Saudi Arabia, Sudan ...



ENISA: European Network and Information Security Agency

- Agency set up by EU
- Created in 2004
- Based in Heraklion, Greece
- Mission:
Securing Europe's
Information Society by acting
as a pacemaker for network
and information security
- Authors of this study:
 - Slawomir Górnaiak, ENISA
 - Dr. Ingo Naumann, ENISA
 - Dirk Hartmann, HJP
 - Stephan Körting, HJP
- Published on 3 Feb 2010



Security Issues in Cross-border Electronic Authentication





Introduction



Introduction

- Over the past decade, European Member States and EEA countries have gradually rolled out identity management solutions that were best suited to their national goals and ambitions
- The goals of such initiatives were uniformly the same:
 - improving administrative efficiency
 - improving accessibility and user-friendliness
 - reduction of costs
- At the European level, these goals could be advanced by improving the interoperability of electronic identification/authentication solutions being offered at the national level.



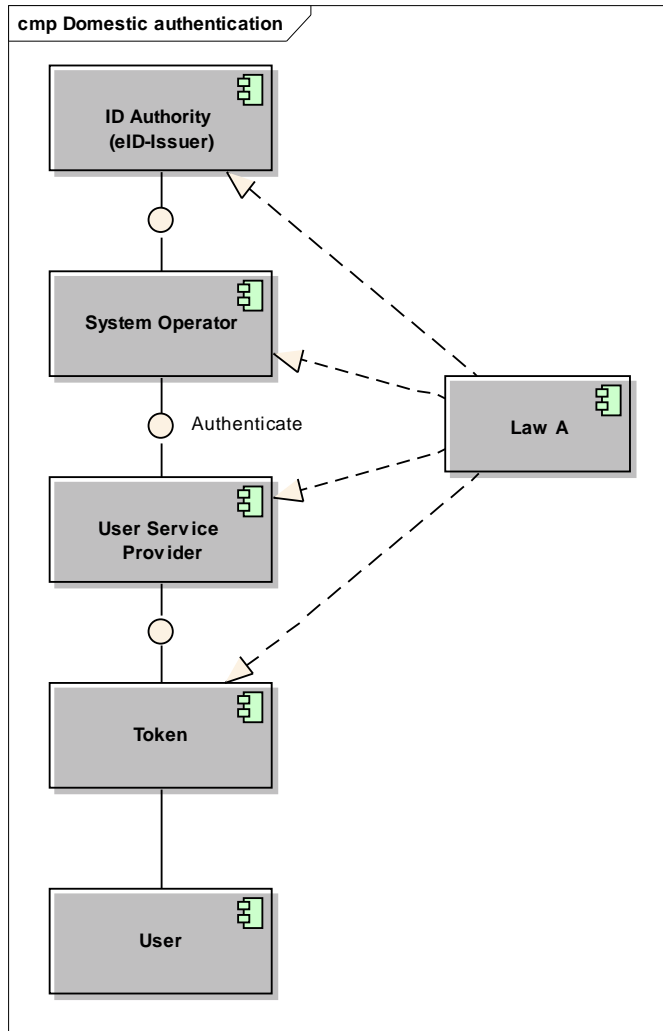
Unified eID Management

- One of the considerations for a more unified eID management vision is the issue of security and trustworthiness
- Considerable efforts have been made in several projects to face the challenges of pan-European interoperability of electronic authentication and to answer the question of the feasibility of different approaches
- There are significant differences between the security and trustworthiness of eIDs used in different Member States
- The generic technical models between domestic and cross-border authentication differ fundamentally!



