A Hierarchical Model for Cross-Domain Communication of Health Care Units

Dimitris Geneiatakis[1], Costas Lambrinoudakis[2] , Stefanos Gritzalis[2]

[1] *Dept. of Telecommunications Science and Technology, University of Peloponnese*
End of Karaiskaki St., GR-22100, Tripolis, Greece
email: dgen@uop.gr

[2] *Dept. of Information and Communication Systems Engineering,*
University of the Aegean, Samos GR-83200, Greece
Tel: +30-22730-82224, Fax: +30-22730-82009
email: {clam,sgritz}@aegean.gr

Abstract [1]

Common practice for healthcare organizations is to maintain locally their own files, thus causing a geographic distribution of healthcare records. On the other hand, healthcare personnel treating a patient needs access to previous diagnosis and treatment data, maintained by various institutions in many different locations. Currently, the lack of a reliable authentication and authorization framework is considered a major obstacle for interchanging Electronic Healthcare Records (EHRs). This paper proposes a hierarchical model for controlling access to EHRs and protecting the privacy of subjects of care and healthcare personnel, while facilitating the exchange of information among healthcare information systems.

1. Introduction

Healthcare has always been a favoring area for the application of Information and Communication Technologies (ICT) and healthcare organizations were among the first to incorporate information systems in their operation. Following the trend, Health Information Systems (HIS) have followed an evolutionary course leading to a new generation of eHealth systems. Personalization of service, ubiquitous information management, integration of intelligent and communicating devices are only a few of the new features that HIS are expected to embed in the near future. Moreover, HIS store and process information, which is characterized as highly sensitive. Therefore, privacy and security have been acknowledged as high-priority issues and critical factors for the adoption and effective integration of ICT in the healthcare sector [8].

Healthcare records are distributed in various locations, as each Healthcare Organization keeps its own files. However, medical personnel treating a patient often needs access to previous diagnosis and treatment data, which are kept in different locations and/or by various institutions. One possible solution would be to develop a central medical databases (e.g. at National level). This approach has, at least, two serious disadvantages: (a) the privacy of patients and healthcare professionals is seriously jeopardized and (b) the administrative burden of keeping such a central database is huge. The other alternative is to explore ways for interconnecting HISs and at the same time ensure that only authorized people access the information. Standardization organizations have issued standards that support the development of interoperable Healthcare Information Systems (HIS) and the exchange of Electronic Healthcare Records (EHRs). In Europe, CEN (European Committee for Standardization) has developed a series of such

[1] The work presented in this paper has been conducted in the framework of a National project, funded my the Greek Ministry of Health, regarding the utilization of smart cards for authentication and authorization purposes (e.g. accessing EHRs) as well as for communicating information between doctors, insurance companies, pharmacies and the patient (e.g. prescriptions).

standards[2] [7]. In terms of the access control mechanisms currently employed by most HISs, in order to control access to EHR, they are mainly based on the Discretionary Access Control (DAC), Mandatory Access Control (MAC), or the Role Based Access Control (RBAC) models [10]. The latter appears to be the most relevant of the three for the HIS case [27] and is currently being applied to XML documents, achieving the incorporation of RBAC authorization policies to portable documents [9,11].

However, authorization decisions in interconnected co-operating HISs are far more complex, requiring the assessment of several factors, such as the position of the requesting agent in the healthcare organization, his/her specialty, his/her relation with the subject of care, the purpose of use, the location of the requesting agent (e.g. in a country that does not have adequate legal protection for personal information), the content of the EHRs and the level of trust on the credentials provided by the requesting agent, as well as the reliability of the information in the EHR.

Consequently, Health Care Units (HCU) develop domain specific policies to provide security services on EHR. Even though the same policy specification e.g XACML [1] (a medical purpose medical language) may be utilized by different HCU domains the establishment of the appropriate level of trust between them cannot be assured. For example, consider the case in which an entity (e.g doctor) that belongs to HCU in domain A requests access to a specific HCU resource belonging to a different domain B. Though domains A and B have implemented the same security policy, a secure communication link among them can not be established due to the lack of trust between them. In this paper we elaborate on the establishment of the appropriate trust level among nodes with no pre-established relationships. Specifically, the proposed solution is based on a two layer hierarchical architecture for establishing the appropriate level of trust.

