Using the NETC@RDS Approach as a Basis for Cross-Border Electronic Authentication

George Pangalos, Noel Nader, Ioannis Pagkalos

Using the NETC@RDS Approach as a Basis for Cross-Border Electronic Authentication

I. Pagkalos[1], N. Nader[2], G. Pangalos[3]

[1] Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki
[2] Direction des Programmes, International Projects Coordinator, GIE SESAM-Vitale,France
[3] Informatics laboratory, General dept, Faculty of Technology, University of Thessaloniki,

[1]ipagkalo@auth.gr,
[2]Noel.Nader@sesam-vitale.fr,
[3]pangalos@auth.gr

Abstract. Many countries, European and worldwide, have increasingly issued during the last decade electronically readable identity documents to their citizens, for different purposes and applications. However, a major characteristic of all these systems is that they are basically available in a national context. For example, European citizens that move freely through the Member-States face the problem that their eIDs from their home state do not allow access to services of another Member-State in which they are temporarily present. Public Administrations are also unable to provide services to European citizens from other Member-States with the same ease and efficiency as they do to their national citizens. In order to avoid such confusing situations, cross-border services should be fully integrated in the national/regional and local information systems. It is, therefore, an important task to improve the cross-border interoperability of electronic identification and authentication systems. ENISA, the European agency for the security of computer systems and networks, recently published a report dealing with an important aspect of this problem: the security issues in cross-border electronic authentication. The report assesses the risks of electronic authentication in cross-border solutions and provides a generic implementation model. This paper describes an implementation methodology for addressing the cross-border interoperability of electronic authentication problem, based on the ENISA generic model. The proposed implementation methodology has been based on the successful NETC@RDS project approach and experience, described herein. This methodology can provide a suitable secure cross-border, multi-purpose authentication implementation based on the aforementioned generic model that can be used in various sectors.

Keywords: Electronic authentication, cross border authentication, security.

adfa, p. 1, 2011.

1 Introduction

Many countries increasingly offer citizens electronic access to their services [1,2,3]. These e-services often use electronic authentication (eID) and are usually implemented at a national level with specific technologies, specific security concepts and specific business logic. As a result, in most cases these systems can only be accessed from within the Member-State and by citizens of that state.

For example, during the last decade, several E.U. Member-States (France, Belgium, Germany, Austria, Italian regions, Slovenia and others) have distributed more than 200 million of health insurance smart cards to the population as evidence of entitlement for health care access and/or reimbursement at national level. A major characteristic of all these systems is that they are basically available in the national context. One reason for this is that citizen identification (like social and health insurance benefits) is usually related to services regulated at national or regional level. Existing solutions were, therefore, designed to be most efficient and fitting with respect to national requirements and infrastructures. Despite that, the goals of these systems are, in general, identical for all Member-State: managing identities, improving administrative efficiency, improving accessibility and user-friendliness, reducing abuse and fraud and reduction of costs.

Today, this may represent an undue restriction on the usage of these services to European citizens that move freely through all Member-States. This can lead to serious inequalities since, for example, health professionals might be reluctant to apply for cross-border benefits-in-kind procedures and, as a consequence, European patients might have to pay the bill for medical care delivered abroad themselves. Therefore, there is a need to extend these services beyond the national borders and beyond the user group of national citizens. At the same time, the European and national security and data protection laws and regulations must be respected and should not be undermined by any cross-border distribution of personal data.

Logically, the implementation of secure cross-border services, or the extension of a domestic system across borders, poses several challenges in the legal, organizational, security, semantic, socio-economic, and technical level.

An obvious technical challenge may be, for example, the fact that disparate IT systems with different technologies must be interfaced. Any problems rising from this are usually limited to designing a proper technical and financially affordable solution. Differences in the business logic of the national solutions are more difficult though. Health care and educational systems in particular differ greatly in the way that services are provided, evaluated and billed. Setting up a business or dealing with taxes is also very different from one State to another. 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.

Another major prerequisite of any such e-government or e-health service is the trust in the authenticity of all participants and the provided data. Since most services of this type handle confidential data, the confidentiality must also be protected in a cross-border scenario. Some services also require a high availability if the citizen is

not to suffer undue consequences. This establishes the need to discuss, evaluate and implement IT security in such cross-border applications.