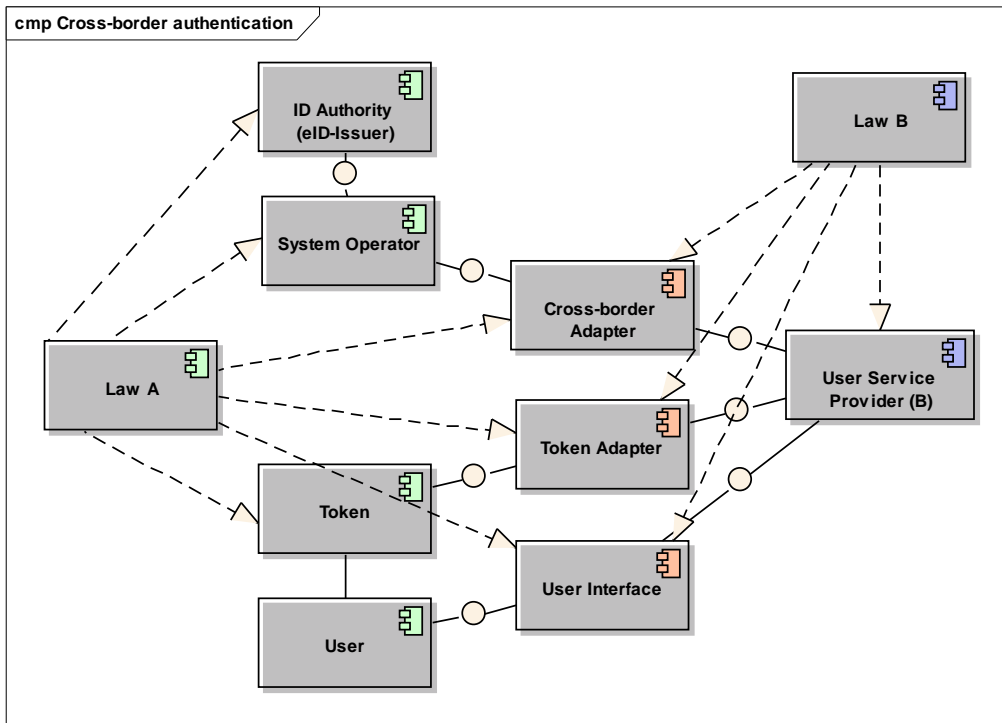
The Generic Technical Models and Challenges

