

AUTHENTICATION OF PROFESSIONALS IN THE RTS E-HEALTH SYSTEM

André Zúquete

*IEETA / Univ. of Aveiro, Campus Univ. de Santiago, 3810-193 Aveiro
andre.zuquete@ua.pt*

Helder Gomes

*IEETA / ESTGA / Univ. of Aveiro, Campus Univ. de Santiago, 3810-193 Aveiro
helder.gomes@ua.pt*

João Paulo Silva Cunha

*IEETA / Univ. of Aveiro, Campus Univ. de Santiago, 3810-193 Aveiro
jcunha@ua.pt*

Keywords: e-Health, authentication, public key certificates, PKI, smartcards, SSL/TLS, roles, RBAC

Abstract: This paper describes the design and implementation of a PKI-based e-Health authentication architecture. This architecture was developed to authenticate e-Health Professionals accessing RTS (Rede Telemática da Saúde), a regional platform for sharing clinical data among a set of affiliated health institutions. The architecture had to accommodate specific RTS requirements, namely the security of Professionals' credentials, the mobility of Professionals, and the scalability to accommodate new health institutions. The adopted solution uses short lived certificates and cross-certification agreements between RTS and e-Health institutions for authenticating Professionals accessing the RTS. These certificates carry as well the Professional's role at their home institution for role-based authorization. Trust agreements between health institutions and RTS are necessary in order to make the certificates recognized by the RTS. As a proof of concept, a prototype was implemented with Windows technology. The presented authentication architecture is intended to be applied to other medical telematic systems.

1 INTRODUCTION

RTS (Rede Telemática da Saúde (Cunha et al., 2006; Cunha, 2007)) is a regional health information network (RHIN) providing an aggregated view of clinical records provided by a set of affiliated health institutions (HIs). Each HI uses its own system to produce and manage clinical records, which can be browsed and presented in different ways by RTS. The goal of RTS is not to replace the systems used by the affiliated HIs, but to provide a mediated, global view of patient's clinical records independently of the HIs holding their records.

RTS provides Portals for accessing clinical records. Two Portals were foreseen: the Patients Portal and the Professionals Portal. The first is to be used by Patients to communicate with their family doctor and other health system issues such as renovation of prescription and schedule appointments. The second is to be used by healthcare Professionals for accessing clinical records required for their normal, daily work.

The RTS Professionals' Portal is a web server accessible through RIS (Rede Informática da Saúde¹), a nation-wide, private network, interconnecting all HIs, including the ones affiliated with RTS. Professionals access data provided by RTS using a normal web browser running on a computer connected to the RIS.

¹Health Computer Network

This paper describes an authentication architecture providing strong authentication for Professionals accessing the Professionals' Portal. Strong authentication is provided by using a two-factor approach: possession of a security token and knowledge of a secret. For the security token we chose a smartcard. Smart cards are tamperproof devices with security-related computing capabilities which are very convenient for running computations using private keys of asymmetric key pairs.

This paper is organised as follows. Section 2 overviews the authentication architecture and some RTS requirements. Section 3 presents some design goals. Section 4 presents the proposed authentication architecture. Section 5 presents some related work. Section 6 presents our prototype implementation. Section 7 evaluates the architecture and the implementation. Section 8 concludes the paper.

2 OVERVIEW

This paper describes an authentication architecture providing strong authentication for Professionals accessing the Professionals' Portal. Strong authentication is highly recommended in this case, as Professionals can access sensitive data — the patients' health records. The architecture allows Professionals to roam between computers of their HI or other HIs.

Our authentication architecture had also to deal with authorization issues. In fact, the RTS Portal uses a role-based access control (RBAC) policy for deriving the Professionals' authorizations to access clinical data. Therefore, each time a Professional accesses the RTS Portal, the later must learn a role that the former may legitimately play for deriving authorisations.

The proposed architecture uses public key cryptography as the basis for its operation. Each Professional is given a smartcard for storing and using personal credentials for accessing the RTS Portal. The Professionals' authentication process uses a facility provided by web browsers, the SSL/TLS client authentication with asymmetric keys and X.509 public key certificates (PKCs), to prove the authenticity of the Professional to the RTS Portal (Housley et al., 1999; Dierks and Rescorla, 2006).

Furthermore, the PKCs used by Professionals in the SSL authentication process provide extra information to the RTS Portal, besides the identity of the Professionals, such as the HIs they are affiliated to and the role they are playing. As a Professional may play several roles simultaneously (e.g. Doctor and Chief Doctor), the PKC must contain all the roles we can play, being up to the RTS Portal to chose the role to play, from the possible ones, in each session.