The rest of the paper is organized as follows: Section 2 provides a brief survey of existing security and access control mechanisms in healthcare architectures. Section 3 briefly describes the security requirements for interconnected EHR systems. Section 4 presents a security architecture suitable for medical environments, while Section 5 introduces a method to elaborate on the development of trust between "unknown" domains, utilizing the proposed architecture. Section 6 presents a qualitative comparison of the proposed architecture with other similar solutions. Finally, Section 7 concludes the paper by summarizing the characteristics of the proposed security architecture and by providing pointers to future work.

2. Related Work

Access control mechanisms in healthcare environments play an important role for the protection of patient's sensitive data, like EHR, against unauthorized access and/or modification and that is why many researchers, all around the world, focus on the provision of such services. However, all of them study / propose access control mechanisms for a single HCU domain. Moreover, none of them takes into account the security requirements that should be fulfilled for establishing the appropriate level of trust among interconnected collaborating HCU domains. Equally important is the protection of the patient's privacy, another issue that currently lacks the attention of existing security solutions for HCU domains. In [16] the privacy implications of single sign on authentication are analyzed, while [17] presents a solution that covers both the security and privacy requirements that have been considered necessary.

For enhancing the security level "inside" an HCU domain, [12] and [13] suggest the utilization of existing commercial security solutions and services like Secure Socket Layer (SSL) [5], Internet Protocol Security (IPSec) [22], firewalls and intrusion detection systems. While such mechanisms/solutions protect EHR integrity and confidentiality during transmission, supplementary solutions were required in order to "ensure" that access to EHR is only granted to authenticated and authorized entities. To this direction, a number of authentication and authorization systems for HCU have been proposed.

As far as the authentication solutions are concerned, they were initially based on passwords but due to the various limitations of these systems [24],[25] the utilization of single sign on mechanism has been recommended [14],[15]. Authorization systems are mainly based on DAC, MAC or RBAC models. On top of that recent research work focuses on mapping frameworks that can achieve role integration between different administrative domains by translating or mapping roles from one domain to the other [18]-[21].

Beyond and above current research work, countries all around the world have developed their security solutions for HCUs, taking into account their specific legal and regulatory framework. An overview of these solutions can be found in [26].

[2] It should be noted that these standards mainly focus on the interoperability of EHR structure.

3. Security Requirements for Interconnected EHR Systems

Some of the key issues that must be carefully considered prior to the design of a security architecture for interconnected EHR systems are the following [2,3]:

- The interconnection of EHR systems facilitates the collaboration of independent HCU, each unit remaining sovereign in its own domain and defining its own security policy. However, users in one domain may ask to access information in any other domain.
- The network of interconnected sites is not static. New HCU may join the network at any time.
- There is no central authority administrating or even enforcing a common policy to all interconnected sites.
- The fact that medical information can be accessed from some unknown remote location, possibly belonging to a different domain and thus exhibiting a different security policy, imposes the need to treat the data in accordance to specific security attributes (policies) attached to it.
- No predefined trust relations among individual health care units or groups of units can be assumed. Trust evaluations should be dynamic.

Taking into account the above characteristics, which render most of the current commercial security solutions inapplicable, the security requirements that have been identified are listed next:

- Each HCU should have the freedom to design its own security policy and to enforce it within its domain. Through the interconnection of different domains a multiple-security-policies environment [4] will emerge. Consequently, several policy conflicts may occur, posing the need for a 'resolving' mechanism.
- Static and rigid security policies, based on the currently dominant "subject-to-object" paradigm are not suitable. The requirement is for policies that are context-aware and adaptable.
- The integrity and confidentiality of medical information should be ensured.
- Medical records, when communicated to remote health care units (different domains), should be protected through their own access control policy.
- Users should be authenticated in their local EHR systems (local domain). When they request authorization to access resources in some remote system they should not be asked to re-submit their credentials or to provide any additional ones.
- Single-sign-on capability should be provided.
- All security mechanisms should be transparent to the users.