Generic Domestic Electronic Authentication



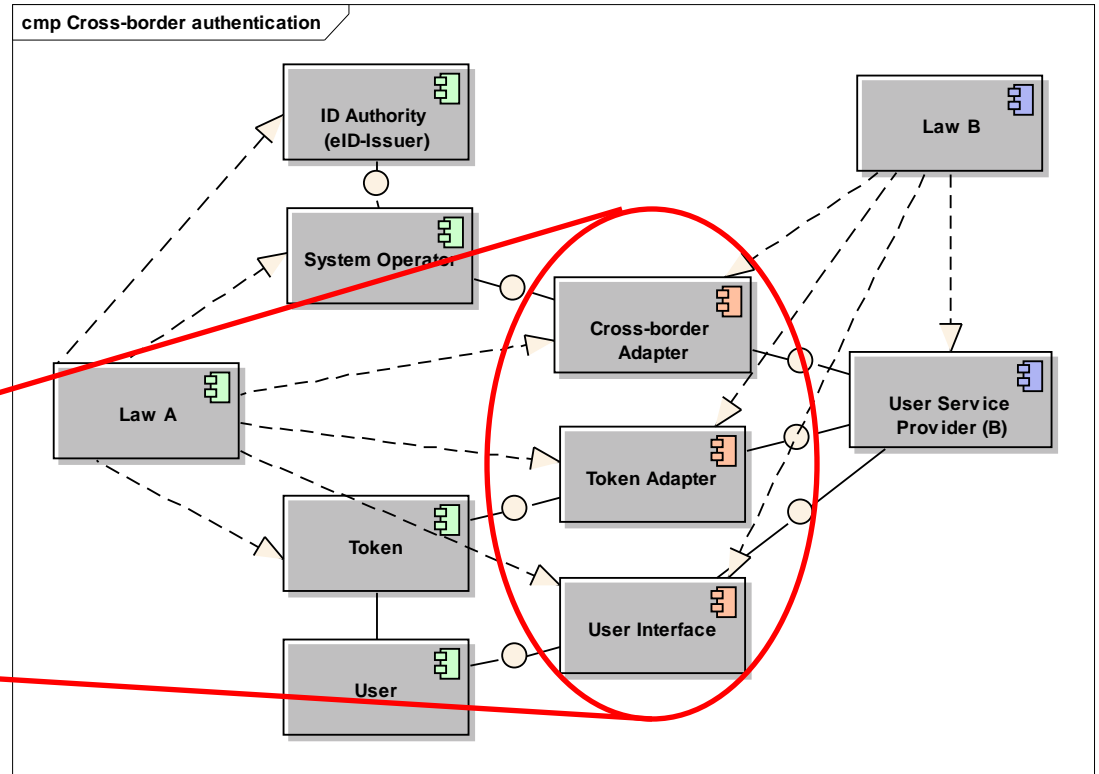
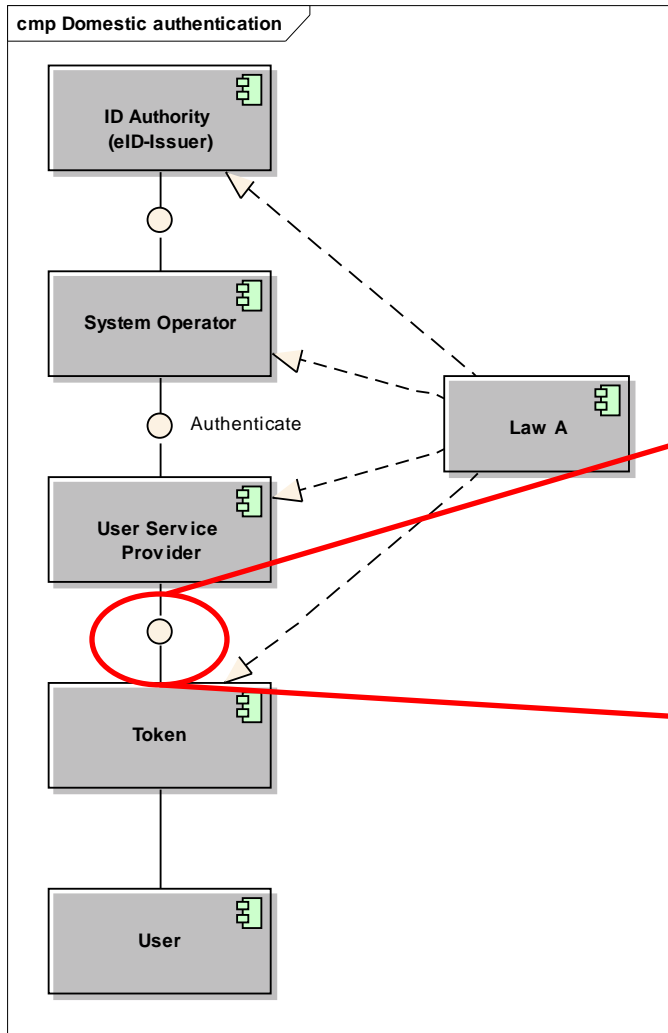
- The **ID Authority** issues a eID (**Token**) e.g. a smart card (health insurance card or a national ID card), representing the User's identity
- The **System Operator** (e. g. a health insurance company, civil registration office). Operates the eID system and realizes any authentication processes
- The **User Service Provider** (e. g. a doctor or a vehicle registration office) interacts with the user and the user's token and providing a service that is linked to the application operated by the system operator.
- The system, its participants, components and processes are governed by the same set of laws, regulations (**Law A**)

Generic Cross-Border Electronic Authentication



- The big difference is that the fact that the **User Service Provider (B)** is actually the user service provider from another system, who is governed by different laws (**Law B**)
- The **Cross-Border Adapter** proxies an electronic authentication request from the local service provider (B) across the border between countries and systems to the system operator.
- The **Token Adapter**'s main task is interfacing a token from one country with the user service provider from another country.

Differences between national and cross-border e-authentication





Challenges of Cross-Border Authentication (I/II)

- There may be different types of credentials which links the user's identity to a token
- The reliability of the credentials may differ
- A wide range of different tokens appears:
 - Electronic and non-electronic tokens with different security levels
 - Tokens with different validities
 - Tokens from previous and/or related systems
 - Tokens which bear different datasets
 - Tokens issued by different system operators or on behalf of the government

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.