Since a Professional's PKC carries roles the owner can play, a mechanism must be provided to deal with role changes. A possibility was to use certification revocation for outdating given roles. However, revocation validation requires online communication between the PKC validator and the PKC issuer, which may not be possible or convenient. Furthermore, some roles are very short in time, for example, vacation substitutions, and these dynamics can be more easily managed by short lived certificates than by Certificate Revocation Lists (CRL).

Alternatively, we chose to used short-term validity periods for Professionals' PKCs, as in (Ribeiro et al., 2004). This way, Professionals' PKC get automatically invalid after a short period of time after their issuing and Professionals must apply for new ones. A simple and secure enrolment process was also conceived for getting new PKCs.

The public key infrastructure (PKI) for managing Professionals' credentials for accessing RTS uses a flexible, scalable grassroot approach. Each HI and the RTS have their own PKI, including root and issuing certification authorities (CA). The issuing CA of each HI is responsible for issuing RTS credentials for local Professionals. The issuing CA of RTS is responsible for issuing credentials for the RTS Portal. The validation of certificates issued by separate PKIs is enabled by cross-certification agreements. This means that the RTS Portal will only be able to validate Professionals' credentials issued by HI CAs cross-certified by RTS; other people, including Professionals from other HIs, cannot be authenticated by the RTS Portal, therefore cannot access protected clinical data.

In this paper we mainly describe our architecture for using smartcards for authenticating Professionals and the RTS Portal when interacting with each other and for providing Professionals' roles to RTS. However, the architecture was designed taking into consideration future enhancements and synergies, such as:

- Enable Professionals to use the same smartcard for producing signed data as input for health information systems.
- Enable Professionals to give signed consents regarding accesses to the clinical data.
- Adoption of a similar authentication model for authenticating Patients, possibly using the new, smartcard-enabled Citizens Card.
- Usage of PKIs deployed for managing smartcards to generate credentials for mutual authentication within secure communications between hosts or servers used in the RTS and in HIs (e.g. with IPsec or SSL/TLS (Kent and Atkinson, 1998; Dierks and Rescorla, 2006)).
- Usage of PKI deployed in each HI for managing the local authentication of Professionals accessing local services (e.g. secure wireless network access).

3 DESIGN GOALS

A set of design goals were defined at start. Those goals derived both from RTS requirements and from previous experiences with informatics services in healthcare environments.

The first goal was Professionals' mobility. The authentication architecture should not restrict the mobility of Professionals; at the end it could be possible to use any computer, belonging to the RIS, to access RTS services. Naturally, this goal depends on software and hardware installed in client computers accessing Professionals' authentication tokens. Nevertheless, we tried to facilitate the widespread use of those tokens by using common hardware (e.g. USB ports) and free software packages (e.g. software packages already provided by operating system vendors).

The second goal was to be pragmatic regarding the implementation of a PKI for managing asymmetric keys and PKCs. Nation-wide PKIs do not exist for this purpose. And, though they could be advantageous, they are also difficult to deploy and to manage. Thus, we chose to start from a sort of minimalist, ad-hoc scenario, with no global PKI on top of the RTS and all the HIs, but instead with isolated, standalone PKIs on each entity, RTS and HI.

The third goal was RTS independency regarding the management of personnel in affiliated HIs. Each HI is an independent organization, with its own Professionals, human resources management department and some kind of directory service to store the Professionals' information. Independent of RTS, they will continue to manage their Professionals because

of their own, internal systems. It thus makes sense to reuse HI Professionals information and let each HI to manage the access of its own Professionals to the RTS. This way, we avoid replication of information and a centralized enrolment of Professionals in RTS.

The fourth goal was to minimize communication overheads related to the authentication of Professionals and fetching/validation of role membership. Namely, we tried not to use on RTS any online services from HIs to deal with details regarding the identification, authentication and role membership of Professionals. Since Professionals' information is managed solely by their home HI (our previous goal), this means that Professionals' identification and authentication credentials should convey RTS as much information as possible, to avoid contacting online services at Professionals' home HIs.

The fifth and final goal was browser compatibility. To avoid the requirement of using a specific browser, no client-side active code (ActiveX and Java Applets) is used in RTS. Therefore, we could not use any special code for managing the authentication of Professionals using a browser to access RTS. In other words, the authentication mechanism using a two factor approach should be already available within the basic functionality of all browsers. As we will see, although the basic functionality exists in all popular browsers (support of SSL client-side authentication), the exact mechanisms and policies used to handle such support are different and raise some problems.

