PKI Security in Large-Scale Healthcare Networks

Georgios Mantas[1], Dimitrios Lymberopoulos[1], and Nikos Komninos[2]

[1]Wire Communications Lab., Electrical & Computer Engineering Dept.
University of Patras
GR-26500, Rio Patras, Greece
{gman, dlympero}@upatras.gr

[2]Athens Information Technology
GR-190 02, Peania, Greece
nkom@ait.edu.gr

Abstract: During the past few years a lot of PKI (Public Key Infrastructures) infrastructures have been proposed for healthcare networks in order to ensure secure communication services and exchange of data among healthcare professionals. However, there is a plethora of challenges in these healthcare PKI infrastructures. Especially, there are a lot of challenges for PKI infrastructures deployed over large-scale healthcare networks. In this paper, we propose a PKI infrastructure to ensure security in a large-scale Internet-based healthcare network connecting a wide spectrum of healthcare units geographically distributed within a wide region. Furthermore, the proposed PKI infrastructure facilitates the trust issues that arise in a large-scale healthcare network including multi-domain PKI infrastructures.

Keywords: PKI; healthcare network; trust list; identity certificates; attribute certificates

1. Introduction

Nowadays, the growing need for high quality healthcare provision and the increasing mobility of citizens have led to the realization of large – scale healthcare networks interconnecting many different stakeholders (e.g. hospitals, clinics, pharmacies) of the healthcare sector. The main goal of large – scale healthcare networks is to enhance the provision of healthcare services to the citizens in a more efficient way. They provide higher quality of emergency care, improve the efficiency of emergency healthcare units and enhance patient safety.

A large – scale healthcare network can be seen as an amalgam of heterogeneous information systems, facilitating the exchange of healthcare information effectively across healthcare institutions geographically distributed within a wide region. Moreover, several services such as email and video conference are supported for assisting the efficient and productive collaboration of remote healthcare units.

Therefore, healthcare professionals located in different healthcare units are able to collaborate, share opinions and expertise with their peers to provide care to patients in a more proficient way. Additionally, they are allowed to access information resources, such as clinical data and administrative information, stored in

different healthcare units from any place and any time. Furthermore, this infrastructure supports telemedicine services to patients that prefer to stay at their own home with minimum intervention from healthcare professionals instead of being hospitalized [2, 5, 14].

Modern large – scale healthcare networks are based on Internet technology, since it provides an attractive infrastructure for efficient and cost - effective communication as well as data sharing among doctors, staff members and healthcare units. However, these benefits come with a noticeably great factor of risk as Internet technology has not been designed to guarantee security. Moreover, the fact that patient information is extremely sensitive and critical information introduces many serious security concerns which should be handled appropriately at all possible levels. Hence, when designing the security of large scale Internet-based healthcare networks, it is essential to define the security requirements that should be fulfilled. Authentication, authorization, data integrity and data confidentiality are the most important security requirements that should be satisfied in large-scale healthcare networks. The PKI technology has been widely accepted as the best solution to satisfy these requirements for data exchange over insecure networks such as the Internet. The PKI technology enables the deployment of PKI infrastructures that issue, revoke and manage digital signatures and public key certificates in order to replace handwritten signatures in government services, commerce, and legal proceedings. Digital signatures and public key certificates allow remote parties, who have no previous relationship, to reliably authenticate each other and communicate in a secure way. Moreover, authorization is achieved due to the use of the public key certificates. Furthermore, digital signatures are used to ensure the integrity of the exchanged data. In addition, the uniqueness of the digital signature provides non-repudiation. Finally, the PKI technology enables encryption of the transferred messages in order to provide confidentiality [9, 11]. However, the adoption of PKI solutions in large-scale healthcare networks is moving slowly because of trust concerns that arise among the participating parties.

First of all, large-scale healthcare networks consist of many different interconnected PKI trust domains, since each participating healthcare unit comprise a different PKI trust domain. Additionally, there are not trust management mechanisms to deal with multiple interconnected PKI trust domains appropriately. Consequently, PKI trust development in large-scale healthcare networks is of utmost importance in order to ensure secure communication and exchange of data [5, 10, 13].