Challenges of Cross-Border Authentication (II/II)

- Different technical infrastructure and equipment are in use
- Different authentication protocols and procedures are in place
- Different sets of personal data coming from different countries
- Acceptance and trust of personal data coming from a foreign country
- Manually checking the authenticity of a foreign token
- Checking the authorization of a foreign User Service Provider



The Risk Assessment



Risk Assessment Methodology

- International standards on evaluating information security and information security management systems are found in the ISO standards of the ISO 2700x family
- 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
- These standards are compatible to the ISO 2700x standards with the added advantage of:
 - Practicability
 - more detailed instructions on how to evaluate security issues
 - how to set up an appropriate system of security management and security measures



Risk Assessment Approach – Assets

- Core of any security evaluation according to BSI 100-2 “IT-Grundschutz Methodology” is the definition of assets that must be protected
- “Assets” refers to all the protection-worthy data as well as to the systems which process, store and transport this data
- Each asset is considered against the three basic protection values confidentiality, integrity and availability:

Basic Protection Values according to ISO/IEC 27002	
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

Risk Assessment Approach – Protection Requirements

- Each asset is assigned a protection requirement according to the basic protection values as defined in BSI 100-2 categories:

Protection Requirements Categories		
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.

In 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

- Assigning protection requirements to an asset, potential 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, i.e. the impairment of reputation and confidence
- Financial consequences

Risk Assessment Approach – Example

- For each asset the results of this analysis is collated in a single table as the following:

Object name		Personal data: (<u>yes</u> /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		

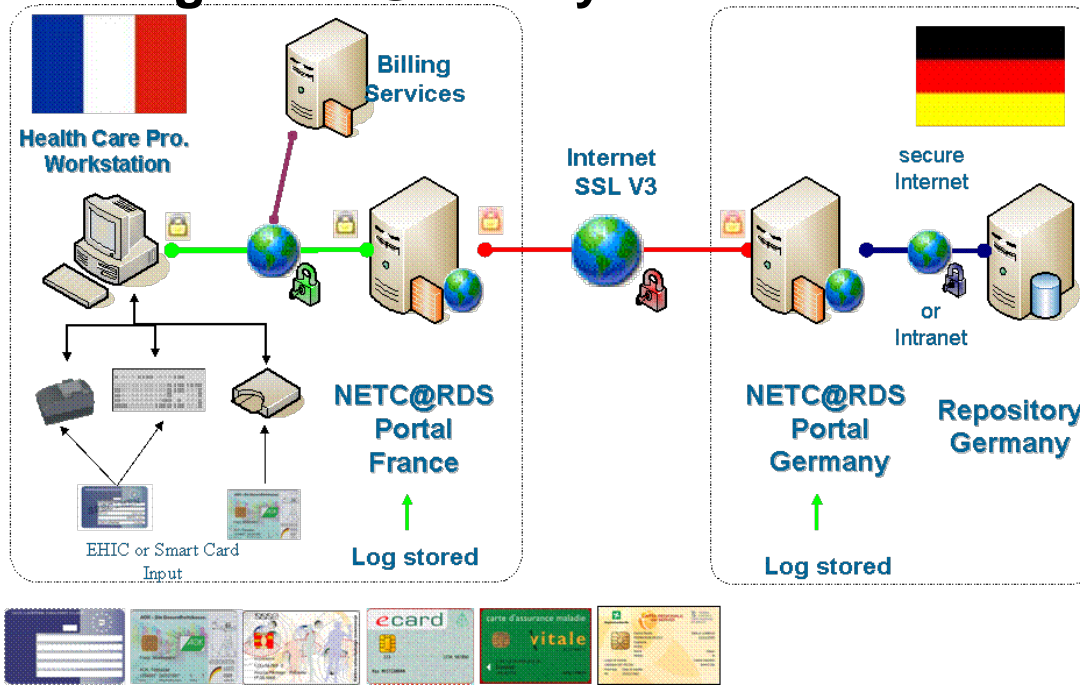


The Projects

NETC@RDS for eEHIC ID

- The NETC@RDS project 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
- The project consists of the NETC@RDS Consortium, which includes stakeholders from 15 European countries and is co-founded by the EU
- Started in September 2002 and is currently in the implementation phase (since June 2007)
- A preceding evaluation phase tested 85 pilots successfully across 10 EU Member States and establishing the first existing pan European eHealth connection
- The implantation phase will encompass 500 health care service points in 260 service units in 16 EU/EFTA Member states and Switzerland