4 AUTHENTICATION ARCHITECTURE

The authentication architecture is resumed in Figure 1. The Professional uses a web browser to access the web server that implements the RTS Portal, and uses an SSL secure channel for protecting the communication from eavesdropping. Furthermore, mutual authentication is required in the establishment of the SSL secure session, thus the browser authenticates the RTS Portal and the RTS Portal authenticates the Professional using the browser. Similarly, the Professional uses a web browser a mutually authenticated SSL session to access the HI Issuing CA web server for requesting fresh RTS credentials.

4.1 The Professionals' Smartcard

A Professional's smartcard carries two types of asymmetric key pair and corresponding PKCs. One type we call **RTS credentials**, which are to be used to authenticate himself when accessing the RTS Portal. The other type we call **HI credentials**, which are to be used to authenticate himself when accessing his HI issuing CA for getting new RTS credentials.

Smartcards are initialised and provided by HIs to their own Professionals. At start they only carry the HI credentials. When required, the owner uses them for requiring RTS credentials. These credentials can then be used to access the RTS Portal.

RTS credentials are short lived, lasting for one or a few days. The RTS Portal doesn't use remote HI services for checking for their validity. Instead, it assumes that a Professional's role revocation will naturally be enforced by not being able to get a new RTS credential including the revoked role. On the contrary, HI credentials are long lived, because they are used for long periods of time for getting new RTS credentials.

4.2 Professional Authentication

The Professional authentication is requested by the SSL server-side of web servers and conducted by the SSL client-side running on browsers. The SSL client-side authentication uses the Professional's smartcard for his authentication. The browser is configured to use smartcard services and when client-side authentication is required it will prompt the Professional for the right credentials, including the ones inside the smartcard, he intends to use. The Professional chose the right pair of asymmetric keys from the smartcard, and the PKC of the public key, and the browser uses them to provide client-side authentication.

This client-side approach is the same for accessing the RTS Portal or the HI Issuing CA. It is up to the Professional to choose the right set of credentials, from the smartcard, to get authenticated. And in all cases it needs to introduce a PIN to unblock the smart card for producing digital signatures required by the SSL authentication protocol.

The web servers used by the RTS Portal and the HI Issuing CA perform the following actions: (i) validate the PKC chose and presented by the Professional, (ii) use the certified public key to validate the SSL secure channel establishment and (iii) enable the service, RTS or CA, to access the Professional's PKC. The RTS learns from the PKC the Professional's identity, his home HI and his roles; the CA learns only the Professional's identity.

4.3 Role Assignment and Selection

The roles of each Professional are embedded in the PKC of his RTS credentials. These roles are stored in extension fields, namely the Extended Key Usage (EKU) field. Each role was given a numerical tag, an ASN.1 Object Identifier, reserved at IANA² for RTS.

Each time a Professional requests RTS credentials, he gets, after proper authentication at the HI Issuing CA, a new PKC with the current roles he can play. This PKC is communicated to the RTS web server during SSL authentication and, if successful, the PKC is made available for consulting by the RTS Portal during the SSL session. This way, when a Professional initiates an SSL-protected session with the RTS Portal, it can easily learn the set of roles the Professional can play and prompt the Professional for selecting the right role for the current session.