In this paper, we propose a PKI-based security infrastructure to provide security in a large-scale Internet-based healthcare network connecting hospitals, clinics, primary care units, pre-hospital health emergency care, homecare units and pharmacies dispersed over a wide area. Additionally, at the same time the proposed infrastructure intends to provide scalability, flexibility and reduced administration costs, especially when the number of participating healthcare stakeholders increases. Furthermore, the proposed PKI infrastructure facilitates the trust issues that arise in a large-scale healthcare network including multi-domain PKI infrastructures.

Following the introduction this paper is organized as follows. In Section 2, we briefly present some related work of PKI infrastructures for healthcare networks to ensure secure communication services and exchange of data among the participating parties. In Section 3, we discuss the main open issues associated with the efficient adoption of PKI technology in large-scale healthcare networks. In Section 4, we describe the proposed PKI Infrastructure. Furthermore, the proposed PKI Trust Model and the main components of the proposed PKI Infrastructure are presented. In Section

5, the description of the Certificate Evaluation Process is given. Finally, Section 6 concludes the paper.

2. Related Work

During the past few years a lot of effort has been invested in research and development of PKI infrastructures for healthcare networks in order to ensure secure communication services and exchange of data among the participating parties. Some related work regarding the current efforts follows.

In [5], a PKI-based e-Health authentication architecture is proposed to authenticate healthcare professionals accessing the RTS (Rede Telemática da Saúde), a regional platform for sharing clinical data among a set of affiliated health institutions over a dedicated national health network. The proposed PKI makes use of unpublished and short-lived certificates as well as cross-certification agreements between the RTS and e-Health institutions to authenticate the healthcare professionals when they access the RTS. The certificates are stored on smart cards and they are also used for professionals' authorization as they incorporate roles of the professionals at their home institution. Furthermore, trust agreements between the e-Health institutions and the RTS take place in order to make the certificates recognized by the RTS.

In [3], the authors present the PKI and the security architecture for a system that gives opticians Internet access from their high street shops to patient data stored in a hospital Diabetes Information System (DIS), using a standard Web browser. The authors show that in a well-designed system the underlying PKI is virtually invisible to the users, and its security is taken for granted in a transparent manner. However, they state that in complex information systems such as their proposed PKI, failure of just one component or administrative procedure can lead to catastrophic effects on the availability of the entire system.

Additionally, in [8] the authors propose the use of Public Key Infrastructure (PKI), Attribute Certificates (ACs) and public key enabled protocols such as TLS in order to provide the appropriate framework to support security services (i.e. authentication, authorization and confidentiality) in mobile online healthcare networks. In other words, this paper proposes a framework which integrates ACs and the TLS protocol in order to support mobile e-health transactions and sustain high level of data confidentiality to the involved entities. Furthermore, the feasibility of the proposed framework is evaluated through extensive experimentation.

In [7], the authors present a hybrid public key infrastructure solution to comply with the HIPAA (Health Insurance Portability and Accountability Act) privacy and security regulations in systems supporting Internet-enabled healthcare applications. The proposed schema is contact based instead of adopting conventional session based cryptographic key management. The presented public key infrastructure can be constructed from existing cryptographic technologies where various relevant security standards, tools and products are available.

In addition, there are many national healthcare PKI systems applied over national health data networks in many countries such as UK and Australia [4]. The major objective of such networks is to provide an integrated environment for efficient delivery of healthcare services within a country.

In [15], it is discussed that Australian government has been exploring how digital certificates issued by a national PKI can act as electronic credentials for a

number of different types of professionals. Especially, in 2006, the Australian federal Department of Health and Ageing commissioned an independent security analysis that strongly endorsed digital certificates for e-prescribing. Moreover, in [15] it is mentioned that in France and Germany, healthcare smartcards are upgraded with PKI-capable chips in order to support new healthcare applications that require patients' signatures.

Finally, MedCom, the national health data network of Denmark, supports a nation-wide PKI system in order to provide user authentication, for both citizens and professionals. It is achieved using Public Certificates for Electronic Services (OCES certificates) issued by the national PKI that can be used in a plethora of national public services. Healthcare professionals can use several OCES certificates: a) administrative digital signature, b) health professional's digital signature based on personal identifier and c) authorization for treating patients [16].