How the existing NETC@RDS system works

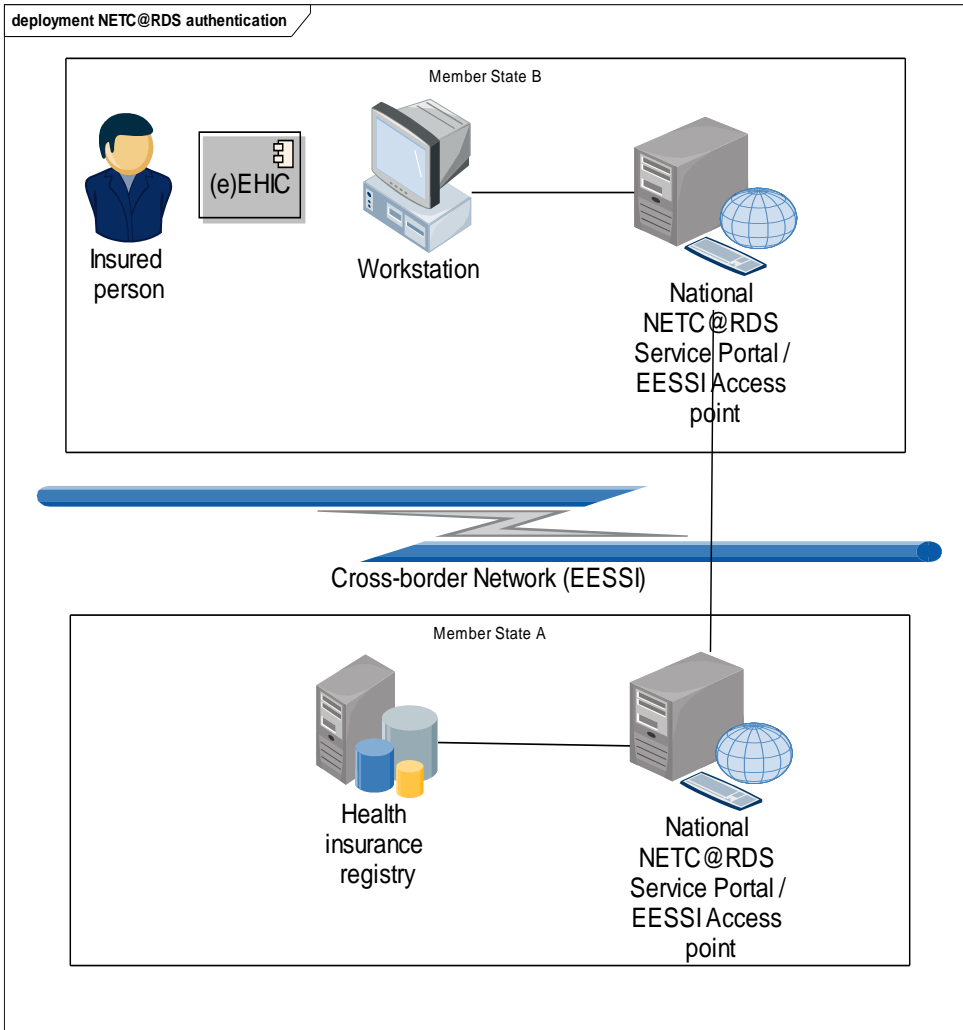


- A cross-border mutual authentication is established every time a NETC@RDS user (typically a hospital clerk or a health practitioner) operates an online verification of the e-EHIC dataset as entitlement to receive health care abroad in one of the NETC@RDS service units/points
- The technical architecture consists of secure network connections within a Member state and between the Member states, linking national service portals and registries in each country with workstations within all service facilities

Usage Scenario

- (1) A French citizen is on vacation in Germany and needs to use unplanned healthcare services, i.e. the visitor goes to a German doctor because of sickness or maternity
- (2) 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
- (3) The card, containing the eEHIC dataset, is read by a smart card reader connected to the front desk workstation
- (4) This workstation connects to the national German NETC@RDS Service Portal via online connection and tries to verify the dataset
- (5) 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
- (6) 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