²<http://www.iana.org>

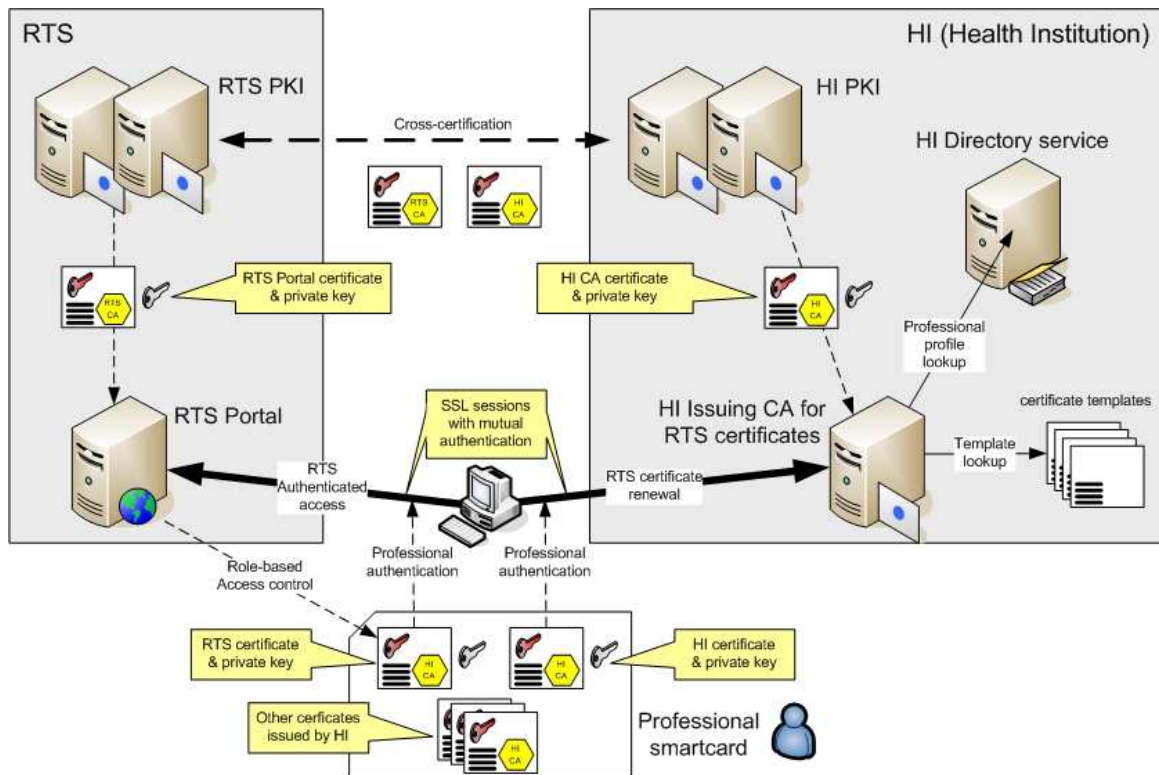


Figure 1: Overview of the authentication architecture for HI Professionals whiling to access the RTS Portal

4.4 Trust Relationships

Each entity, RTS and HI, uses an independent PKI for managing RTS and HI authentication credentials used by Professionals. The RTS is not meant to serve as a CA for all HIs; it only deploys a PKI mainly for managing its own certificates. HI certification hierarchies may be isolated or integrated in wider hierarchies providing large-scale validation of certificates. For the RTS that is irrelevant, all it requires is an Issuing CA for issuing RTS credentials for local HI Professionals.

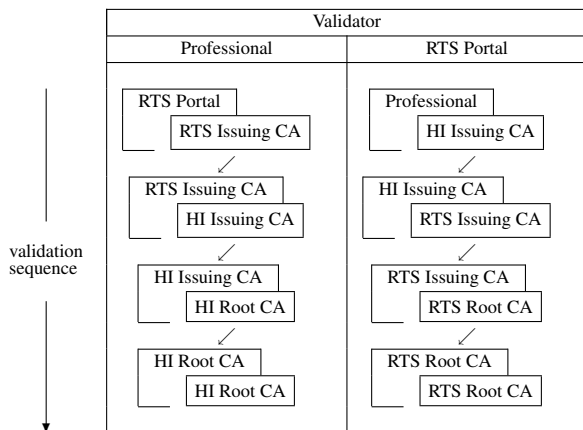
Since RTS and HI certification hierarchies are isolated from each other at the beginning, some mechanism is required to enable the RTS Portal to validate Professionals' RTS credentials, issued by HIs. Similarly, some mechanism is required to enable professionals to validate the credentials of the RTS Portal, issued by RTS. This mechanism is cross-certification.

When an HI gets affiliated to the RTS, the RTS Issuing CA issues a certificate for the public key of that HI Issuing CA. With this certificate, the RTS is able to validate all the PKCs of RTS credentials issued for the Professionals of that HI. Similarly, the HI Issuing CA issues a certificate for the RTS Issuing CA, enabling local Professionals to validate the credentials of the RTS Portal.

4.5 Validation of Certificates

With this cross-certification in place, the validating of certificates' certification chains works as follows. The RTS Portal trusts only on the (self-signed) certifi-

cate of the RTS Root CA. Similarly, the Professional trusts only on the (self-signed) certificate of his HI Root CA. Since certificate chain validations progress recursively until finding an error or a trusted certificate, the validation chains are the following:



where \boxed{X}_Y represents the PKC of X issued by Y.

Besides cross-certification for certificate chain validation, trust relationships between the RTS, HIs and their Professionals must be complemented by common certification procedures. Namely, all HIs affiliated to the RTS should follow similar procedures for issuing RTS credentials. For instance, smartcards with HI credentials should be initialised by HIs and personally delivered to Professionals.

4.6 Validity of Authentication Credentials

The authentication credentials stored inside a Professional's smartcard are the HI credentials and the RTS credentials. The first ones are used to establish an authenticated session to get the second ones.

