This is the published version:


Available from Deakin Research Online:

http://hdl.handle.net/10536/DRO/DU:30008145

Reproduced with the kind permission of the copyright owner.

Copyright : 2007, IEEE
An Authentication Framework for e-Health Systems

Fahed Al-Nayadi and Jemal H. Abawajy
School of Engineering and Information Technology
Deakin University
{fahad, jemal}@deakin.edu.au

Abstract—The high-level sensitivity of medical information mandates stronger authentication and authorization mechanisms to be used in e-Health systems. This paper describes the design and implementation of certificate-based e-Health authentication and authorization architecture. This architecture was developed to authenticate e-Health professionals accessing shared clinical data among a set of affiliated health institutions based on peer-to-peer networks. The architecture had to accommodate specific medical data sharing and handling requirements, namely the security of professionals’ credentials.


I. INTRODUCTION

With increasing mobility of populations, patient data may be distributed over many locations in different electronic healthcare (e-health) systems. Recently, how to access this distributed patient data to provide the best possible care has received attention both from governments, healthcare providers and researchers [5]. Advances in networking technology make it possible to interconnect these independent and geographically distributed e-health systems such that healthcare professionals (i.e., doctors, nurses, etc.) are able to access patient health data and related information from any location at any time. For example, using interconnected e-health infrastructure, data like images and lab results can be communicated rather fast and thus, guarantee an optimized care process. However, given the highly sensitive nature of personal health data, the protection of data integrity, availability, authenticity, confidentiality and privacy as well as compliance with personal data protection regulations are critical factors towards achieving users’ trust and acceptance of e-health systems [6].

While it is important that a way to allow health professionals have access to the necessary patient data and information to do their job the best way, increasing automation of the electronic medical record presents, among others, significant patient privacy and confidentiality issues that could expose the healthcare providers and users to liability. Moreover, each e-health system in the network is independently and autonomously managed by the healthcare providers with authority to control access to their locally managed patient health data and information. In addition, the healthcare providers are responsible for defining access-rules to protect resources and each brings its own set of concerns. Also, legal responsibilities and accountabilities pertinent to health data collection and management are the driving force behind healthcare providers guarding patient data and related information securely.

Therefore, research in secure mechanisms to prevent and protect the confidential information and privacy-sensitive patient data as well as fostering trust between healthcare consumers and providers is paramount in e-health infrastructure. In this paper, we consider the authentication problem for networked multi-team e-health systems. The use of networked healthcare systems is generally controlled by authenticating and authorizing particular users and uses.

Authentication is the process where a networked resource user establishes a right to an identity. Authorization and authentication framework is a necessary tool for deploying and using a reliable, secure and trustworthy e-health system. A large number of techniques may be used to authenticate a user: passwords, biometric techniques, smart cards, and digital certificates. Generally, the authentication methods used should match the value of the data being accessed. It should also correspond to the type and level of access the user is providing. Moreover, a method of user authentication is needed that imposes a minimum additional workload on the user.

In this paper, we propose an authentication framework for distributed and multidisciplinary team e-health systems with multilevel administrative domains. The major goal of this system is to produce a usable authorization system for an environment consisting of distributed resources used by geographically and administratively distributed users. The proposed authentication protocol is based on digital certificates that convey identity, use-constraints, and attributes. The proposed protocol offers a number
of advantages such as user-friendly access to remotely managed patient data and related information, it does not require a vast amount of ongoing maintenance, provides strong authentication and gives confidence that systems are secure. Moreover, it is suitable for fine-grained access control and guarantees user privacy and confidentiality. It also addresses user accountability, with administrators able to investigate if improper use is discovered.

The rest of the paper is organized as follows: In Section 2, we outline the related work. The proposed authorization framework is then presented in Section 3. The conclusion and future work is discussed in Section 4.

II. RELATED WORK

In this paper, we refer to e-health system as healthcare systems and services that are interconnected and can work together easily and effectively, while maintaining patient and professional confidentiality, privacy, and security. We assume a multidisciplinary team environment where patients will be treated by a potentially large team of health providers geographically distributed in various locations.

Each healthcare provider operates autonomously within distinct domain and has different healthcare information systems to support local patient care. The healthcare providers and their systems deal with a whole range of sensitive issues related to patient information such as diagnostic reports, MRI images, pathological test results, diagnosis reports, prescriptions, and so on. In the rest of the paper, we define healthcare professionals (HP) as any person involved in any kind of health care related services that include doctors, nurses, administrative staff, support staff and IT staff.