How the NETC@RDS system will work in the future



- The EESSI project (formerly PROTECTUS) will allow the pan-European electronic exchange of data regarding social security between Member States
- With the introduction of the EESSI (Electronic Exchange of Social Security Information) service network, which will connect institutions at a European level through a central node, it is planned to establish the connection between the national service portals via the EESSI



Identified Major Security Issues (I/II)

■ Authenticity of the eEHIC

- The e-EHIC does not necessarily authenticate itself ! This by design due to the necessity to support all kinds of EHIC technologies
- This may lead to
 - fraudulent use of copied eEHICs to receive health care services
 - play-back attacks where a health care provider uses eEHIC data sets to create fake incidents that are billed to the health insurance companies

■ Authenticating Health Professionals

- The HPRO CARD project has established a working group in 2007, but it may be expected to take several years before the HPRO CARD will be in widespread use in Europe in the form of an electronic smart card with strong authentication
- This leads to difficulties in establishing sufficient trust in the identity of a health professional or a health care institution across borders



Identified Major Security Issues (II/II)

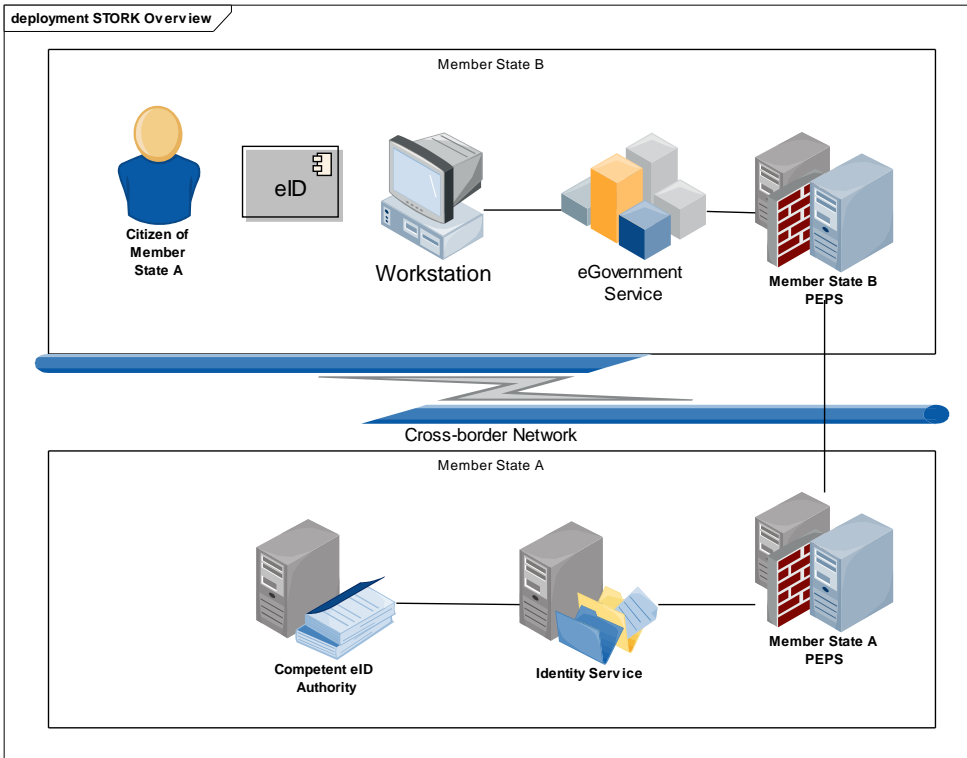
- **Entrusting personal data to an institution that is not governed by the same set of laws and not by the same regulations on data protection**
 - The health insurance companies will not have direct contractual (non-disclosure) agreements with each health care provider in another European country
 - This may lead to disclosure of personal data of insured persons in and may cause severe damage to the public trust in the national health insurance system



STORK **(Secure idenTity acrOss boRders linKed)**

- The STORK project develops rules and specifications to assist mutual recognition of eID, taking into account existing infrastructures and specifications
- STORK runs under the ICT Policy Support Programme of the Competitiveness and Innovation Framework Programme (CIP). As of mid 2009 there are 14 States and a total of 29 consortium partners composed of public and private sector organisations participating in the project
- Started in June 2008 and will run for three years
- Pilot applications will be realized, implementing and utilizing cross border authentication in real life environments
- Pilot 1 shall demonstrate the operation of cross-border electronic authentication in several Member States
- Interacts with other European eID projects to maximize the field of applications.