ENISA, the European agency for the security of computer systems and networks, recently published an interesting report dealing with an important aspect of this problem: the security issues in cross-border electronic authentication. More specifically, the report assesses the risks of electronic authentication in cross-border solutions and provides a generic implementation model [1].

This paper describes a possible implementation methodology for addressing this cross-border interoperability of electronic authentication problem, based on the ENISA report. The proposed implementation methodology has been based on the successful approach of the NETC@RDS[1] project and past experience in secure cross-border electronic authentication [2].

2 The ENISA generic models of domestic and cross-border electronic authentication

According to the ENISA report terminology [1], in any domestic 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 (e.g. 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 (e.g. a health insurance card or a national ID card) to the User that identifies the user as the person with a specific eID. The token may contain the eID and other data in electronically readable form. The User Service Provider (e.g. 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. 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 (figure 1).

The entire system, its participants, components and processes are governed by the same set of laws and regulations (Law A). These laws comprise the range from general regulations on the handling of personal data (e.g. 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 of tokens and electronic authentications is vast, the general principle is the same for all such systems. For example all such systems are homogenic with respect to technology, are governed by a single set of laws, and "know" all system participants, i.e. they are closed to non-participants.

[1] NETC@RDS service for the electronification of the European Health Insurance Card: a pan-European project supported by the EU's eTEN Program [2]

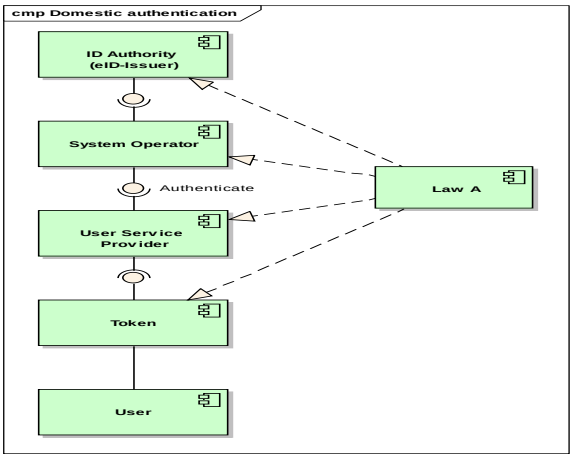

Fig. 1. The domestic ENISA electronic authentication scheme

When dealing with cross-border applications or utilizing a service with a token provided from outside the user service provider's state, the domestic model must be enhanced [1]. The notable difference to cross-border authentication as opposed to the domestic model is 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) and business rules. In addition, this 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 System Operator are different, which raises all kinds of problems, from data protection to liability and insurance issues (figure 2).

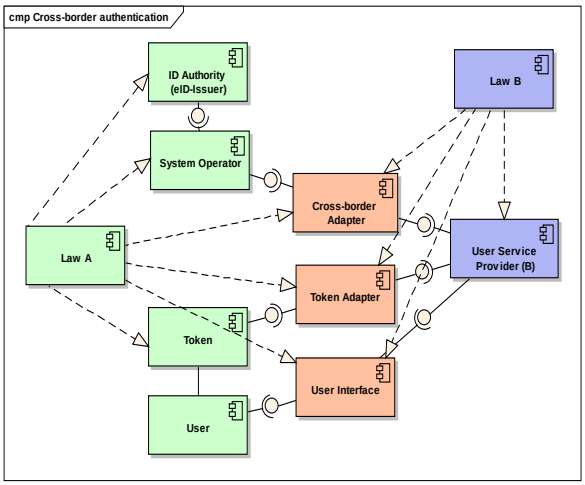

Fig. 2. The generic ENISA model of cross-border authentication

In order to achieve compatibility of the two systems to the point that a user of the first system may receive services from the second system, two adapter components must be introduced into the systems [1].

The first one is the 'Cross-Border Adapter' which 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. 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 second component is the 'Token Adapter' 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. Usually it may be considered to be an extension of the IT systems of the local service provider that is operated by him.