3. Open Issues

There are a lot of open issues regarding the efficient adoption of PKI technology in large-scale healthcare networks involving many communicating parties. First of all, one of the main issues regarding the adoption of PKI technology in such networks is the trust model that will be applied. The choice of the appropriate trust model is of critical importance for the designing of an efficient inter-organizational healthcare PKI infrastructure. Healthcare PKI infrastructure requires the establishment of a trust model on which it can rely and be deployed. The decision of the trust model is conducted from the trust relationships that exist in the environment in which the PKI will be deployed. The trust relationships are based on the organizational (i.e. administrative) structure of the healthcare domain. However, there are many trust concerns associated with subordination between the participating parties in multi-domain PKI infrastructures [2, 10, 13].

Furthermore, the level of complexity of the certificate path processing in a healthcare PKI infrastructure is one more factor that affects the efficient adoption of PKI technology in large-scale healthcare networks. Healthcare multi-domain PKI infrastructures deployed for large-scale networks consisting of many Certification Authorities should keep low complexity of the certificate path processing. Essentially, the certificate path processing includes two main processes; path construction and path validation. Consequently, path construction including the aggregation of all the certificates, which are required to form a complete path from a given target certificate to a trust anchor, should be simple. Additionally, path validation should be performed directly in order to determine if the public key of the certificate can be trusted or not. Especially, path validation is critical in cases of trust extension. However, at the same time the determination of the quality of a given certificate is of utmost importance. End-entities should be provided with information about the Certification Authority (CA) liabilities as well as quality of service parameters of the certificates that the Certification Authority (CA) issues [2, 6, 13].

4. Design of the Proposed Healthcare PKI Infrastructure

The proposed healthcare PKI is focused to be applied on a large-scale Internet-based healthcare network that serves a healthcare domain interconnecting all the healthcare professionals registered to the healthcare units located within a defined large-scale region.

We have assumed that the healthcare domain consists of a wide range of healthcare units (i.e. healthcare stakeholders) including central hospitals, clinics, primary care units, pre-hospital health emergency care units, homecare units and pharmacies. Furthermore, we have assumed that the large-scale Internet-based healthcare network enables communication and exchange of data among the healthcare professionals of the interconnecting healthcare stakeholders. Moreover, we have considered that the healthcare domain follows the hierarchical organizational structure consisting of three levels of hierarchy.

In the highest level of organizational hierarchy, there is a governmental agency of the Ministry of Health. The governmental agency is considered as the national healthcare authority and all the central hospitals and clinics of the network are under its exclusive administrative control.

The second level of the organizational hierarchy involves the central hospitals and the clinics. We have assumed that under the administrative control of each central hospital and clinic there is a number of the pre-hospital health emergency care units, home healthcare units and pharmacies located close to the corresponding central hospital or clinic. Additionally, we have supposed that each central hospital can include under its administrative control primary care units which are located close to it. Essentially, the central hospitals and clinics play the role of the regional healthcare authorities.

Finally, the third level consists of the end-users of all the healthcare units included into the given large-scale healthcare network. We have assumed that the end-users of the included healthcare units are their healthcare professionals. The given large-scale healthcare network comprises a wide range of groups of healthcare professionals including doctors, nurses, administrative staff, pharmacists, support staff and IT staff. Each healthcare professional of the given large-scale healthcare network is registered to a central hospital or clinic. Consequently, we consider that the registered end-users to each central hospital and clinic are their healthcare professionals as well as the healthcare professionals of the primary care units, the pharmacies, the pre-hospital health emergency care units and the home healthcare units that are under administrative control of each central hospital and clinic.

4.1 Proposed PKI Trust Model

Due to the fact that we have assumed that the healthcare domain follows the hierarchical organizational structure, we propose a centralized PKI trust model with hierarchical CA structure. The proposed PKI trust model follows the traditional hierarchical PKI trust model which is based on the establishment of superior-subordinate CA relationships. It can be represented as an inverted tree with the root at the top and the branches extending towards. The elements of the inverted tree are nodes and leaves. The nodes represent the CAs and the leaves represent the end entities. The root is the node located at the top of the inverted tree and is known as the root CA. Below the root CA there are zero or more layers of subordinate CAs. The

root CA is the starting point for trust. It is the "trust anchor" for the entire trust model and issues a self-signed certificate as well as certificates to subordinate CAs that are immediately below it but not to the end users. Subordinate CAs, in turn, issue certificates to other lower level subordinate CAs or end-entities. The certificates issued to CAs are known as CA certificates and the certificates issued to end-entities are known as end-entity certificates [12, 13].