4. A Two Layer Hierarchical Healthcare Architecture

Although, one of the security requirements identified for interconnected EHR system was to avoid the existence of a central authority enforcing a common policy to all interconnected sites, we argue that every HCU is part of a general health care hierarchical structure. Specifically, the establishment of the appropriate level of trust between communicating parties is based on the assumption that we have a model with two hierarchy levels: a) the local level and b) the global level. For instance, the local-level could represent the communication paths and trust relationships among HCUs at National level (thus representing the structure of the National Health Care System), while the global level the communication paths and trust relationships among different regulation domains (e.g different countries). Note that even though we identify two hierarchical levels, for management reasons the nodes of each level could be re-organized also in hierarchical topology. Figure 1 depicts the proposed architecture.

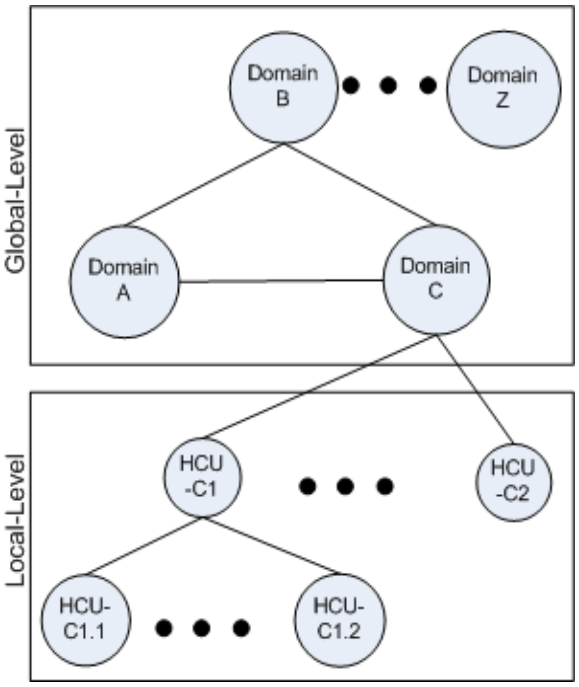

Figure 1. The Proposed two-level Hierarchical Architecture

Figure 2 illustrates a simple example of how the proposed architecture could be applied to the Greek health care system. For the purposes of this example we assume that on the global hierarchical level we have other European countries.

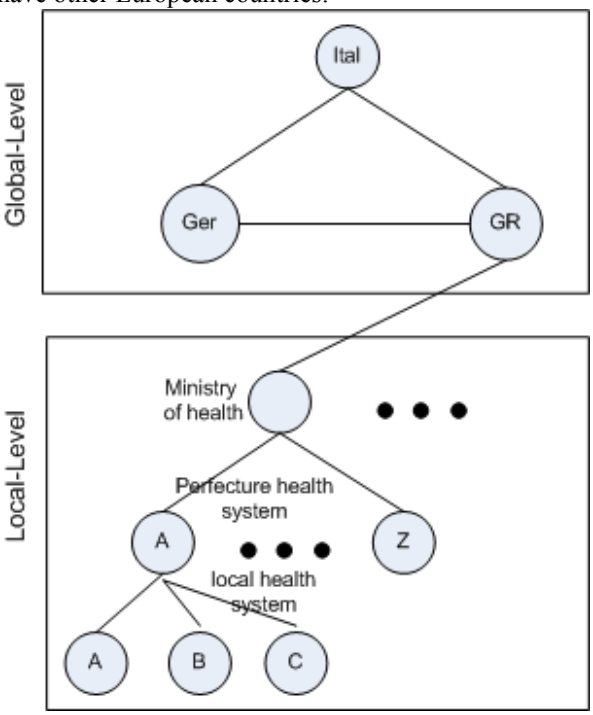

Figure 2. An example of the Proposed Architecture

One could argue that there is no reason to employ such an architecture, as the HCUs could dynamically generate the appropriate communication and trust paths between them. However, the relationships that a specific HCU should manage in order to ensure trust among all the available HCUs is (n * (n -1)) / 2 (where n is the number of HCUs). With the proposed architecture a node requires to manage a trust relationship only with its ancestor. Even when managing trust relationships at the global, where the number of relationships is (n' * (n'-1)) / 2, it is much smaller than the relationships required in a single dynamic environment as n>>n'.