HI credentials are to be used frequently, for instance, once per day or once for a couple of days, to fetch new RTS credentials. Therefore, they should have long validity periods and CRLs must be published to prevent unwanted use of them after a given instant. For instance, if a Professional moves from one HI to another one, his smartcard from the former HI must be returned and a CRL should be issued to invalidate the public key of the HI credentials inside the smartcard. Note, however, that CRL issuing and validation are all executed within the same HI, and not by external clients.

RTS credentials are valid only during short periods of time, one or two days. Therefore, no CRLs are used to validate them, since the error window is too narrow to allow a Professional to play a role he is no longer allowed to. Consequently, by default the HI Issuing CA doesn't publish CRLs for RTS certificates.

In special cases, such as disciplinary processes and legal inquiries, it should be possible for the HIs to provide to the RTS Portal, just in time, a list of RTS certificates that should no longer be accepted while in validity period. But since such cases should be rare, it is preferable to deal them as the exception to the general rule above stated: no CRLs exist and are checked for RTS certificates.

All the certificates used in both HI and RTS credentials do not need to be published by Issuing CAs. In fact, these certificates are used solely in the context of SSL mutual authentication, and are communicated to the interacting peers within the SSL protocol. Therefore, they need not be published in some public directory System, as other certificates do, because no one needs them for other purposes.

5 RELATED WORK

The following e-Health Systems were analysed: HYGEIANet and MedCom/Sundhed.dk.

5.1 HYGEYANET

HYGEIANet is the RHIN of Crete, Greece. It was developed by the Institute of Computer Science (ICS) of Foundation for Research and Technology – Hellas (FORTH) to provide an integrated environment for delivery of health care services in Crete Island (Katehakis et al., 2005; Tsiknakis et al., 2005).

Similarly to RTS, HYGEIANet is formed by several HIs, namely Hospitals and Primary Care Units, each with its own health data, information services and human resources. HYGEIANet operates above these independent healthcare units, providing an infrastructure for sharing clinical information. Also, the

Integrated Electronic Health Record (I-EHR) is a key element as it aggregates the patient health information in all participating healthcare units.

The trust and security frameworks are implemented in HYGEIANet with VPNs, SSL, smartcards, PKI, security certificates and digital signatures. A Regional certification authority issues the certificates for users and applications. These certificates can be used to authentication and digital signing of documents and in case of user certificates they can be stored in smartcards (Katehakis et al., 2005)

Authentication is a centralized process in HYGEIANet. All applications and services are registered in the Health Resource Service (HRS) and issued a unique ID. Each HYGEIANet user also must register in HRS to be able to use HYGEIANet services, and a unique user name and password is provided. The username and password are communicated to an authentication server (AS) and a certificate is issued from the regional CA.

In terms of authorization it follows a decentralized approach, where each individual service maintains and manages roles (groups) and role based permissions. The user must be assigned to the proper role in each service he is to have access.

When accessing a service, the user is authenticated through the Authentication Service and gets his individual access rights validated through the individual service.

The RTS and HYGEIANet approaches for authentication differ: HYGEIANet has a centralised management of resources (users and services), with certificates issued by a regional CA, and requires an online AS for user authentication. On the contrary, RTS has a decentralized management of resources, reusing the management services belonging to the affiliated HIs, with certificates issued by HI CAs for their own users and services and not requiring any online user authentication service to be used by RTS.

5.2 The Health Portal (Sundhed.dk) and the Health Data Network of Denmark (MedCom)

MedCom is the National Health Data Network of Denmark. It is working since 1994, and it connects more than 2000 Hospitals, Pharmacies, General Practitioners (GPs) and Specialists. It started has a VAN network exchanging EDIFACT messages (ISO 9735, 1988). In 2004 it started the process of migration to the Internet and EDIFACT messages were translated into XML messages. Today, both message formats are used (MedCom IV, 2003).

Network security is implemented at three levels (Pedersen, 2005; Voss et al., 2005).

At the first level are VPN connections connecting healthcare networks to a central hub in a star topology. This solution allows the reuse of Internet connections that all the health care units already have.

At a second level there is an agreement system that controls the data flows from and to any of the local healthcare networks. When a connection between two healthcare networks is needed, a previous access to the agreement system is required to establish the connection between the two networks.

The third level of security is user authentication, made locally through his username and password, or his asymmetric key pair and PKC.

The Health Portal started in December 2003. It works on top of the Health Data Network and reuses its infrastructure and services. Unlike the Health Data Network, that only provides services for Professionals, the Health Portal provides services for both Citizens and Professionals (Sundhed.dk, 2006).