Comparing the ENISA generic model of a cross-border authentication system with the domestic system, some changes to the general principles of system design are evident which are relevant to any security evaluation. The cross-border system is heterogenic with respect to technology, is governed by two separate and at least partially disjoint sets of laws, and does not "know" all system participants, i.e. they are potentially open to non-participants.

Extending a domestic system to allow cross-border electronic authentication with a communication partner that is not native to the domestic system poses also a number of security challenges [1]. All of these challenges must be addressed and overcome to successfully implement cross-border interoperability. Examples include the different types of credentials that may link the user's identity to a token, the fact that the reliability of the credentials may differ, the wide range of different tokens used, the acceptance and trust of identity data coming from a foreign country, the authenticity check of a foreign token, and the authorization check of a foreign User Service Provider. Furthermore, the following important issues must also be taken into account:

Security Issues. International standards on evaluating information security and information security management systems can be found in various formats (e.g. the standards of the ISO 2700x family). However, these standards provide fundamental but often rather generic security requirements. According to the ENISA report, the core of any security evaluation (see also BSI 100-2 "IT-Grundschutz Methodology" [18]) is the definition of assets that must be protected and the protection requirements for these assets. Then each asset is assigned a protection requirement for the three basic protection values of confidentiality, integrity and availability.

Protection Requirements. The following assets are considered worthy of protection in the ENISA report [1]: Identity Data, Application Data, Token, IT systems of the system operator, User Service Provider, Cross-Border Adapter, Token Adapter and User Interface. It must be noted, however, that while they are discussed in the generic model, this can only be a starting point when it comes to the evaluation of a specific application. This is because the assessment of the protection requirements for each asset may differ greatly from application to application.

Other Technical and Legal Issues. Several other important technical and legal issues are also encountered when studying the ENISA generic model. For example [1]: the different types of credentials and their reliability, the tokens with different security levels that differ in their trustworthiness, the different technical infrastructures that elevate the amount of security vulnerabilities due to different security levels, the different authentication protocols and procedures that elevate the amount of security vulnerabilities due to different security levels and the attacks on the availability of the cross-border authentication process. Several legal problems also arise. For example, national restrictions on the transfer of identity data may differ, national regulations may prohibit authentication across borders, and the identity data may not be processed in an adequate, relevant and not excessive way to the purposes for which they are collected and/or further processed.

3 The NETC@RDS approach for implementing cross-border electronic authentication

3.1 The NETC@RDS project

NETC@RDS is a pan-European project supported by the EU eTEN program which aims to improve the secure access of mobile European citizens to cross-border health care using advanced smart card and web services technologies [2,39]. More specifically, NETC@RDS aims to simplify health care access for citizens with health insurance evidence of entitlement while abroad and also to provide a reliable source of information for health care provider front office staff checking insured entitlement or initiating interstate billing/clearing procedures. It also aims to develop and use a Common Administrative Electronic Dataset for improved health insurance providers back office billing/clearing workflow applications and further modernization of post-processing activities.

NETC@RDS is basically addressing the following three business cases: (i) The automatic capture of the EHIC dataset, either by optically scanning the EHIC front layout or by electronically reading a national/regional health insurance smart card, (ii) The on-line verification of the EHIC dataset at the point of health care delivery against national/regional repositories located in the home country, and (iii) The sending the EHIC scanned copy, or the EHIC dataset to the competent institution, in view of further e-billing processing [2,39].

The NETC@RDS Consortium includes stakeholders from 16 European countries. It started in 2002 and ended in 2011. The service is however still provided today through the ENED consortium [39], created and supported by participating member states. The last implementation phase encompassed 626 health care service points in 16 EU/EEA Member states and Switzerland. The deployment of NETC@RDS infrastructure is also regarded as a test bed for the ongoing introduction of the e-EHIC.

3.2 System overview

The NETC@RDS project [26,28] has established a cross-border online pan-European service to authenticate a patient's health insurance card and/or a patient's entitlement to health insurance benefits abroad 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 data exchange.

The NETC@RDS technical architecture [2,26] consists of secure network interconnections within a Member state and between the Member states, linking national service portals and registries in each country with workstations within all service facilities. 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 NETC@RDS architecture currently features a direct communication between the individual national service portals as shown in figure 3.