5. Trust Establishment & Access Control

In order to establish the appropriate level of trust among the communicating entities of the proposed architecture, every node should posses a valid certificate. At the global level certificates are issued by a common trust certification authority, while at the local one, ancestor nodes are responsible to issue the appropriate certificates for descendant nodes. It should be stressed that in the proposed architecture there is not a complete chain of trust between all nodes in the hierarchy; instead we assume that a node trusts only his neighbors (parent & child). Consequently, the issued certificates instead of including all ancestor certificates, developing a complete chain of trust, embeds only its ancestor certificate, creating one hop chain of trust. Besides, with this approach the size of the certificate remains fixed (independent of the height of the hierarchy). However, the main problem in the case of one hop chain of trust is that it does not support trust establishment among distant domains. For instance, an entity with a specific role (e.g doctor) belonging to a health care unit of domain A (see Figure 2) may request access to a health care unit of domain Z. Due to the lack of pre-established trust between these domains the access is not allowed.

According to our approach in such cases the entity generates a request that consists of a) the entity's certificate b) the requested resource, and c) the request's (certificate, resource) digital signature.

It is important to stress at this point that in order to protect the privacy of the patient, the social security number, that is part of the initial request, as well as any medical data transmitted from one domain to the other are encrypted with the public key of the destination HCU. In this way only the requesting HCU can decrypt patient's EHR ensuring her privacy.

After the entity has signed the request it forwards it to its parent node, which in turn a) validates the signature and b) signs the incoming request (assuming

that the validation was successful). Irrespective of whether the request belongs to the administrative domain of the parent node or not, every processing node must follow the same procedure with the initial parent node, until the request reaches its final destination.

Assuming that the request is successfully validated by all nodes in the path, the trust relationship among the requesting entity and the requested resource has been established. As part of the trust establishment procedure, the final destination node (FDN) issues a response message consisting of the initial request and a session ticket encrypted with the requesting entity's public key (retrieved from the certificate which is included in the initial request). Moreover, for integrity reasons this response message is signed by the FDN, and is then forwarded to the appropriate node. The procedure followed for delivering the response message to the requesting entity is exactly the same with the delivery of the request. As soon as the requesting entity receives the response, it validates it and decrypts the issued session ticket in order to communicate directly with FDN (employing some symmetric algorithm and the session ticket for encrypting the data exchanged). The aforementioned procedure is depicted in the Figure 3.

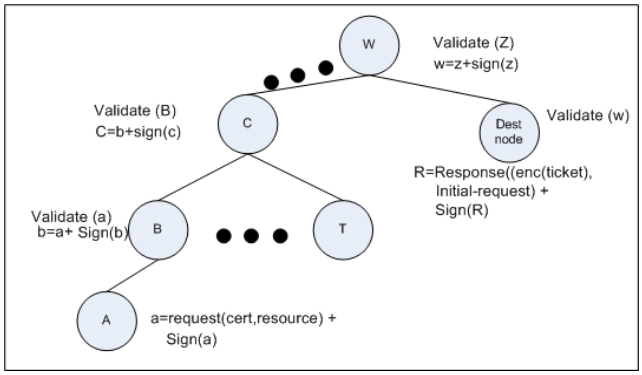

Figure 3. Suggested Trust Establishment & Access Control Procedure.

In cases where a trust relationship among HCUs belonging to different regulation domains (i.e. different countries - see Figure 2) is required, the trust establishment procedure at the local level remains the same while at global level it is achieved through secure socket layer (SSL) [5].

As far as the communication cost for trust establishment is concerned it requires at most 2(n-1) communications, while the maximum size of the request is

(2*(n-1)) * sizeof(signature) + sizeof(request).

As far as the overhead introduced is concerned, it is considered negligible since, according to [24], the average time for creating and validating a digital signature is less than 70 millisecond for a computer system with a Pentium 4 @ 1GHz processor and 128 MB of RAM. In the proposed scheme the delay introduced is influenced directly by the number (n) of intermediate nodes between the communicating parties. Consequently, the overall delay introduced is approximately: 2*(n-1)*70 milliseconds.

Table 1 overviews the evaluation of the proposed scheme.

Communication Cost	2*(n-1)
Computation Cost	2*(n-1)*(validation_time+sign_time)
Size	(2*(n-1))*sizeof(signature)+ sizeof(request).

Table 1. Performance Evaluation of the Proposed Scheme

Besides, in order to achieve efficient management of the distinct responsibilities and privileges of the entities involved in the health care environment, each entity is assigned a specific role. For this reason, roles should be included, as attributes, in the certificates issued, as suggested in [6]. Note that if a specific role does not exist in the requested domain, the processing node is compelled to traverse the hierarchy up to the top-level node, which is responsible to resolve this type of conflicts.