User authentication, for both Citizens and Professionals, is made using OCES certificates³ issued by the national PKI that can be used in several national public services. Professionals can use several OCES certificates: (i) Administrative digital signature for region, hospital or GP, (ii) health professional's digital signature based on personal identifier and (iii) authorization for treating patients (Rossing, 2005).

Comparing with RTS, the Danish system extensively uses asymmetric keys and PKCs, benefiting from a nation-wide PKI. However, many of the Danish system security requirements, such as Professionals' digital signatures, are currently not required by RTS, since it is not used for entering signed data into the health information system. We believe, however, that our architecture can evolve, but keeping its basic structure, for provide security services similar to the ones provided by Danish system. Furthermore, our PKI may coexist with a national-wide PKI encompassing all HIs, though not necessarily using it.

6 PROTOTYPE IMPLEMENTATION

As a proof of concept, a prototype of the authentication architecture was implemented. The prototype extensively used available products for Windows operating systems, because of its dominance in the computer desktops of the HI currently affiliated to RTS.

The prototype included an RTS service, with a two-level PKI and a web Server (Professionals' Portal), one HI instance, with a two level PKI, an Active Directory Server and one registered Professional (one smartcard). CAs were implemented with Windows Certification Services available in Windows 2003 Server Enterprise Edition. When installed in Enterprise mode, this CA interacts with AD to obtain user information for certificate issuing, and uses certificate templates, stored in AD and subject to AD access control rules, for certificate issuance management.

³OCES certificate: Public Certificate for Electronic Service

The key aspects to test in the prototype were (i) the impact of different middleware software in smartcard deployment, (ii) the deployment of an HI PKI for the management of RTS credentials for local Professionals, and (iii) the use of short lived RTS credentials to access RTS services.

6.1 Smartcard Deployment

Since smartcards are portable devices, in theory they may be used to authenticate Professionals accessing the RTS from different computers. However, this requires some software installed in those computers: (i) the card reader driver and (ii) middleware to fill the gap between applications and smartcard services.

There are different trends in this specific middleware area. Windows applications, such as the Internet Explorer browser, use the CryptoAPI (CAPI), which can use several Cryptographic Service Providers (CSP) for interacting with different smartcards. Another approach is to use PKCS#11 (PKCS#11, 2004), a standard interface for cryptographic tokens. This interface is used by Netscape and Firefox browsers.

Since middleware modules are usually specific for smartcard manufacturers and some manufacturers impose limits on the number of computers where they can be installed or do not provide similar modules for all operating systems, the following approaches were foreseen: (i) the use of smartcards with native support from the operating system, (ii) the use of open source software or free binaries and (iii) the use of non-free software providing support for multiple smartcards.

In our prototype we used only Windows XP systems for the Professional computers and two smartcard tokens: Rainbow iKey 3000 and Schlumberger⁴ Cyberflex e-gate 32k. None of them was natively supported by Windows. Also we were not able to get an open source solution (openSC/CSP#11) working reliably. For the non-free solution we used SafeSign Standard 2.0.3 software, and both smartcards worked properly after their first initialization was made by SafeSign. If this first initialization is not made by SafeSign, chances are that smartcards are not recognized, has it happened with Cyberflex Card.

After low-level initialization (e.g. personalization), smartcards were incepted with the Professional HI credentials, allowing the owner to enrolment for RTS certificates. The HI credentials cannot be renewed and the smartcard becomes useless when the HI certificate validation period expires.

6.2 HI PKI deployment

The HI PKI was implemented with an offline Root CA and an online Issuer CA. The latter interfaces with an AD and with an IIS 6.0 server with a web interface for certificate enrolment, CRL Distribution Point (CDP) and Authority Information Access (AIA) functionalities.

⁴Now Gemalto, after being Axalto

Some groups were defined in AD, one for each identified professional role, and Professionals assigned to them. They provide access control for certificate enrolment.

Certificates issued by the Issuing CA are tailored using certificate templates. These templates allow the definition of certificate characteristics and access control rules. Certificate templates were created, one for each professional role that only differ in the specification of certificate extensions and certificate security. An application policy was defined for each Professional role, to be included in RTS certificates issued for the role; application policies are simple ASN.1 OIDs used by RTS after reservation at IANA. The application policy OID is stored in the certificate EKU (Extended Key Usage) field. Also a certificate template was defined for the HI certificate, with an application policy for RTS certificate renewal.

Note that RTS certificates should contain all the current roles of a Professional, and not only one. However, that is simply not possible with certificate templates and access control rules. Therefore, in the prototype a Professional may have several RTS credentials, one for each role, and chose the proper one when starting a session with the RTS Portal.