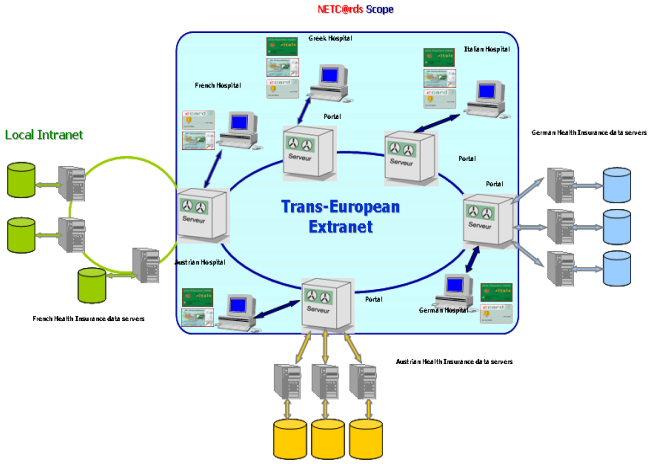

Fig. 3. How the existing NETC@RDS system works

3.3 The NETC@RDS Secure cross-border electronic authentication

Security is a critically important issue for NET@RDS deployment. Without adequate security in place none of the NETC@RDS systems can be used in real-life environments. The secure network interconnection between the 16 national portals relies on a common Information Security Systems Policy (ISSP) [28]. The Security Policy describes the NETC@RDS information system security needs and requirements and provides the basis for a secure operational environment.

Each partner must respect the ISSP to be allowed to access / connect its portal to other portals. It is also foreseen in the ISSP that security audits must be conducted each year to verify the NETC@RDS ISSP compliance [28]. A suitable security audit

procedure and tool has also been constructed and approved. The audit procedure has been agreed and implemented by all partners.

The NETC@RDS security infrastructure has been divided in three layers: Layer 1 (international/country-to-country level, between national NETC@RDS portal servers), Layer 2 (national level, portal-to-backoffice), and Layer 3 (national level, portal-to-Service Units).

Layer 1 security implementation is common in all participating countries. At this level all national portal servers intercommunicate through the internet using PKI infrastructure to achieve a high level of secure communication. All servers should have a reverse proxy service in place that redirects communication either to other national portals or to local BackOffice services. All communication should also be SSL v3 encrypted and performed under HTTPS protocol. Additionally server identification and authentication should also be achieved using certificates. In other words, portal-to-portal communication should involve server and client certificate exchange in order to attain server identification, authentication and authorization. Layer 2 security layer refers to the security infrastructure that is in place in the NETC@RDS infrastructure between the national portal server and the back office services, while layer 3 refers to the security infrastructure that is in place in the NETC@RDS infrastructure between the national portal server and the Service Unit workstations (Service Unit points).

The NETC@RDS common security policy has been constructed under the basic principle that the network build among the NETC@RDS partners should not add any unacceptable new risk within any partner organization. In addition, appropriate technologies and procedures must be used to ensure that data travels with adequate safety over the network build among the NETC@RDS partners and is only disclosed to authorized parties**.** The NETC@RDS information security policy should also provide means of proof and essential checks which give users trust in the given information. It should also help establish the basic security requirements that must be satisfied in order to ensure system continuity and prevent and minimise the impact of security incidents by implementing a stable, reliable and secure infrastructure. Finally, the NETC@RDS security policy is constructed under the principle of well-proportioned answer to the incurred risk.

Regarding its context, the NETC@RDS ISSP recognises three main actors that interact in the NETC@RDS system: the end users group, the health insurance organizations and the national access point providers. It also recognises two main beneficiaries (the insurees and the liaison offices), and four main data exchanges (Authentication Data, Administrative Data, Validation data and Data with Test Values) (figure 4).

