Virtual Health Card System

Tiago Pedrosa[1,2], Carlos Costa[2], Rui Pedro Lopes[1], and Jose Lu s Oliveira[2]

[1] Polytechnic Institute of Bragança, Portugal
[2] University of Aveiro, IEETA, Portugal

Abstract Electronic Health Records are key components to an efficient exploitation of information technologies in health care institutions. Nevertheless, several barriers that hinder its wide adoption subsists. The co-existence of dissimilar and incompatible health information systems and the absence of a unique central repository for personal medical data are some examples. This paper, we propose a web-based health records repository that allow citizens to have a unique virtual card that integrates all their personal clinical data. Privacy policies and the access control mechanisms are also discussed.

Resumo Os registos médicos electrónicos são fundamentais para uma utilização eficiente das tecnologias de informação em instituições de saúde. No entanto, existem várias barreiras que atrasam a sua implementação em larga escala. A co-existência de sistemas de informação de saúde díspares e incompatíveis, bem como a falta de um repositório central de informação médica pessoal, são alguns dos exemplos. Propomos um repositório médico, baseado em tecnologia web, disponibiliza aos cidadãos um cartão virtual único que agrega toda a sua informação médica. Questões relacionadas com a privacidade e mecanismos de controlo de acesso são também abordados.

1 Introduction

The use of Information Technologies (IT) to support health care services is a reality commonly spread in the society. Nevertheless, one of the biggest challenges in the health informatics is still the creation of an Integrated Electronic Health Record (IEHR) - a patient longitudinal record that aggregates all generated information in clinical consultations. The balance between privacy and accessibility issues is one of the reasons that makes health care a rich scenario for security technologies [8]. On one hand, we must enforce the privacy of sensible information and, on the other, the quality of healthcare services demands sharing and remote access to patient information [9,7].

The IEHR is an important tool that clinicians can use to be better informed about patients' medical history. Due to changes in citizens way of living, it's

normal one person to have several clinical appointments in diﬀerent cities, regions and even countries. Citizens move their residence during lifetime, travel more regularly, for working, for leisure or even for medical care [12]. Hence, the information generated will be disperse along several institutional information systems. A unique view of the disperse EHR, would improve the quality of healthcare services. To create an integrated access to the information that is disperse amount several systems, a single patient identiﬁer should be necessary to simplify the aggregation of medical data. However, this isn't a straightforward task since each patient may have diﬀerent identiﬁers in various systems.

As the information is spread in several organizations, its sharing has to respect rigid laws and regulations that makes diﬃcult the IEHR implementation. Other diﬃculty is based on the lack of well established communication standards between diﬀerent EHRs systems, despite some eﬀorts [11].

2 Materials and methods

In most scenarios, the regulatory and law framework for sharing health records can be satisfied imposing the patient informed consent (several models use this approach [5,1,3]). As the patient is entitled to request a copy of its records and share with anyone that he decides, the sharing is make using his consent instead of the organization that stores the records.

In those heterogeneous environment, involving diﬀerent organizations, public or private, a secure authentication mechanism is mandatory. In the last decade, the use of smart-cards in healthcare information systems has been consensual, as they provide a secure way for storing information and authentication credentials for remote authentication [6]. The Electronic Health Card (EHC) is basically a smart-card that is used for saving useful information for administrative tasks, emergency medical information, security certiﬁcates and, in some cases, e-prescriptions. This type of tokens are used in some countries like, for instance, Germany and Austria to achieve a national IEHR solution.

As discussed, the IEHR implementations needs to provide an integrated access mechanism to disperse information. So, the integrator system must know the data location, more precisely the query engine service to extract information of a speciﬁc patient. This linkage information can be stored in the integrator database, however some projects decided to extend electronic health card to support that service. Hence, the Virtual Unique Electronic Patient Card (VU-EPR) appears as a possible solution [4].

The VU-EPR is based on a token containing card-owner resident clinic-admin information, as well as structured references to its electronic records. The smart card securely contains this reference structured data set. The implementation of Public Keys Cryptography and Crypto Smart Cards, unequivocally provides a way to securely store, transport and access the card-owner information. Moreover, it also grants the owner full control over the access to its data, through a Pin and/or biometric registration. Finally, it also allows the card-owner to entitle information access levels to other users such as the clinical professionals. The

main beneþts associated to this solution can be characterized by highly scattered geographical storage requirements. This model empowers patient enabling the discretionary access to remote data, when crossed VU-EPR card with health professional card, and allows an open access to the medical emergency data stored in the card. Upon this model, we developed a VU-EPR solution named Multi-Service Patient Data Card (MS-PDC). The MS-PDC was modeled to provide þve complementary services and results from an extension of a þrst developed (VU-EPR) model exclusively oriented to Electronic Patient Records [5,4] information: i) Administrative data support; ii) Emergency Clinical data support; iii) Hyperlink base, build upon the URL schema and that allow to link the patient clinical and genetic distributed information; iv) Patient digital credentials support and management; v) PDC owner veriþcation capability.

