The New Navigators: from Professionals to Patients
R. Baud et al. (Eds.)
IOS Press, 2003

A New Concept for an Integrated Healthcare Access Model

Carlos Costa [a], José Luís Oliveira [a], Augusto Silva [a], Vasco Gama Ribeiro [b]

[a] *University of Aveiro, Electronic and Telecommunications Department / IEETA, 3810-193 Aveiro, Portugal*
[b] *CHVNG, Cardiology Department, V. N. Gaia, Portugal*

Abstract

The increase of population mobility has been promoting a crescent dispersion of patient clinical records in Healthcare Information Systems. In this scenario, it is mandatory that new services will be available for healthcare practitioners, namely web-based interfaces with strong control access mechanisms providing effective authentication and identification of persons, and the establishment of new access models to the disperse patient information.

This paper proposes and describes a Healthcare Access Model that integrates a new set of functionalities coping with patient mobility and implements an innovative concept of a virtual unique Electronic Patient Record - EPR.

Keywords:

Healthcare Information Systems (HIS), Distributed HIS, Authentication, Patient Data Card (PDC)

1. Introduction

The Medical Informatics expression appeared some decades ago associated to the first applications for specific medical issues [1]. During this time many applications have been built in the field, supported by different technologies and materials.

Looking to the clinical process at a macroscopic view we realise that patient data is generated, manipulated and stored along several institutions where the patients are treated. In this heterogeneous and complex scenario, sharing and remote access to patient information is capital for health care best practices.

The first step towards this policy was done by the worldwide adoption of digital clinical processes and of the Electronic Patient Record (EPR) concept. The information is collected, archived and distributed, in digital formats replacing traditional paper-based recording and providing healthcare services with improved quality and efficiency. However, one of major problems is the lack of interoperability between Healthcare Information Systems (HIS).

When the sharing of clinical information must cross an administrative domain, such as a hospital, new problems have to be solved, namely it is necessary to establish normalized interfaces between HIS. Besides the conformity on the interfaces, efficient and robust security mechanisms must be adopted for the success of this internetworking.

If security is granted and political constraints solved, healthcare can take full advantage of Web technology and Internet to allow widespread sharing and remote access of medical data between healthcare intervenient'.

Currently, web services in healthcare are mainly related to information search (such as MEDLINE). However, this infrastructure has an enormous potential for developers, practitioners and patients. While Internet has been largely adopted in diverse business areas, the healthcare sector is making short and careful steps towards this community. While physicians were the initial target users of web-based medical applications, patients are also demanding new applications to improve their knowledge.

Many pertinent questions related with functional, legal and ethical aspects must be addressed to the wide adoption of web-based healthcare information systems:

- The proof and authentication of patient, in a strong way.
- The adequate profile to a specific remote health care professional.
- The access to the historic clinic data of a patient in a fast and transparent way.
- Possibility to select the required information in a huge and distributed EPR.
- The accomplishment of a trust relation between health care institutions, professionals and patients.

Besides several technological solutions can fit in some of the above questions, the resolution of the overall problem in a unique and consistent manner remains an open issue.

This paper proposes a functional model (Figure 1) that aims to fill the previous enumerated gaps. The main motivation associated to the model is the provisioning of a secure access mechanism that (based upon a distributed HIS) presents a virtual unique EPR.

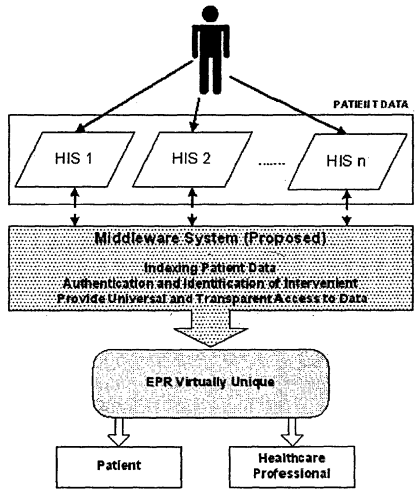

Figure 1: The virtually unique EPR.