According to the proposed PKI trust model, each central hospital and clinic hosts a regional CA that issues the certificates (i.e. identity certificates and attribute certificates) of its registered end-users (i.e. healthcare professionals). In other words, the regional CA, which is set up into a central hospital or clinic, issues the certificates of the end-users of the corresponding central hospital or clinic as well as the certificates of the end-users of the primary care units, the pharmacies, the pre-hospital health emergency care units and the home healthcare units that are under its administrative control.

Furthermore, the governmental agency of the Ministry of Health hosts the national CA that issues the CA certificates (i.e. identity certificates and attribute certificates) of all the CAs which are set up into the central hospitals and clinics included into the large-scale healthcare network.

The proposed hierarchical trust model, in case that it is applied into a healthcare domain consisting of N central hospitals and K clinics, is shown into the following Figure 1:

Figure 1: Proposed Hierarchical Trust Model

The proposed PKI trust model enables the compartmentalization of risk, management and certificate processing, since it is based on the traditional hierarchical PKI trust model. Thus, it can support the deployment of a more extensible and scalable healthcare PKI. Moreover, each CA is able to embody multiple Certificate Policies leading to a more efficient PKI infrastructure. Additionally, the proposed PKI trust model takes advantages of the hierarchical PKI model's features regarding path construction and path validation processes. Essentially, in the proposed PKI trust model, the path construction process presents low complexity since there exists always a single path from any end-user of the PKI infrastructure up to the root CA (i.e. trust anchor) located within the governmental agency of the Ministry of Health. Hence, the proposed PKI trust model has a great advantage in terms of path construction process complexity against the Bridge CA model that was first introduced by the U.S. Federal Government to facilitate the interconnection of CAs through a cross-certification process. Although the Bridge CA model is quite simple for the end-user, it is characterized by technical difficulties since the path construction is intrinsically complex and several checks must be performed throughout the certification chain [13]. In addition, the path validation process of the proposed PKI trust model is achieved efficiently, since the hierarchical trust models allow the relying party to determine easily if the certificate path is valid [9].

On the other hand, the main disadvantage of traditional hierarchical PKI trust model is the trust issues related to subordination between participating parties. There is not a consensus about who is going to manage the root CA and how the responsible party is going to do it [13]. However, our proposed model addresses this issue introducing the national healthcare authority which is a governmental agency of the

Ministry of Health and everyone is obliged to follow its decisions and policies. Thus, our proposed model is able to address all possible legal and political interoperability issues raised due to the wide range of different PKI trust domains included in the healthcare network where our proposed model is applied.

In addition, the proposed PKI model makes use of Trust Lists which are published and managed by the governmental agency of the Ministry of Health that plays the role of a Trust Provider. The provided Trust Lists allow more efficient determination of whether an end-user that makes a request for healthcare services is trustworthy as well as qualified sufficiently to be provided with the corresponding services according to his/her request. Moreover, the provided Trust Lists are the essential mechanisms that enable the interfacing between any healthcare stakeholder (e.g. hospital, clinic, pharmacy) participating in the healthcare network and any external healthcare organization that is willing to participate in the healthcare network. It is achieved due to the fact that the Trust Lists keep information about each healthcare organization that leaves or joins the healthcare network.

Finally, the proposed PKI model can be implemented using current existing technological PKI solutions provided by companies such as VeriSign and OpenTrust. The main advantage of the proposed PKI model is that it provides the concept of how to design and implement a scalable, flexible and reliable PKI infrastructure for a large-scale healthcare network including multi-domain PKI infrastructures. However, the current existing technological PKI solutions are generic and can be modified efficiently in order to implement a PKI infrastructure that meets the requirements and specifications of our proposed PKI model specified in healthcare networks.

4.2 Architecture of the Proposed PKI Infrastructure

The proposed PKI Infrastructure consists of a wide spectrum of components including identity certificates, attribute certificates, Regional Healthcare Certificate Authorities (RHCAs), a National Healthcare Certificate Authority (NHCA) and Trust Lists.

4.2.1 Certificates

Certificates are the main components of any PKI based infrastructure. In the proposed PKI infrastructure, we have supposed the use of two types of certificates; identity certificates and attribute certificates.

Identity certificates are digital documents used to certify the identity of an entity. Namely, identity certificates verify that a public key belongs to an identity. They bind the identity of an entity to a public key and are digitally signed using the private key of the issuing CA. Identity certificates are the vehicle by which public keys are distributed over unsecured media such as Internet-based networks [1, 9]. In the proposed PKI infrastructure, there are two types of identity certificates; CA identity certificates and end-user identity certificates.