The MS-PDC uses URLs to fetch the information on the disperse systems and present them to the user as a unique view of all distributed data. This model copes well with mobility issues, such as the gathering of disperse data and controlling the access to it. Nevertheless, in a wider concept of mobility it's not feasible that all patients will hold the same type of card world-widely. Other discussable aspect is the need of the presence of the physical card in the system whenever exists the need to access the patient EHR. Thus, we propose a model where a system will hold the card in behalf of the user.

3 Results

The Virtual Health Card System (VHCS) proposed, appears as a solution to overcome the drawbacks associated with physical token dependency. Instead of the EHC being hold by the patient (Figure 1), it will be hold by a service (Figure 2). The service will store and provide access to the EHC when requested and only if the authorization is granted by the predeþned policies. Therefore the information can be used after patient informed consent, since the links to the information will be on the system. The informed consent will be also stored in the card, visible to other system components that can read it and apply that policies controlling the access to the patient information. Moreover, other important advantages could be identiþed in this proposal. First, it expedite the processes of backup and revalidation of credentials. Secondly, an important issue, it allows the dynamic update of links on the patient card whenever new information is created. Most of this features became available due to the continuos presence of the card in the system(Figure 2).

This approach will permit the disassociation between the credentials used by users in system authentication and the credentials used inside the system. For accessing to his EHC, the user will authenticate using a token. The system is suŽciently exible to support diÞerent tokens including the new Portuguese Citizen Card, an electronic identiþcation card (eID card) that contains a certiþcate for authentication. Moreover, if the user token or eID is lost or stolen, the system can temporary block the access to the Virtual Health Card until the new token be available and associated to a patient Virtual Health Card.

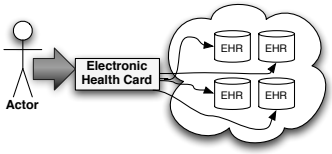

Figure 1. Patient hold his electronic health card

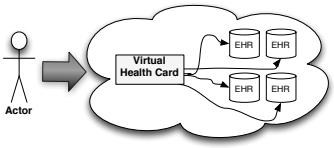

Figure 2. System holds patient electronic health card

Our proposed model (Figure 3) is composed by 4 main components: the credentials, the access policy and two types of Universal Unique Identiþers (UUIDs). The credential component is responsible for securely storing the private and pub-

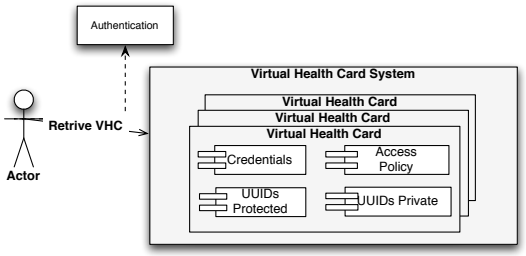

Figure 3. Virtual Health Card System

lic key of the user. The access to the private-key container is only available to the authenticated user (the actor), by the way of a secret (could be a password or other method [2]). The private-key inside the container is the credential that will be used internally for authentication, signing, cypher and de-cypher the information. This modus operandi separates the credentials for authentication in the system from the credentials that the user will use to logon.

In access policy component, the patient deþnes the informed consent to his information, identifying healthcare professional and granting speciþc permissions. Each new entry is signed with the patient's private-key. Hence, each time a system component makes a request to access the patient information, the system checks if the requesting user has the necessary privileges (through the access policy), verifying always if the policy was really signed by the patient.

The UUIDs represent indexes to the disperse patient information. The VHCS use this information to create an unique view of it IEHR. These universal unique identiþers will work as links to the remote information. Moreover, each link has also complementary information about access mechanisms (or services). The system provides two types of UUIDs spaces, enabling a patient private links area (i.e. UUID Private) to have information that only him can reference and other

area (UUID Protected) where are placed the references accessible to speciþc healthcare professionals.

The Private UUID may be used to handle references of very sensible and discriminatory information. On this component, the patient can manage the information that he does not want accessible to any health professionals, in any occasion. To enforce this behavior, the system will cypher the references with the users correspondent public-key forcing that only with the private-key of the user this information could be read. The access to this private information demands always the explicit patient consent.