The customization of Windows certificate templates has also some limitations. Namely, certificate templates do not allow for validity periods shorter than two days. This may be problematic if two days is considered a large risk window for RTS credentials. But in our opinion two days is perfectly reasonable.

The Issuer CAs also issues cross-certificates for the public key of the RTS Issuing CA. Name constraints were used to define the name space for the accepted certificates. Certificate (issuance) constraints and application constraints were not used because they are not interpreted by browsers, since they require some application context (Lloyd, 2001).

A web interface, adapted from the Microsoft Certificate Services web interface, was deployed for enrolment for RTS certificates. After the Professional authentication using its HI credentials, RTS certificates are immediately issued and installed in the Professional's smartcard. Both Internet Explorer and Netscape can be used for RTS credential renewal.

6.3 Usage of RTS credentials for accessing the RTS Portal

The validation of Professionals' RTS credentials by the RTS Portal, an IIS 6.0 web server, was performed at two different levels. At the IIS level, validation follows SSL rules and certification chains. At the application level, validation includes checking RTS OID values placed in EKU field of the received RTS certificate. The Portal only initiates a session with a Professional if his certificate is considered valid at both levels.

Finally, Professional can use both Internet Explorer and Mozilla Firefox to access the RTS Portal.

Tests were made in order to determine if the number PKCs from the HI PKI hierarchy in the smartcard could be reduced, but due to different approaches between browsers for building and validation of certificate chain, we conclude that all certificates must be present in order to allow both browsers to be used.

7 EVALUATION

In this section we evaluate the architecture and implementation of our authentication system taking into consideration the design goals presented in Section 3.

Concerning the first goal, a pragmatic PKI implementation, it was achieved, since no specific, large-scale PKI is required. On the contrary, the PKI is build on top of independent PKIs and cross-certification agreements. Trust relationships between RTS and affiliated HIs are reflected in such cross-certification and on common policies for issuing RTS certificates for Professionals.

Concerning the second goal, Professionals' mobility, smartcards embedded in USB tokens are the most promising solution nowadays but still raise some problems. For instance, they (still) cannot be used with PDAs and smartphones. Furthermore, and more problematic, the usage of smartcards in USB-enabled computers still raises the problem of software installation for dealing with them. As we saw in Section 6, it is not simple to find a ubiquitous, free solution for the middleware required by different applications (browsers) to interact with many smartcards.

Concerning the third goal, leaving RTS out of the management of Professionals working at the HIs, it was totally attained. The RTS Portal only requires Professionals to have a valid certificate issued by their HI and containing a set of role on it. HIs have full control on the management of local Professionals and their role, enabling RTS access by issuing RTS certificates with the proper contents, namely Professional identity, HI affiliation and possible roles.

The fourth goal, to minimize communication overheads between RTS and HIs for authenticating Professionals and getting their role, was also fully attained. The RTS Portal, by itself, is capable of authenticating Professionals just by validating their certificate, without checking CRLs remotely, and capable of learning their role also from the certificate. No on-line communication between RTS and HIs is required in this process.

The fifth and final goal was browser compatibility. In this case we must say that it may be difficult to provide the same set of functionalities with all the browsers, because of the differences between the existing middleware solutions for bridging the gap between applications and smartcards (CAPI, PKCS#11, etc.). Furthermore, some smartcard management activities, such as garbage collection of useless credentials inside the smartcard, may require the deployment of active code for running within Professionals' browsers.

8 CONCLUSIONS

In this paper we described the design and implementation of an authentication architecture for Professionals working within the RTS e-Health environment. Since Professionals access RTS services using a browser and an RTS Portal, the authentication of Professionals was mapped on top of SSL client-side authentication. The credentials used in this authentication are provided by their HIs and formed by a private key and a short-lived X.509 PKC, both stored inside a smartcard. The short lifetime of these certificates allows issuing CAs to simplify their PKI: they are not published and they are not listed in CRLs.

The key characteristics of the authentication architecture are (i) the use of smartcards for strong authentication, to store Professional credentials and to improve their mobility, (ii) the use of short-lived RTS certificates carrying Professional identification and roles for authentication on the RTS Portal and authorization of operations required to the RTS, (iii) the use of “normal”-lived HI certificates for Professional enrolment for RTS certificates, (iv) a PKI where the RTS and each HI run their own, private PKI with (v) cross-certification for the establishment of trust relations required to validate Professionals credentials and RTS credentials within SSL sessions. This authentication architecture is highly scalable and is prepared to be applied to other medical telematic projects such as the Brain Imaging Network Grid (BING) (Cunha et al., 2007) and the Grid-Enabled REpoSitories for medicine (GERESmed), two medical networks now under development an IEETA/University of Aveiro.