Moreover, mobile HCUs can join the proposed architecture (at the local-level) by presenting to the appropriate node a special purpose "join certificate", issued by the top level hierarchy node, signed with its private key. The responsible node requests a validation of the "join certificate" by its ancestor. If the ancestor is the top level hierarchy node validates the certificate and responds with a verification message to the requesting node. Otherwise, the ancestor validates the signature of the join-request and forwards it to its ancestor in a fashion similar to the procedure described for trust establishment among HCUs belonging to different domains.

6. Qualitative Comparison

As already mentioned in Section 2 there are many different approaches / proposals for providing the appropriate HCU security services. Although these solutions have been designed with different characteristics in mind, all of them aim to improve the security level of the HCU environment. In order to facilitate a comparison among these solutions and the

proposed one we consider the following characteristics:

- Type of Cryptography System (**S**ymmetric/**A**symmetric/**P**assword Based)
- Need for Pre-established Trust (Yes/No)
- Provided Security Services (**C**onfidentiality / **I**ntegrity / **A**uthenticity / **Au**thorization)
- Architecture (**C**entral/**D**istributed/**F**ederated)
- Supporting the Interconnection of Different HCU Domains (Yes/No)
- Privacy Protection (Yes/No)

Table 2 highlights how the above-mentioned characteristics are satisfied by existing HCU security solutions and the proposed mechanism. Solutions [12],[13],[17] utilize both symmetric and asymmetric cryptosystems for providing confidentiality, integrity and authenticity, while [14],[15] provide a single sign on system for user authentication that relies on a password scheme. However, in these solutions there is no explanation of how interoperability/interconnection between two different HCU domains could be established. Even solutions [18]-[21] that focus on the interconnection of different domains, it is assumed that a trust relation among the communicating parties pre-exists (for this reason the "Yes" is marked with asterisk symbol).

Finally, as already explained in section 5, only the proposed solution takes into account and protects patient's privacy.

7. Conclusions & Future Work

The increased patient mobility, combined with the fact that different health care items are frequently offered by different health care units, have resulted in the development of distributed electronic health care records. Although such systems facilitate access to the entire medical history of the patient, it is not straight forward to design and implement security mechanisms for ensuring the confidentiality and integrity of the data or/and the privacy of the patient, without limiting the communication of information between health care professionals and sacrificing system flexibility. In this paper we have described a security architecture that can support distributed systems, focusing on authentication and authorization issues in a multiple-security-policies environment (interconnection of different security domains).

Specifically, in the proposed architecture each domain remains independent and autonomous to determine its own security policy. Besides, trust and access is accomplished dynamically utilizing one hop chain of trust. Assuming successful establishment of trust between nodes, communication is protected through encryption that utilizes a session ticket. This specific session ticket could be also utilized for realizing single sign-on functionality in the domain. However, this issue requires further investigation.

	[12]	[13]	[14]	[15]	[17]	[18]	[19]	[20]	[21]	Our
Type of Cryptography System	A/S	A/S	P	P	A/S	None	None	None	None	A/S
Pre-established trust	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No
Architecture	C/D	C	C	C	C	C	C/D	C	C	C/D
Interconnection Support	Yes	Yes	No	No	No	Yes*	Yes*	Yes*	Yes*	Yes
Provided Security Services	C/I/A	I/A	A	A	C/I/A	None	Au	Au	Au	C/I/A
Privacy Protection	No	No	No	No	No	No	No	No	No	Yes

Table 2. Qualitative Comparison between Existing HCU Security Solution and the Proposed one

8. References

[1] Organization for the Advancement of Structured Information Standards (OASIS), "Extensible access control markup language specification 1.0", OASIS Standard, November 2002 (available at www.oasis-open.org).

[2] Blobel B., "Security requirements and solutions in distributed Electronic Health Records", in Proc. of the 13th IFIP International Information Security Conference (SEC-1997), 1997.

[3] Blobel B., Katsikas S., "Patient Data and the Internet: Security Issues", Proc. of the IMIA Conference on Common Security Solutions for Communicating Patient Data, 1997.

[4] Kokolakis S., Kiountouzis E., “Achieving interoperability in a multiple security policies environment”, Computers and Security, Vol. 15, No. 3, September 2000.