Each end-user identity certificate of the proposed PKI infrastructure incorporates a certificate extension, called NHCA Trust List Link that contains the URL location of the NHCA Trust List including the reliable CA identity certificates of the proposed PKI infrastructure. Additionally, each end-user identity certificate incorporates one more certificate extension, called Identity Certification Revocation List Link (ICRL Link) that contains the URL location of the Identity Certification

Revocation List including the serial numbers of the revoked identity certificates of the RHCA in which the holder of the end-user identity certificate is registered.

Attribute certificates, which are also known as authorization certificates, are digital documents that do not include the subject's public keys. Instead, they carry authorization information associated with the AC holder. An attribute certificate can incorporate attributes (i.e. privileges) that specify access control information (e.g. group membership, role) and other authorization information related to the AC holder. Furthermore, attribute certificates can enable the support and implementation of a critical part of the authorization process.

In the proposed PKI infrastructure, we have supposed the use of two types of attribute certificates; CA attribute certificates and end-user attribute certificates. Both of these types are used for controlling access to the large-scale healthcare network resources and employing role-based authorization policies. Besides, CA attribute certificates include information about the quality of the issued end-user identity certificates.

Each end-user attribute certificate of the proposed PKI infrastructure involves a certificate extension, called NHAC Trust List Link that contains the URL location of the NHAC Trust List including the CA attribute certificates of the reliable CAs. Moreover, each end-user attribute certificate contains a certificate extension, called Attribute Certification Revocation List Link (ACRL Link) that contains the URL location of the Attribute Certification Revocation List including the serial numbers of the revoked attribute certificates of the RHCA in which the holder of the end-user attribute certificate is registered.

The incorporated links in the end-user identity certificate and the end-user attribute certificate are shown in the following Figure 2:

Figure 2: Incorporated links in the end-user certificates

4.2.2 Regional Healthcare Certificate Authorities (RHCAs)

One RHCA is set up in each regional healthcare authority (i.e. central hospitals and clinics) included in the large-scale healthcare network. Each RHCA includes three main components; the Regional Identity Certificate Authority (RICA), the Regional Attribute Certificate Authority (RACA) and Regional Registration Authority (RRA).

Regional Identity Certificate Authority (RICA): Each RICA is configured to issue, renew and revoke identity certificates for the end-users registered to it. Each RICA issues end-user identity certificates to the end-users who are able to prove their identity. Namely, the RICAs of the large-scale healthcare network issue doctor identity certificates, nurse identity certificates, administrative staff identity certificates, support staff identity certificates and IT staff identity certificates. Moreover, the RICAs issue the identity certificates of the end-users of the pre-hospital health emergency care units, home healthcare units and pharmacies. Finally, only the RICAs of the central hospitals issue also the identity certificates of the end-users of their primary care units. All the issued end-user identity certificates of each RICA are distributed to the eligible end-users. Essentially, the RICA of each central hospital or

clinic plays the role of the root CA for the end-users registered to the corresponding central hospital or clinic.

Furthermore, each RICA is responsible to inform the end-users when end-user identity certificates issued by it are no longer valid. For instance, an end-user identity certificate may become invalid before the normal expiration of its validity period in case that the end-user changed his personal information or the private key associated with the certificate is compromised. Under such circumstances, the RICA revokes the identity certificate by listing its serial number on a list, called Identity Certification Revocation List (ICRL). An end-user is allowed to have access to the ICRL of any RICA using the ICRL Link embodied in each end-user identity certificate.

Regional Attribute Certificate Authority (RACA): The RACA issues end-user attribute certificates for the end-users registered to it based on their specific requirements and needs. In other words, RACAs play a significant role to control the access to the stored information, the role of the accessing end-user and the type of information use. Each end-user attribute certificate contains authorized end-user's attributes and binds them to the end-user identity certificate. An end-user attribute certificate verifies that the holder possesses a value for a given attribute (e.g. qualifications, permissions, authorities granted) in order the holder to obtain the required healthcare services. Consequently, in the proposed PKI infrastructure, due to the attribute certificates each end-user is assigned a set of specific rights that governs the permissions required to accomplish his/her tasks. Furthermore, each end-user can possess different attribute certificates associated with different purposes of use in different situations. The issued end-user attribute certificates of each RACA are distributed to the eligible end-users. Additionally, in the proposed PKI infrastructure, each RACA is responsible to verify the validity of the end-user attribute certificates and revokes attribute certificates in case that they are no longer valid, compromised or lost. The end-user attribute certificate validity period is based on the validity period of the end-user identity certificate. Each RACA revokes the end-user attribute certificates by listing their serial number on a list, called Attribute Certification Revocation List (ACRL). An end-user is allowed to have access to the ACRL of any RACA using the ACRL Link embodied in each end-user attribute certificate.