Usage Scenario



- (1) A Spanish citizen stays in Belgium and starts using a Belgian eGovernment service (e. g. for registering the change of his address in Belgium) via his workstation
- (2) The selected eGovernment service requests an authentication of the citizen’s identity and offers an option for authentication of non Belgians
- (3) The eGovernment service sends a request for authentication with the required level to the Belgian PEPS
- (4) This offers the Spanish citizen a list of qualified Member States which support the required electronic authentication
- (5) After the citizen selects “Spain” the Belgian PEPS sends the request for authentication to Spanish PEPS



Identified Major Security Issues (I/II)

■ Linkage between the eID and the holder

- It is essential to ensure that the token can only be used by the rightful holder within the authentication process
- The STORK project supports different types of credentials within the electronic authentication process. They range from Username/Password over TAN lists to qualified hard certificates with PIN
- The Username/Password credentials are the weakest credentials: they might be easily compromised by guessing, social engineering and replay attacks



Identified Major Security Issues (II/II)

■ End User Workstations

- A broad range of attacks can compromise a workstation's integrity
- The misuse of eIDs in eGovernment services might have serious consequences to its holder
- On the other hand, the workstation is under the control of the user and can be intentionally misused to compromise and abuse data or to attack the other systems, e. g. with denial of service attacks



Conclusion



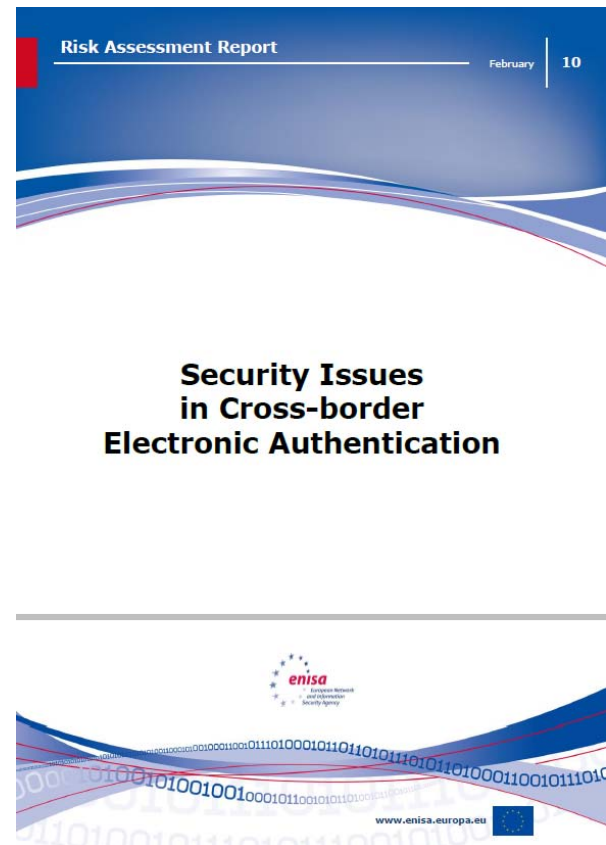
Critical Success Factors for the Security of Electronic Cross-border Authentication

- Establishing the legal and contractual framework
- Identifying the citizen through credentials
- Securing online connections
- Bridging technological differences
- Establishing and agreeing on a common security policy



The study is now online available:

<http://www.enisa.europa.eu/act/it/eid>





Questions?

HJP Consulting GmbH

Markus Hartmann

Hauptstraße 35

33178 Borcheln, Germany

tel: +49-5251 - 41 77 610

fax: +49-5251 - 41 77 666

e-mail: markus.hartmann@hjp-consulting.com

web: www.hjp-consulting.com

For contacting ENISA or for enquiries on this study, please use the following details:

Email: eid@enisa.europa.eu

Internet: <http://www.enisa.europa.eu/act/it/eid>