[5] Dierks T., Rescorla E., “The Transport Layer Security (TLS) Protocol”, RFC 4492, 2008.

[6] Farrell, S. and Housley, R. “An Internet Attribute Certificate Profile for Authorization“, RFC 3281, 2002.

[7] Kokolakis S., Lambrinoudakis C., “ICT Security Standards for Healthcare Applications”, Upgrade electronic journal (www.upgrade-cepis.org), Special Issue: Standardization for ICT Security, Vol. 6, No. 4, 2005.

[8] European Parliament and the Council of the EU. Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, Official Journal of the European Communities, 1995; L281/38.

[9] Damiani, E., Samarati, P., di Vimercati, S. and Paraboschi, S. Controlling access to XML documents. IEEE Internet Computing, 5(6):18-28, 2001.

[10] Jajodia, S., Samarati, P., Sapino, M.L. and Subrahmanian, V.S. Flexible support for multiple access control policies. ACM transactions on database systems, 26(2):214-260, 2001.

[11] Kudo, M. and Hada, S. XML document security based on provisional authorization. Proc. 7th ACM Computer and Communication Security, ACM Press, New York, pp.87-96, 2000.

[12] Ruotsalainen, P., "A cross-platform model for secure Electronic Health Record communication", International Journal of Medical Informatics pp. 291-295, 2004

[13] Kailar, R. , Muralidhar, V., "A Security Architecture for Health Information Networks", American Medical Informatics Association (AMIA) Symposium, Chicago, 2007

[14] Heckle R., Lutters W. G., Gurzick D., "Network Authentication using Single Sign-On: The Challenge of Aligning Mental Models", Computer Human Interaction for Management of IT (CHIMIT'08), San Diego, CA, U.S.A, 2008

[15] Yanjang Yang, Deng R. H., Bao F., "Fortifying Password Authentication in Integrated Healthcare Delivery Systems", in proceedings of ASIAN ACM Symposium on Information, Computer and Communications Security, (ASIACS '06), 2006

[16] Rosa R. Heckle, Wayne G. Lutters, "Privacy Implications for Single Sign-on Authentication In a Hospital Environment" in proceedings of Symposium On Usable Privacy and Security (SOUPS), 2007

[17] Jiankun, H., Hsiao-Hwa C., Ting-Wei H., "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations", Computer Standards & Interfaces, 2009

[18] Sartipi, K., Dehmoobad A. "Cross-Domain Information and Service Interoperability", 10th International Conference on Information Integration and Web-based Applications & Services, 2008

[19] Gritzalis, S., Belsis, P., Katsikas S. K, "Interconnection Autonomous Medical Domains: Security, Interoperability, and Sematinc Driven Perspectives for Electronic Health Records", IEEE Engineering in Medicine and Biology Magazine, 2007

[20] Sucurovic, S., Simic D., "An Approach to Access Control in Electronic Health Record", Journal of Medical Systems, 2009

[21] Bhatti, R., Moidu, K., Ghafoor A., "Policy-Based Security Management for FedPolicy-Based Security Management for Federated Healthcare Databases (or RHIOs)", in proceedings of Fourth International Conference on Autonomic and Autonomous Systems, International Workshop on Healthcare Information and Knowledge Management (HIKM’06), 2006

[22] Thayer, R., Doraswamy, N., Glenn R., "IP Security Document Roadmap", RFC 2411, 1998

[23] Kambourakis G., Rouskas A., Gritzalis S. and Geneiatakis D., "Support of Subscriber's Certificates in a Hybrid WLAN-3G Environment", Computer Networks, Vo. 50, No. 11, pp. 1843-1859, 2006, Elsevier.

[24] Adams, A., and Sasse, M.A, "Users are not the enemy", Communications of the ACM 42 (12), 20-46, ACM

[25] Ives, B., Walsh, K.R and Schneider, H., "The domino effect of password reuse", Communications of the ACM, 47 (4), pp. 75-78, ACM

[26] Blobel, B., "Comparing approaches for advanced e-health security infrastructures", International Journal of Medical Informatics, Volume 76, Issue 5, pp. 454-459, Elsevier

[27] Zhang, L., Ahn, G-J and Chu, B-T. "A role-based delegation framework for healthcare information systems", in proceedings of SACMAT'02, ACM Press, June 2002.