Regional Registration Authority (RRA): Finally, each Regional Registration Authority (RRA) is responsible for gathering certificate requests from the potential end-users of the corresponding central hospital or clinic and checking their credentials in order to verify identity of the applicant.

4.2.3 National Healthcare Certificate Authority (NHCA)

The NHCA is set up in the governmental agency of the Ministry of Health and consists of the following three national main components; the National Identity Certificate Authority (NICA), the National Attribute Certificate Authority (NACA) and the National Registration Authority (NRA).

National Identity Certificate Authority (NICA): The NICA is responsible for issuing, renewing and revoking CA identity certificates in accordance with one or more Certificate Policies. The NICA issues CA identity certificates only to RHCA set up into the regional healthcare authorities (i.e. central hospitals and clinics) involved

into the large-scale healthcare network and can prove their identity and credentials. In other words, the NICA plays the role of the root CA for the RHCA of the large-scale healthcare network.

National Attribute Certificate Authority (NACA): The NACA is responsible for issuing CA attribute certificates for the RHCA. The CA attribute certificates incorporate qualifying information (i.e. service parameters) associated with the services that the corresponding certificate holder (i.e. central hospitals, clinics) can provide to each end-user.

National Registration Authority (NRA): The National Registration Authority (NRA) is responsible for gathering certificate requests from the RHCA and checking their identity in order to implement the function of registration. Furthermore, the NRA enhances the over scalability of the proposed PKI infrastructure.

4.2.4 Trust Lists

In our proposed PKI infrastructure, the NHCA plays also the role of a Trust Provider and is responsible to publish and manage two types of lists; the National Healthcare CA Trust List (NHCA Trust List) and the National Healthcare Attribute Certificate Trust List (NHAC Trust List).

National Healthcare CA Trust List (NHCA Trust List): The NHCA Trust List is a signed list, including the trusted CA identity certificates of the legal and reliable current RHCA of the PKI infrastructure. Moreover, the NHCA Trust List comprises information that validates the integrity and authenticity of the data included in it. Additionally, the NHCA Trust List is updated every time that a RHCA leaves the PKI infrastructure or a new RHCA joins the PKI infrastructure. Namely, the NHCA Trust List is updated every time that a central hospital or clinic leaves or joins the large-scale healthcare network. Consequently, the NHCA Trust List allows access to the reliable CA identity certificates of the current reliable RHCA at any time that an end-user is involved in an electronic transaction and needs to validate if the issuer of an end-user identity certificate is currently a legal entity. The end-user is allowed to have access to the NHCA Trust List using the NHCA Trust List Link embodied in each end-user identity certificate.

National Healthcare Attribute Certificate Trust List (NHAC Trust List): The NHAC Trust List is a signed list, including the CA attribute certificates of the RHCAs. Similar to the NHCA Trust List, the NHAC Trust List includes also additional information that validates the integrity and authenticity of the stored Attribute Certificates. The major importance of the CA attribute certificate derives from the fact that the relying party is able to interpret the incorporated service parameters of the CA attribute certificate and decide if the issuer is qualified for a given specific purpose. The NHAC Trust List is updated based on the NHCA Trust list. In other words, in case that a CA identity certificate is added/removed in/from the NHCA Trust list, the corresponding CA attribute certificate is automatically added/removed in/from the NHAC Trust List. Finally, the end-user can access the NHAC Trust List using the NHAC Trust List Link embodied in each end-user attribute certificate.

5. Certificate Evaluation Process

In the proposed PKI infrastructure, the certificate evaluation process consists of a number of steps in order to define whether the end-user, who makes a request, is trustworthy as well as qualified sufficiently to be provided the corresponding services according to his/her request. To present the certificate evaluation process, we assume the case that an end-user (i.e. identity certificate holder) of a central hospital intends to get involved in an electronic transaction with another end-user (i.e. the relying party) of a clinic. The required steps of the proposed PKI infrastructure are shown in the following Figure 3:

Figure 3: Certificate Evaluation Process

Step 1: First of all, the identity certificate holder should send his/her identity certificate to the relying party.