2. Materials and methods

Trust establishment and security in healthcare environment are not new concepts. In the last years several projects have produced some guidelines for normalization [2]. The HARP project [3] is an important example studying the establishment of Shared Care environment in a trustworthy way between healthcare institutions in open and heterogeneous environments.

In the E-World, it is crucial for individuals and entities the capability of mutual identification in a unique way. In HIS the necessity for user identity proof and strong authentication are fundamentals to grant an efficient security policy. However, the reality tells us that current HIS strategy of security remains often based on primitive processes as the simple authentication with username and password. Data transmission can be protected through mechanisms like IPSec, SSL and TLS. Nevertheless, the authentication trust still largely based in insecure knowledge factor, often predictable, making impracticable the implementation of effective security services like data privacy, integrity, and non-repudiation of clinic acts/actions.

A Digital Credential is an excellent tool for performing identification and authentication in digital transactions. A Digital Certificate, which relies heavily on Public Key Cryptography (PKC), establishes a trust relationship between its designated subject (the user) and the holder of a secret cryptographic key by means of the issuing organization, a reliable certification authority (CA). One the most secure and flexible way to store sensitive information, such as personal details or cryptographic keys, is through the use of smart cards [4] [5]. This technology, when correctly combined with emerging technologies, like biometrics, can strongly enforce access control through personal identification and authentication [6].

The proposed model was developed in cooperation with the CHVNG Cardiology Department and takes advantage of previous technological solutions and know-how obtained in several projects in areas such as PACS [7] and telemedicine platforms [8].

Due to the current absence of a national Trusted Third Parties (TTP) services, it was implemented an internal Public Key Infrastructure (PKI) contemplating CA functionalities,

management and issuing of digital credentials. In parallel it was developed a Healthcare Professional Card (HPC) focused on providing internal and external authentication on that HIS, contemplating the use of biometry in specific access scenarios. Later, a Patient Data Card (PDC) was created as a way to store and transport patient's administrative and emergency clinical data. It also includes a new model for storage and management of structured hyperlinks that allow the access to remotely distributed patient information. Both cards are PKC based where digital credentials are a key-point to implement and perform a solid user identification and authentication. Both cards are supported and complemented by a Card Portal Service where intervenient can, for instance, request a card, download the API browser to navigate inside card contents, backup/restore some information related with remote access links to EPR (on PDC), or renovate user digital credentials or download digital certificates revocation lists (CRL).

3. Results

Until the implementation of the HPC (PKC-based), the services of the department HIS were limited to indoor access. Recently physicians' insistences to have access to a user friendly HIS interface outside the institution and supported by universal Internet browsers was the starting point to the distinct projects developed in this area. The implementation of the internal PKI and a HPC with digital credentials, in parallel with the XML/Web-based interface implementation; were carried out to provide outdoor access to the HIS from distinct client platforms [9] as it is represented in figure 2.

The HPC, aims to provide strong authentication to healthcare professionals, proposes a new vision to integrate smart cards, digital credential, biometric fingerprint and user password, contemplating the worldwide access scenarios. The main goal was the achievement of a flexible and robust security access system to verify and ensure that the users are in fact who they claim to be. In the developed model, biometrics recognition and password acquisition have been integrated into a PKC-based crypto token to achieve strong identification and authentication of users.