A prototype was implemented as proof of concept and based exclusively in technology provided by Windows systems or developed for Windows systems. Regarding the browsers used by Professionals, we tested two of the most popular ones also on Windows systems: Internet Explorer and Mozilla Firefox.

The major source of problems that we found for implementing the prototype was the use and management of smart cards by Professionals' systems and browsers. The variety of middleware existing for managing smart cards and the different approaches followed by different applications (browsers) regarding the middleware make it very hard to provide a clean, ubiquitous interface for Professionals. Furthermore, this is a critical issue in the deployment of this authentication architecture along many different systems and computers.

Acknowledgements

This work was financed by the Aveiro Digital Programme 2003-2006 of the Portugal Digital Initiative, through the POSI programme of the Portuguese Government, and by the FCT (Portuguese R&D agency) through the programs INGrid 2007 (grant GRID/GRI/81819/2006) and FEDER.

REFERENCES

- Cunha, J. P. (2007). RTS Network: Improving Regional Health Services through Clinical Telematic Web-based Communication System. In *eHealth Conference 2007*, Berlin, Germany.
- Cunha, J. P. S., Cruz, I., Oliveira, I., Pereira, A. S., Costa, C. T., Oliveira, A. M., and Pereira, A. (2006). The RTS Project: Promoting secure and effective clinical telematic communication within the Aveiro region. In *eHealth 2006 High Level Conference*, Malaga, Spain.
- Cunha, J. P. S., Oliveira, I., Fernandes, J. M., Campilho, A., Castelo-Branco, M., Sousa, N., and Pereira, A. S. (2007). BING: The Portuguese Brain Imaging Network GRID. In *IberGRID 2007*, pages 268–276, Santiago de Compostela, Spain.
- Dierks, T. and Rescorla, E. (2006). The TLS Protocol Version 1.1. RFC 4346, IETF.
- Housley, R., Ford, W., Polk, W., and Solo, D. (1999). Internet X.509 Public Key Infrastructure Certificate and CRL Profile. RFC 2459, IETF.
- ISO 9735 (1988). Electronic data interchange for administration, commerce and transport (EDIFACT). <http://www.iso.org>.
- Katehakis, D. G., Sfakianakis, S. G., Anthonoulakis, D., Kavlentakis, G., Tzelepis, T. Z., Orphanoudakis, S. C., and Tsiknakis, M. (2005). A Holistic Approach for the Delivery of the Integrated Electronic Health Record within a Regional Health Information Network. Technical Report 350 (FORTH-ICS/ TR-350), Foundation for Research and Technology - Hellas, Institute of Computer Science, Heraklion, Crete, Greece.
- Kent, S. and Atkinson, R. (1998). Security Architecture for the Internet Protocol. RFC 2401, IETF.
- Lloyd, S. (2001). CA-CA Interoperability. PKI Forum.
- MedCom IV (2003). MedCom – the Danish Healthcare Data Network. MedCom IV, Status Plans and Projects. <http://www.medcom.dk/dwn396>.
- Pedersen, C. D. (2005). An baltic healthcare network and interoperability challenges. Cisco eHealth think tank meeting.
- PKCS#11 (2004). PKCS #11 v2.20: Cryptographic Token Interface Standard. RSA Laboratories.
- Ribeiro, C., Silva, F., and Zúquete, A. (2004). A Roaming Authentication Solution for WiFi using IPSec VPNs with Client Certificates. In *TERENA Networking Conference 2004*, Rhodes, Greece.
- Rossing, N. (2005). The Health Portal (www.sundhed.dk) And The Health Data Network Of Denmark. Executive Summary of Presentaion in eHealth Athens 2005. <http://www.ehealthathens2005.gr>.
- Sundhed.dk (2006). The Danish eHealth experience: One Portal for Citizens and Professionals. <http://dialog.sundhed.dk>.
- Tsiknakis, M., Katehakis, D. G., Sfakianakis, S., Kavlentakis, G., and Orphanoudakis, S. C. (2005). An Architecture for Regional Health Information Networks Addressing Issues of Modularity and Interoperability. *Journal of Telecommunications and Information Technology (JTIT)*, 4:26–39.
- Voss, H., Heimly, V., and Sjögren, L. H. (2005). The Baltic ehealth Network – taking secure, Internet-based healthcare networks to the next level. Norwegian Centre for Informatics in Health and Social Care.