Step 2: Upon receiving the end-user identity certificate of the identity certificate holder, the relying party needs to validate if the given identity certificate is not revocated. Thus, the relying party makes use of the ICRL Link incorporated into the received identity certificate and points to the ICRL including the serial numbers of the revocated identity certificates of the RHCA in which the holder of the end-user identity certificate is registered. In case that the serial number of the received identity certificate is stored in this list then the process is stopped. Otherwise, the relying party should validate if the issuer (i.e. the corresponding RHCA) of the end-user identity certificate is currently a legal and reliable authority that he/she can trust. This validation should take place in Step 3, before the appropriate procedures for path construction and path validation take place.

Step 3: The relying party makes use of the NHCA Trust List Link included in the received identity certificate and points to the NHCA Trust List including all the current valid CA identity certificates of all the RHCAs included into the large-scale healthcare network in order to check whether the RHCA issued the end-user identity certificate is still valid and can be trustworthy. In case that the CA identity certificate of the RHCA is not included in the NHCA Trust List, then the RHCA is considered untrustful and the process is stopped. Otherwise, in case that the CA identity certificate of the RHCA is included in the NHCA Trust List, then the RHCA is considered trustworthy and the path construction and path validation processes can take place in order to examine the validity of each certificate of the path. In case that any concern is raised regarding the validity of one or more certificates of the path then the process is stopped. In different circumstances, the identity certificate holder is considered as trustworthy and the procedure is continued in Step 4. in order the relying party to define whether the holder is qualified to be provided the services that he/she request.

Step 4: The relying party should request the attribute certificate of the identity certificate holder in order to be able to decide whether the identity certificate holder is qualified efficiently and has the rights to be provided with the requested services. Additionally, the relying party should request the attribute certificate of the identity

certificate holder in order to be able to decide whether the relying party can provide the appropriate services to the holder of the identity certificate in case that the holder is qualified sufficiently. Regarding the first decision, the CA attribute certificate of the RHCA, in which the holder is registered, should be checked. Furthermore, the second decision is based on the matching of the relying party's attribute certificate and the attribute certificate of the identity certificate holder.

Step 5: The identity certificate holder should send his/her attribute certificate to the relying party.

Step 6: Firstly, the relying party should validate if the received attribute certificate is not revoked. Thus, the relying party makes use of the ACRL Link incorporated into the received attribute certificate and points to the ACRL including the serial numbers of the revoked attribute certificates of the RHCA in which the holder of the attribute certificate is registered. In case that the serial number of the given attribute certificate is stored in this list then the process is stopped. Otherwise, the process is continued in Step 7.

Step 7: The relying party should decide whether the identity certificate holder has the rights to be provided with the requested services. Hence, the relying party uses the NHAC Trust List Link included in the received attribute certificate and points to the NHAC Trust List involving the CA attribute certificates of all the reliable RHCAs included into the large-scale healthcare network in order to access the corresponding CA attribute certificate of the given RHCA and check if the holder has the appropriate rights. In case that there is no concern regarding the rights of the holder, then the matching process of the relying party's attribute certificate and the attribute certificate of the identity certificate holder should take place in order to decide whether the relying can provide the appropriate services to the holder.

6. Conclusion

In this paper, we have proposed a PKI infrastructure to provide secure communication services and exchange of data among healthcare professionals over a large-scale Internet-based healthcare network connecting a wide range of healthcare units dispersed over a wide area. The proposed PKI infrastructure aims at addressing the raised issues related to the deployment of PKI infrastructures over large-scale healthcare networks. It adopts the traditional hierarchical PKI trust model in order to enable the compartmentalization of risk, management and certificate processing. Furthermore, it facilitates the trust issues raised in a large-scale healthcare network including multi-domain PKI infrastructures. Moreover, in the proposed PKI infrastructure, the certificate processing is characterized by low complexity. Additionally, our PKI infrastructure suggests the use of Trust Lists in order to provide a mechanism that allows more efficient determination of whether an end-user that makes a request for healthcare services is trustworthy as well as qualified sufficiently to be provided with the corresponding services according to his/her request. Moreover, at the same time the proposed infrastructure intends to provide scalability, flexibility and reduced administration costs, especially when the number of participating healthcare professionals increases.