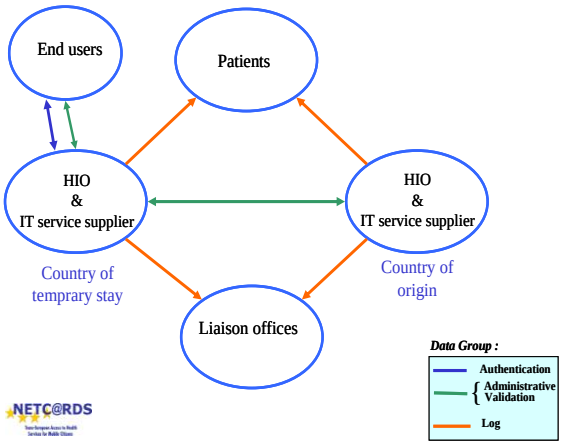

Fig. 4. Exchanges of data in the NETC@RDS context

Finally, as far as the legal basis is concerned, there are two distinguished dataflows identified in the ISSP for the NETC@RDS system: the NATIONAL dataflow level (from the End User to his National HIO/IT service supplier, or other related national dataflows) and the INTERSTATE dataflow level (from the National HIO/IT Service of the Member State of Temporary Stay, to the National HIO/IT service supplier of the Member State of Origin). For the NATIONAL dataflow, the actors should respect the respective national laws on data protection in effect, while for the INTERSTATE dataflow, as a pan European network, the NETC@RDS actors should respect at least the related European legislation (for example the European Directive 95/46/EC on data protection) [28].

The NETC@RDS ISSP includes 7 basic security rules (3 of national and 4 of European competency). It also includes a long list of procedural and technical recommendations.

A secure network interconnection between the national portals can also be provided by the integration in the EESSI architecture [1]. The respective national health insurance networks will be connected in this case by establishing national portals, which connect with each other via EESSI (figure 5). A cross-border electronic authentication request will then be routed through this network. EESSI is devoted to asynchronous cross-border data exchange between social security organizations, while NETC@RDS provides real time authentication mechanisms by on-line control between health practitioners and the foreign competent institution. However, this mechanism can be considered as a generic one and can be also adapted to other e-Gov/e-Health services like e.g. cross-border ID Management.

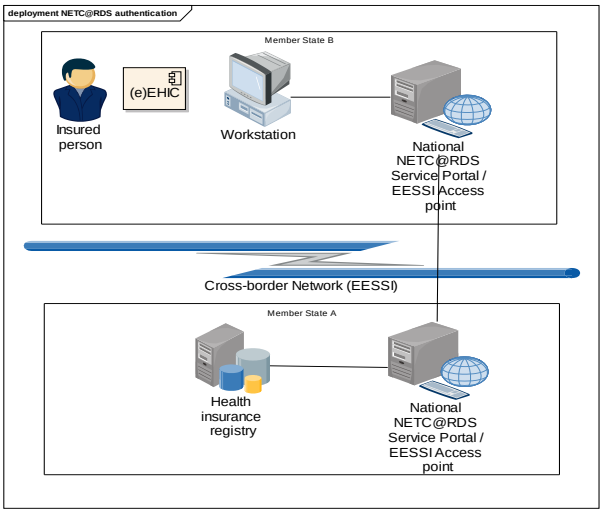

Fig. 5. Integration of NETC@RDS with the EESSI[2] architecture

3.4 Example NETC@RDS Scenario

One of the most important purposes of NETC@RDS and the e-EHIC is to prove, through secure online cross-border authentication, the entitlement of a European citizen outside his/her home Member-State while requesting healthcare services. This can be described, via an example scenario, as follows (figure 6):

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. For her entitlement, she shows either her eye-readable EHIC or, if the EHIC is expired, her electronic national/regional Health Insurance Card 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 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 back office database for verification of the dataset and for authentication of the health insurance smart card shown as proof of entitlement at the point of health care delivery. 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.