Since health professionals have to provide a wide range of distinctive services, the roles of various types of HPs differ widely, which requires differentiated access roles to the users of the e-health system. Also, individuals have the right to expect that their identifiable health information will not be disclosed without their express informed consent. Moreover, accessing patient related data must be on-demanding and on need bases. In addition, as the custodian of patient information, each healthcare provider is responsible for protecting patient information in patient database against un-authorised use.

In general, securing distributed systems continues to be an important research challenge. Authentication in such networked e-health system is important and challenging.

Without proper authentication mechanism, the provision, continuity and safety of health care system could easily be compromised. A large number of techniques may be used to authenticate a user and a survey of existing tools showed that there is no single best approach for providing an authentication and authorisation infrastructure for e-health systems [11]. A PKI and smart card based e-Health authentication architecture to authenticate health professionals accessing a regional platform for sharing clinical data among a set of affiliated health institutions on dedicated national health network known as Rede Telemática da Saúde (RTS) is described in [9].

An authorisation and authentication architecture for e-health services system that integrates the role-based method [7] and the attribute certificate (or privilege) based method [3] into the electronic health service system is discussed in [8]. A fingerprint-based model suitable for medical images privacy protection against unauthorised release of images by an authorised recipient is discussed in [10].

Existing approaches are based on technical solutions that are well known in distributed system with a single centralized node controlling the authentication process. The common denominators of these previous approaches are generally strongly biased toward a single individual interacting with a single application. Moreover, those based on digital certificate and public key infrastructures to build and operate authentication or authorisation infrastructure is only adopted the identity certificate. An identity certificate is an electronic document certificate that provides generally recognized proof of identity just like a passport, or other personal IDs. Identity certificates are issued by certificate authorities (CAs) in much the same way as government agencies issue passports after verifying an individual's identity. CAs can be either independent third parties or organizations running their own certificate-issuing server software. The certificate authority generally uses published verification procedures to ensure that an entity requesting a certificate is in fact who it claims to be.

In our previous work, we proposed an e-health infrastructure (E-HP2) [5] that provides integrated services to health care workers that are more broadly accessible by leveraging P2P technology and electronic health records. In E-HP2, a number of healthcare organisations (e.g., doctors, pathology labs, pharmacies and hospitals) willingly collaborate by virtually integrating their information systems. E-HP2 enables health providers to share patient information in a seamless, fault-tolerant and scalable manner. It is
important to note that the provision of infrastructure services is an enabling mechanism. The infrastructure itself will deliver some benefits, but the main outcomes will be achieved by the provision of additional applications and services.

Although there is a merit for easy accessibility of individual's health information by qualified and authorized individuals using P2P network, this could vastly increase the potential for abuse of that patient data and related information. This work extends our previous work by adding an authentication protocol to make the sharing of patient data and related information in a seamless and secure way. However, authentication protocol is more difficult to achieve in a pure P2P network architecture than in a centralized environment. This is because no central server is used to verify a peer's identity.

The proposed protocol is based on a Public-Key Infrastructure (PKI) that supports the issuing and management of digital certificates which identify and authenticate authorized users. When a certificate authority issues an identity certificate, it binds a particular public key to the name of the entity identified in the certificate (such as the name of a doctor). The certificate also has an expiration date, the name of the certificate authority that issued the certificate and other information. Most importantly, a certificate always includes the digital signature of the issuing certificate authority. We also use an attribute certificate (AC) has a data structure comparable to an identity certificate [14]. However, a major difference is that an attribute certificate does not contain a public key. It contains attributes that specify access control information associated with the AC holder (such as group membership, role, and security clearance). Attribute certificates are able to support and implement a significant part of the authorization process. For example, information about a user's current role (e.g. physician) or a client's ability to pay for a resource access may be more important than the client's identity.

III. CREDENTIAL-BASED AUTHENTICATION PROTOCOL

In distributed and multidisciplinary team e-health systems with multilevel administrative domains, authentication of the HPs is a must. In this section, we discuss the proposed authentication architecture and protocol.

A. Authentication Architecture

The interaction of health providers with the system has to be secured through a complex process of authentication and authorization.