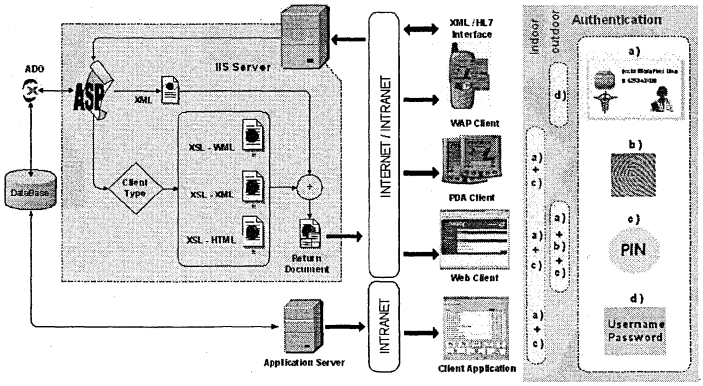

Figure 2: HIS and Healthcare Professional Authentication

The model was delineated to work in a dual mode scenario. Inside the institution the user must provide the token password to gain access to the private key. In outside access it is additionally demanded the presence of a biometric recognition element. This decision was based on the observation that inside the institution domain the identity control of users is associated to their physical presence that simplifies the authentication procedure. In outdoor access we defined that the physical control factor should be replaced or at least attenuated by the inclusion of biometric mechanisms.

Concerning figure 2, current implementation drawbacks are related with actual technological constraints that made impracticable the use of smart cards or biometry on some hand-held devices such as PDA's or mobile phones. Consequently, the implemented access control policy imposes that, for instance, the access from a mobile phone, with username/password authentication, just grants access to healthcare professional administrative zones, like the physician schedule, and no sensitive clinical information is accessible. In this way, one same healthcare professional can have distinct access levels depending from the physical provenience and authentication provided.

Restricting the analysis to the usage of the Web interface, we realize that, inside the institution the healthcare professional is authenticated through an HPC-PIN pair ('*a*+*c*' in Figure 2), but to obtain a similar access level from a remote access it is mandatory the provision of a biometric recognition ('*a*+*b*+*c*'). This option is based on the idea of "avoiding delegation of access permission to third persons" and results on a stronger authentication method.

The presented solution makes use of a fingerprint recognition device that is one the most widely accepted systems currently available, due to its relative ease of use, higher security and low-cost. This automatic system identifies and classifies fingerprints based on minutiae (finger lines forks and terminations) that are extracted from the fingerprint template image and stored inside the smart card for future user identification verification. Two fingerprints captures from the same finger are not exactly equal due to some aspects like the human finger skin elasticity. Consequently, the biometrics system does not give us a "yes" or "no" answer, just a confidence level that have correctly identified the user. Modern systems can reach error rates near 0.001% [10].

A key point on our model is that the effective smart card PIN that protects the PKC private key, is the result of several parameters provided by distinct intervenient elements (user, card issue entity, system designer) and from secret data processing. The master fingerprint template (a byte stream sequence), that is securely stored inside the card, is combined with the user password to calculate the smart card PIN that will unlock the PKC private key. To avoid that the master template leave the card, and may be captured, we decide to use java cards that allow the developing of embed applications, named cardlets [11], which are stored and executed inside the smart card environment. With this solution, the functional model was simplified, and the risk of attack was constrained to the physical layer. In an outdoor access the cardlet running inside the java card accepts as input arguments the user password, the live captured template, and the server side challenge to be signed with the user PKC private key. The matching process is done inside the card without any risk to the master template stored in the card. At the end, the java routine just returns the signed challenge that will be sent to the server in order to provide the necessary user authentication.

The results that were obtained with this particular HPC development, associated with the idea of a unique EPR grounded in a secure-effective share and remote access to patient clinical data, motivate the creation of a solution for an innovative Patient Data Card.

Looking to current PDC implementations, they are typically restricted to specific environments and goals, and are mainly applied just for administrative purposes or to a particular clinical usage. The diabetes card and emergency clinical data card are examples of this last situation. For instance, the DIABCARD project [12] provides an integrated application solution and related security services based on PDC oriented to the diabetes disease context. Considering large-scale utilization, the most generalized PDC implementations are restricted to identification and administrative purposes. This currently reduced utilization of clinic-administrative PDC is primarily explained by its limited storage capability but also by the lack of common policies that enforce the wide use of an interoperable information structure.