[2] EESSI = Electronic Exchange of Social Security Information [5,6]

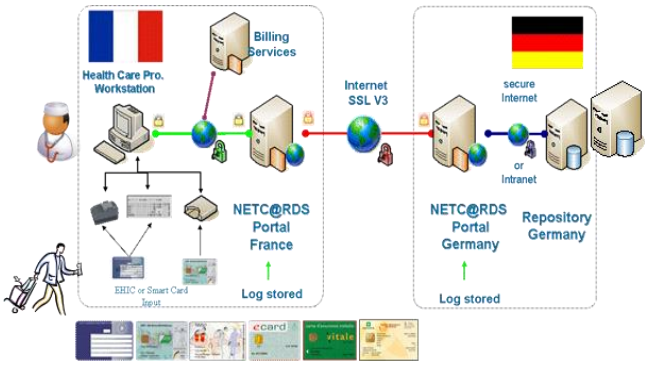

Fig. 6. How the existing NETC@RDS system works – example scenario

It is possible to use either EHIC or different types of electronic national/regional health insurance cards. Independent of what type of card is presented at the patient check-in front desk in a hospital or in an ambulatory facility, the technical infrastructure enables first the capture of the EHIC dataset from various portable documents (i.e. a valid eye-readable EHIC or a national/regional health and insurance smart card or any other ID token) and then the validity of entitlement by the issuing institution. SELECTED STUDIES

4 Mapping the ENISA generic model to the NETC@RDS implementation

The NETC@RDS technical infrastructure using EESSI is mapped below to the proposed ENISA generic cross-border electronic authentication model, therefore proving that it can provide the basis for the implementation of the generic model. The NETC@RDS model including this mapping is described in figure 7.

Mapping the generic model to NETC@RDS is based on the following relations [1,2,28]:

The insured person residing outside his/her home Member-State requesting health services is the generic model's user. This user is entitled to obtain the 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 the 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. The part of the NETC@RDS workstation that interfaces with the NETC@RDS Service Portal must be considered to be a first subcomponent of the Cross-Border Adapter [1].

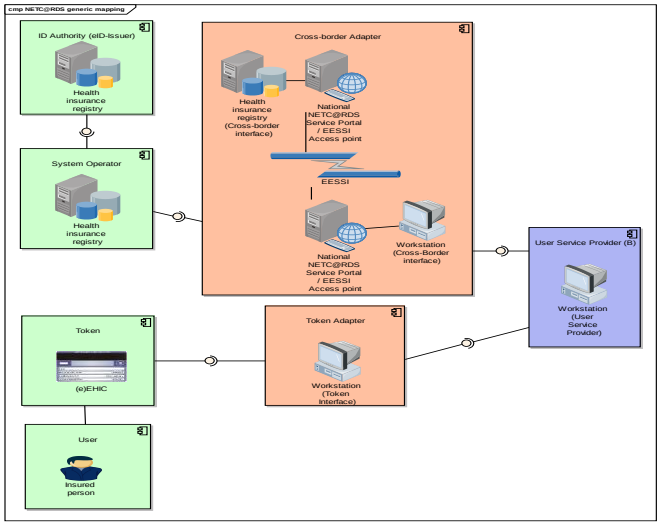

Fig. 7. Mapping of NETC@RDS components to the generic ENISA model

While following this approach, the NETC@RDS project would follow the European Regulations for 883/04 on the coordination of social security systems [4]. Additionally to each Portal, national laws and regulations are applicable.

5 Addressing cross-border protection requirements with the netc@rds implementation approach

The following case study provides an example of addressing NEC@RDS cross-border data protection requirements that demonstrates the suitability of NEC@RDS approach for implementing the ENISA generic security model. It is based on the last evolution step of NETC@RDS in which the national service portals will communicate with each other securely via the EESSI [1]. In this function it is assumed that each national portal authenticates its domestic communication partners as persons or institutions 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.

i. **Identity Data.** The Identity Data used and transmitted in the NETC@RDS electronic authentication is defined in the CEN Workshop Agreement CWA 15974 (May 2009) [25]. According to this document the EHIC identity 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, identification number and acronym of the competent institution, logical number of the card (including a card issuer identifier), and identification of the paper form that is replaced by the card. The EHIC data set is transmitted to the Health Insurance Registry (the System Operator) during authentication.

ii. **Application Data.** In addition to the EHIC data set, other information is also 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.

iii. **eEHIC (Token).** The eEHIC contains the 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 the free access to the eEHIC dataset. The mandatory EHIC dataset is also printed on the eEHIC surface. The eEHIC is under the control of the user, and it is assumed that the user consents to reading the data by handing the eEHIC to somebody.

iv. **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 amount of 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. Nevertheless these aspects are beyond the scope of a risk assessment for cross-border authentication, since the health insurance company is required to maintain the required levels of security also 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.

v. **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 the respective 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.

vi. **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 the 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 respective local laws and contracts. It is assumed that the communication with the national service portal is performed via a secure connection that requires mutual authentication.

vii. **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 network EESSI. 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.