The Protected UUID is the place where other system components (or external services) can update the UUIDs, as new information is being produced in several health systems. Components that in the behalf of an authenticated and authorized user want to access the patient's information, query this component to get information about remote patient data location and how to access it.

The credential component will ensure that only an authorized user can access his private-key and that Private UUIDs will only be accessible using the correct private-key that is stored inside the credential component. It's also propose that the Protected UUID and the Access Policy be cyphered using a system key, that must be shared between the components that need to communicate with the VHCS. Therefore a component is obligated to register in the system to obtain the access key.

In a emergency scenario, the patient could not be able to provide the intend consent. The VHCS is prepared to handle this situation granting the practitioner access to the patient EHR and bypassing the access policy for the UUID Protected. This "break-the-glass" mechanism will only give access to information that isn't protect in the private area (UUID Private component). This mechanism will generate auditing records for future analyze and detection of misconducted access.

The VHCS proposal provides an important indexing and retrieve service of disperse information and the access control mechanisms to ensure the patient data privacy and conþdentiality. It will also enable users to have an unique authentication in the system, providing a single-sign-on behavior. This service will present the user credentials to other components as needed.

4 Conclusions

The proposed model copes well with requirements of mobile citizens EHRs, it separate the credentials used for authentication from the credentials used in the indexing system. It enables the creation of a dynamic mechanism to update references of remote patient information. It also copes with the existence of diÞerent identiþers for the same patient, along diÞerent healthcare systems. Moreover, it empowers patients with the capability to decide what information is absolutely private from all the information that exists in the disperse EHRs. Finally, it implements an informed consent mechanism that respects the regula-

tory framework for sharing of healthcare records between distinct professionals (or institutions) in diPerent regions or countries.

Further work will be need namely to decide how to implement the access control policy. The idea is to have a central RBAC policy database [10] that deþnes the permissions for each role like, for example, the permissions to a practitioner or the permissions to a nurse. With the central RBAC policy database the patient only have to decide which role he grants to each professional proþle in the access policy component.

References

1. Ankica Babic, Carlos Costa, José Luís Oliveira, Natalja Voznuka, Ilidio Oliveira, Markus Storm, Victor Maojo, Fernando Sanches, Miguel Santos, Antonio Sousa Pereira. *Confidentiality and security issues in web services managing patient clinical and genetic data*. Linkopings, Sweeden, 2004.
2. J. Basney, M. Humphrey, and V. Welch. The MyProxy online credential repository. *Software: Practice and Experience*, 35(9):801–816, 2005.
3. J. Bergmann, O. Bott, D. Pretschner, and R. Haux. An e-consent-based shared EHR system architecture for integrated healthcare networks. *International Journal of Medical Informatics*, 76(2-3):130–136, 2007.
4. A. S. Carlos Costa, José Luís Oliveira. Electronic patient record virtually unique based on a crypto smart card. *Lecture Notes in Computer Science*, Volume 2722/2003, 2003.
5. A. S. V. G. R. Carlos Costa, José Luís Oliveira. A new concept for an integrated Healthcare Access Model. *Studies in health technology and informatics*, 95:101, 2003.
6. H. Chien, J. Jan, and Y. Tseng. An Efficient and Practical Solution to Remote Authentication: Smart Card. *Computers & Security*, 21(4):372–375, 2002.
7. F. Colasanti. ICT for Health and i2010-Transforming the European healthcare landscape-Towards a strategy for ICT for Health [online]. June 2006. Luxembourg, 2006.
8. C. Dalton. The NHS as a proving ground for cryptosystems. *Information Security Technical Report*, 8(3):73–88, 2003.
9. K. D. Mandl, P. Szolovits, I. S. Kohane, D. Markwell, and R. MacDonald. Public standards and patients' control: how to keep electronic medical records accessible but private commentary: Open approaches to electronic patient records commentary: A patient's viewpoint. *BMJ*, 322(7281):283–287, 2001.
10. J. Reid, I. Cheong, M. Henricksen, and J. Smith. A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems. *Proceedings of the Eighth Australasian Conference on Information Security and Privacy (ACISP 2003), LNCS*, 2727:403–415, 2003.
11. Technical Committee ISO/TC 215. Health informatics — electronic health record — definition, scope, and context - iso/tr 20514:2005(e). Technical report, International Organization for Standardization, 2005.
12. The European Economic and Social Committee and the comittee of regions. Final report on the implementation of the commission's action plan for skills and mobility com(2002) 72 final. Technical report, Commission of the European Communities, 2007.