The proposed Multi-Service PDC (Figure 3) was modelled and developed in order to provide five complementary services:

- Resident administrative and emergency clinical data support.
- PDC owner verification capability (including fingerprint as an option).
- HyperLink zone [13], build upon the URL schema that allows to link to distributed Electronic Patient Records (EPR).
- Patient digital credentials support and management [14].

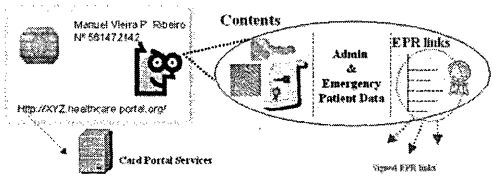

Figure 3: Multi-service PDC – Structured EPR Links

The patient administrative dataset and the emergency dataset are structured following the G-8-Netlink [15] specifications to ensure PDC interoperability at international level. Using the ISO8825 data encoding and following the G-8-Netlink card dataset, compatibility is ensured with G-8-Netlink systems and compliant issued cards.

On the card's zone reserved to the EPR hyperlinks it is possible to store, search and browse remote Web EPR locations. We can see this feature as a mobile clinical patient homepage portal. This is achieved through a structured implementation of hyperlinks associated to remote clinical patient data, creating, by one side, a truly distributed EPR system and promoting, by the other, the idea of a virtual unique and universal EPR. When a patient goes to a healthcare provider and clinic data is produced, the institution with EPR available on a web environment can write on the card a self digitally signed hyperlink referencing this information.

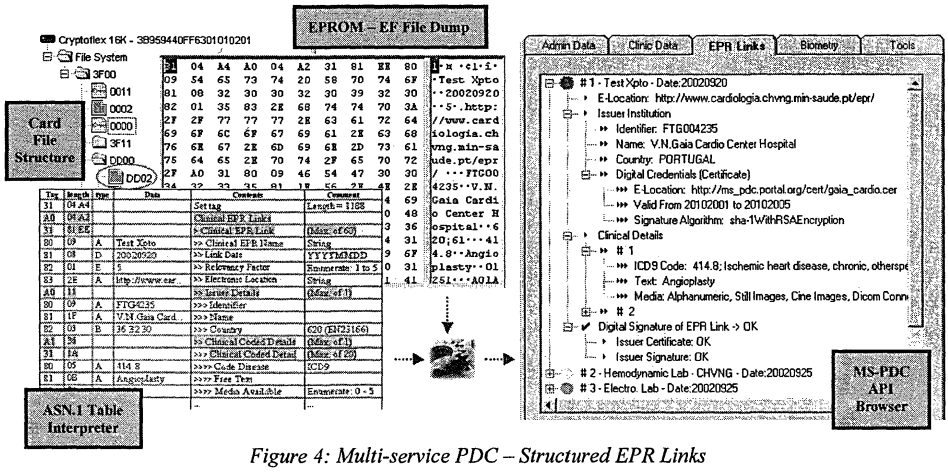

Figure 4: Multi-service PDC – Structured EPR Links

The structured hyperlink dataset (Figure 4) was defined in ASN.1 and follows an ISO8825 data encoding implementation. Every pointer includes, beyond other fields, an electronic record address (URL), the issuer institution identification and digital credentials references, a relevancy factor indicator, as well important coded clinical details (information type, code disease follow the ICD 9 coding table, free text, media type available). They work as structured bookmarks that objectively provide the indexing, sorting, location and access mechanisms to a distributed electronic patient record. As example, a doctor can apply a filter that sorts only the hyperlinks with one specific relevancy factor value and/or information concerning a specific medical specialty and or group code disease. Every institution, making use of their private key, also digitally signs the appended hyperlink. It is

possible verify the veracity, integrity and trust chain of this link because the provider digital certificate location is stored in a hyperlink field.