Fig. 1 shows the proposed overall operational architecture. We assume that each healthcare professional (HP) is assigned a set of specific rights (roles) that governs the permissions needed to accomplish his/her tasks. We propose the use of remote and local user roles with each requiring different authentication mechanisms. First, the healthcare professionals (HP) must be authenticated to the local e-health system. At the second level, there should be a remote access authentication system. These are achieved through two distinct phases.

Initially, every user obtains an identity certificate. We assume that each autonomous domain has its own Identity Certificate Authority (ICA). We also assume that the ICAs in the P2P trust each other. The ICAs are responsible for the creation, digitally signing and distribution of the identity certificates to users registered in that domain. In a multi-team environment, the issue of managing patient consent to the use and disclosure of personal information is paramount. In this paper, we assume that when a patient visits a hospital, the patient provides his/her consent on the use of her medical data and digitally signs the consent form and the consent form is sent to the local data repository.

For remote authentication, we use attribute and consent certificates to assign attributes and patient data use constraints to HP respectively in a verifiable way. Therefore, the second phase consists of obtaining the consent and attribute certificates. The consent certificate will impose use-conditions on the patient data. All of the use-conditions must be met simultaneously in order to satisfy the requirements for patient data access. An attribute certificate certifies that the user possesses a value for a given attribute. An attribute describes a property associated with an individual such as information that describes the qualifications and authorities granted to the target entity. Each attribute

618
Attribute certificate validity period must be within the validity period of the identity certificate. A HP may possess different attribute certificates related to different validity intervals or even different purposes. It must be noted that, generally speaking, attributes are subject to change according to each situation. For example, the rights of HPs usually consist of both static and very dynamic permissions. As a result, the content of attribute certificates varies from case to case. Basically, static permissions are issued by health authorities, dynamic permissions may be issued even by hospitals and clinics. Static qualification and authorization attributes can also be connected with dynamic permissions and admission, for example by a supervisor or administrator within the IT environment of a hospital.

The system uses the attribute certificate authority (ACA) and the individual consent certificate authority (CCA) to control access to information content based on personal consent, the role of the information-accessing entity, and the type of information use. ACA issues attribute certificate that contains authorized person’s attribute and binds to one’s public key certificate. It also verifies the validity of attribute certificate as well as revokes attribute certificate in case of the attribute is changed or is lost.

The CCA maintains and serves information about the consent given by individuals about the use of their personal health information. We assume that patients are able to review and adjust consent information through a web-based interface. The gateway (GW) node at each participating healthcare provider runs the policy engine that determines, based on the roles assigned to HP, the users’ rights with respect to the requested access to healthcare data and resources. Since we focus on remote exchange of healthcare data between different healthcare providers, we will not discuss the local authentication protocol in this paper.

B. Authentication Protocol

Fig. 2 shows the steps performed in the proposed authentication mechanism. Specifically, when HP initiates a new session for remote data request; he/she must first identify and authenticate themselves, with the local gateway (LWG) server, by using their IC and password. The validated IC of the user is then used by the GW to gathers up all the relevant certificates, depending on the responsibility/authority of the HP roles activated by the request. The GW also ensures that the HP has the need for the information sought. This step produces a short-lived attribute certificate with a subset of HP roles from a set of initially assigned roles, which are needed to accomplish specific tasks.

The HP will then send to the remote gateway (RGW) a request for data (R) along with the attribute certificate (AC) and consent certificate (CC). When the RGW receives the access request from the health professionals, it sends the attribute certificate and the consent certificate to the local attribute certificate authorities (ACA) and consent certificate authorities (CCA) for verification respectively. These certificate authorities generally use published verification procedures to ensure that an entity requesting the data is in fact who it claims to be. Attribute verification is the process of establishing an understood level of confidence that an attribute applies to a specific individual. The result of the verification step is used by the authorization step which is outside the scope of this paper.

![Authentication protocol](image)

IV. CONCLUSIONS AND FUTURE DIRECTION

Medical data security is an important issue that poses technical, organisational and ethical challenges. In this paper, we proposed two-level authentication protocol for P2P-based e-health system that provides integrated services to health care providers. The proposed authentication framework is based on identity, attribute and consent certificates that together uniquely identify the HP as well as the roles and accesses associated and constraints imposed on the healthcare data usage. The proposed protocol offers a number of advantages including a user-friendly and strong authentication and gives confidence that systems are secure. We plan to extend the proposed approach such that it is able to delegate and recognize delegated credentials. We also plan to extend it such that a single-sign on capability is realized.
REFERENCES