Our PKI infrastructure can be also used to support secure healthcare services not only for healthcare professionals but also for patients registered to central hospitals or clinics of a large-scale healthcare network. Patients can be one more group of end-users served by the healthcare network. However, a challenging task is going to be the distribution and storage of the identity and attribute certificates of the patients. A possible solution can be the use of smart cards. Despite the fact that this solution can be feasible for the distribution and storage of the healthcare professionals' certificates, it is impractical for the distribution and storage of patients' certificates because of its cost. This solution is not cost effective since each patient should have a smart card including his/her identity and attribute certificates as well as a smart card reader in case that he/she wants to implement a healthcare transaction from his/her own home. Hence, the secure distribution and storage of the identity and attribute certificates of the patients of a large-scale healthcare domain should take place as a future work.

REFERENCES

1. Adams, C., and Just, M., PKI: Ten Years Later. *Proceedings of the 3rd Annual PKI R&D Workshop*. 69-84, 2004.

2. Al-Nayadi, F., and Abawajy, J. H., An Authentication Framework for e-Health Systems. *Proceedings of the 7th IEEE International Symposium on Signal Processing and Information Technology*. 616-620, 2007

3. Chadwick, D. W., Mundy, D., and New J., Experiences of using a PKI to access a hospital information system by high street opticians. *Computer Communications*. Elsevier. 26: 1893-1903, 2003.

4. Ferreira, A., Cruz-Correia, R., Antunes, L., and Chadwick, D., Access Control: how can it improve patients' healthcare?. *Studies in Health Technology and Informatics*. IOS Press. 127: 65-76, 2007.

5. Gomes, H., Cunha, J. P., and Zúquete, A., Authentication Architecture for eHealth Professionals. Meersman, R., Tari Z. (eds.), *OTM 2007, Part II, LNCS*. Springer. 4804: 1583-1600, 2007.

6. Han, S., Skinner, G., Potdar, V., and Chang, E., A Framework of Authentication and Authorization for e-Health Service Systems. *Proceedings of the 3rd ACM workshop on Secure web services*. 105-106, 2006.

7. Hu, J., Chen, H-H., and Hou, T-W., A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. *Computer Standards & Interfaces*. Elsevier. 32: 274 – 280, 2010.

8. Kambourakis, G., Maglogiannis, I., and Rouskas, A., PKI-based secure mobile access to electronic health services and data. *Technology and Health Care*. IOS Press. 13: 511-526, 2005.

9. Komninos, N., PKI Systems. Douligeris, C., and Serpanos, D. N. (eds.), *Network Security: Current Status and Future Directions*. Wiley – IEEE Press. 409-418, 2007.

10. Lopez, J., Oppliger, R., and Pernul, G., Authentication and authorization infrastructures (AAIs): a comparative survey. *Computers & Security*. Elsevier. 23: 578-590, 2004.

11. Menezes, A. J., Vanstone, S. A. and Van Oorschot, P. C., *Handbook of Applied Cryptography*. CRC Press, Inc. 2004.

12. Polk, W. T., Hastings, N. E., and Malpani, A., Public Key Infrastructures that Satisfy Security Goals. *IEEE Internet Computing*. 7: 60-67, 2003.

13. Rifà-Pous, H., and Herrera-Joancomartí, J., An interdomain PKI model based on trust lists. Lopez, J., Samarati P., and Ferrer, J. L. (eds.), *Proceedings of the 4th European PKI Workshop: Theory and Practice (EuroPKI 2007), LNCS*. Springer. 4582: 49-64, 2007.

14. Voss, H., Heimly, V., and Sjögren, L. H., The Baltic Health Network – taking secure, Internet-based healthcare networks to the next level. Engelbrecht, R. Geissbuhler, A., Lovis, C., and Mihalas G. (eds.), *Connecting Medical Informatics and Bio-Informatics: Proceedings of MIE2005*. 421-426, 2005.

15. Wilson, S., Public Key Superstructure "It's PKI Jim, But Not As We Know It!". *Proceedings of the 7th symposium on Identity and trust on the Internet*. 72-88, 2008.

16. Zúquete, A., Gomes, H., and Cunha, J. P., Authentication of Professionals in the RTS E-Health System. *Proceedings of the First International Conference on Health Informatics*. 72-80, 2008.