The Multi-Service PDC is hosted by a cryptographic token, with native capabilities to store and manage the patient digital credentials. Strong authentication mechanisms are implemented with the patient private key protected by a second authentication factor (PIN/Biometry). The confidence on security issues depends strongly on the trust we have on digital certificates (TTP services), on private key storage and how it is verified that the correct person is the owner of the private key. Reflecting these demands, a PDC hosted by a crypto smart card must implement card owner verification procedures. The first identity proof is related with the patient physical card possession. Second, the user private key used to remote authentication is unique and securely stored on the card, protected by a PIN.

4. Conclusion

We have presented an integrated model for the provisioning of access control in healthcare institutions. A focus has been put on the description of the overall architecture and trial experiences.

The presented integrated healthcare access model represents a cost-effective solution that provides strong authentication methods to healthcare professionals, allows high patient data mobility and implements a flexible model to access distributed EPR over open and heterogeneous environments as the Internet. Strong security enforcements and completely scalable utilization are other achievements of the proposal.

References:

[1] Walton, P.L., PROMIS: The Problem-Oriented Medical Informatics System - An Overview,Bureau of Health Services Research, Health Resources Administration, U.S. Department of Health, Education, and Welfare,1973,

[2] Bourka, A., N. Polemi, and D. Koutsouris. *An Overview in Healthcare Information Systems Security.* in *MedInfo2001.* 2001. London.

[3] Harp, P., Harmonisation for the Security of Web Technologies and Aplications,Harp Consortium,www.telecom.ntua.gr/~HARP/HARP/HARP.htm

[4] Marvie, R., Pellegrini, M. et al. *Value-added Services: How to Benefit from Smart Cards.* in *GDC2000.* 2000. Montpellier, France.

[5] Gobioff, H., et al. *Smart Cards In Hostile Environments.* in *Proceedings of The Second USENIX Workshop on Electronic Commerce.* 1996. Oakland, U.S.A.

[6] Hachez, G., F. Koeune, and J. Quisquater, *Biometrics, Access Control, Smart Cards: A Not So Simple Combination,* in *Security Focus Magazine.* 2001 October.

[7] Silva, A., et al. *A Cardiology Oriented PACS.* in *Proceedings of SPIE.* 1998. San Diego - USA.

[8] Costa, C., et al., *A Transcontinental Telemedicine Platform for Cardiovascular Ultrasound.* Technology and Health Care - IOS Press, 2002. vol. **10**(6): p. 460-462.

[9] Costa, C., J. Oliveira, and A. Silva. *Um Novo Mecanismo de Autenticação para Sistemas de Informação Clinica.* in *CRC2001.* 2001. Guarda - Portugal.

[10] Jain, A., et al., *An Identity Authentication System Using Fingerprints.* Proceedings of the IEEE, 1997. vol. **85**(9): p. 1365-1388.

[11] Microsystems, S., Java Card 2.1.2 - Development Kit User's Guide,2001,

[12] Blodel, B., et al., *Security interoperability between chip card based medical information systems and health networks.* International Journal of Medical Informatics, 2001. vol. **64**(2-3): p. 401-415.

[13] Costa, C., et al. *New Model to Provide a Universal Access Mechanism to Clinical Data.* in *Mednet2001 - 6th World Congress on the Internet in Medicine.* 2001. Udine - Italy.

[14] Santos, J.C., J. Oliveira, and C. Costa. *A User-oriented Multi-service Access Control System.* in *CRC2002.* 2002. Faro - Portugal.

[15] G-8-Netlink-Consortium, Netlink Requirements for Interoperability", v2.2,http://www.sesam-vitale.fr/html/projects/netlink

Address for correspondence
Carlos Manuel Azevedo Costa
DET /IEETA - Universidade de Aveiro, 3810-193 Aveiro, Portugal
ccosta@ieeta.pt