6 Limitations and future research directions

As seen above, the proposed NETC@RDS approach can provide a suitable basis for a secure electronic cross-border authentication implementation, based on the ENISA generic security model, that suitably addresses the cross-border authentication requirements. There are still however a number of limitations and areas for further research that need to be addressed if the proposed implementation approach is to be used as a multipurpose electronic cross-border authentication system.

Data privacy must be adequately protected in any such approach to electronic authentication, be it domestic or cross-border. Cross-border activity is governed however by the different laws and regulations of participating states. These laws often either affect or even prohibit specific transactions or data exchanges. Therefore, there is a need to further clarify the approach on how to respect the European and national data protection laws and regulations within the proposed electronic cross-border authentication system. There is, for instance, a need to further review the relevant EU and national law and regulation for impact on the design of the authentication system and also analyze additional legal provisions and regulations at national level. The regulatory basis for the cross-border implementation also needs to be further studied and incorporated. More detailed guidance should also be given to participating countries on how to best establish or extend existing mechanisms that meet the necessary level of trust.

The problem/risk of identity theft in electronic cross-border authentication also needs to be further studied. Further research is required to fully ensure that the eID token is used by its rightful holder and that the request for authentication is really in accordance to the will of a trustworthy authority / holder.

Cross-border authentication must also mutually establish, beyond any reasonable doubt, the identities of the user and the user service provider. To this end, a sufficient chain of trust must be established through all participants in the cross-border authentication process. The issue of how the system operator will establish sufficient trust in the identity of a user service provider across borders poses another interesting concern. The question mainly lies on the reliability and confidence with which a national portal authenticates its participants. The proposed common security policy for all participants in the cross-border exchange could provide the basis for such a suitable common level of security by all participants.

The cross-border system must also effectively ensure secure communications. These can either rely on secured publicly accessible internet connections or be integrated in dedicated secure cross-border networks (as for example EESSI). The authentication of the participants within the overall communication and the security of communication itself (e.g. by sufficiently strong encryption), also warrants further study.

Finally, the implementation of a secure real-time solution, based on existing EESSI flows, as for example the real-time verification of the patient's cross-border entitlement verification at the healthcare providers sites, needs to be further investigated, if the potential of EESSI is to be fully realized. This can be based on both the EHIC or national/regional social security cards and other portable ID documents.

7 Conclusions

Current electronically readable identity documents issued to citizens are usually available today only in a national context. European citizens moving freely through Member States face the problem that their eIDs from their home state do not allow access to services of another Member State in which they are temporary present. It is therefore an important task to improve the cross-border interoperability of electronic identification and authentication systems, something that has been clearly highlighted in the ENISA report on secure cross-border automated services.

As seen in this paper, the NETC@RDS approach can provide a suitable, ENISA-model-based implementation approach for cross-border authentication that can also be applied in several application areas, including the social and health insurance sector. More specifically, it has been shown that the NETC@RDS approach can provide an implementation methodology for the ENISA generic model that can support electronic cross-border ID verification and authentication at an intra-European scale. It also helps address a number of other related risks related to electronic cross-border authentication, such as legal and regulatory issues, improvement of user credentials and bridging technological infrastructures at the national level, on which however further research is required.

8 References

1. Security Issues in Cross-border Electronic Authentication - ENISA, Feb 2010, http://www.enisa.europa.eu/activities/identity-and-trust/privacy-and-trust/eid/xborderauth
2. The NETC@RDS project, www.netcards.eu
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 100-1Infomation 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. The NETC@RDS Security Policy, Deliverable D.5, 2011, available from: http://www.netcards.eu
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 theier families moving within the Community
31. European Community: Decision No. 189 of 18 June 2003 of the Administrative Commision 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
36. European Union: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

37. European Union: Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications
38. EU Data Protection Directive http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
39. The ENED network: http://www.ened.eu