A Mobile Based Authorization Mechanism for Patient Managed Role Based Access Control

Cátia Santos-Pereira[1], Alexandre B. Augusto[2], Manuel E. Correia[2,3], Ana Ferreira[1,4], and Ricardo Cruz-Correia[1]

[1] Center for Research in Health Technologies and Information Systems (CINTESIS), Faculty of Medicine of University of Porto (FMUP), Portugal
[2] Center for Research in Advanced Computing Systems (CRACS), Department of Computer Science, Faculty of Science of University of Porto, Portugal
[3] Department of Health Information and Decision Sciences (CIDES), FMUP, Portugal
[4] Informatics Centre, FMUP, Portugal
{catiap,amlaf,rcorreia}@med.up.pt, {aaugusto,mcc}@dcc.fc.up.pt

Abstract. The Internet has proved the enormous benefits that can be accrued to all players involved in online services. However, it has also clearly demonstrated the risks involved in exposing personal data to the outside world and constitutes at the same time a teeming breeding ground of innovation for highly flexible security solutions that can minimize these risks. It is now widely believed that the benefits of online services to healthcare in general supplant the risks involved, provided adequate security measures are taken and the role played by all the parties involved, be they physicians, nurses or patients are clearly outlined. Due to the highly sensitive nature of the data held on the Electronic Health Record (EHR), it is commonly agreed that providing online access to patients EHR to the outside world carries an unacceptable level of risk not only to the patients but also to the healthcare institution that plays a custodian to that sensitive data. However, by sharing these risks with the patients, healthcare institutions can start to equate the possibility of providing controlled exterior online access to patients EHR. The mobile phone is nowadays the preferred mean by which people can interact with each other at a distance. Not only that, the smartphone constitutes the full embodiment of the truly personal device users carry constantly with them, everywhere. They are therefore the ideal means by which the user can casually and conveniently interact with information systems. In this paper we propose a discretionary online access rights management mechanism based on the Role Based Access Control (RBAC) model that takes advantage on the personal/technical characteristics and data communications capabilities of the smartphone in order to provide patients with the means by which they can conveniently exercise safe discretionary online access permissions to their own EHR.

Keywords: Patient Empowerment, e-health, Electronic Health Records, RBAC, Secure Mobile Wallet, PKI, smartcard, QR codes and Secure Tokens.

C. Böhm et al. (Eds.): ITBAM 2012, LNCS 7451, pp. 54–68, 2012.

1 Introduction

Nowadays, patients want to be better informed about their medical conditions and play a more active role on their own treatments. They usually consult online information by using search engines to educate themselves about etiology, treatments, and the prognosis of the medical conditions. Getting access to their medical records would help the patient to better understand their medical conditions [1]. On this issue the European Recommendation [2] and American Legislation [3] for protection of medical data agree that the patient must have access to his/her medical record and play a major role in the decisions regarding the content and the distribution of his/her medical data [4].

Currently, for patients to have access to their medical records they need to write a request to their custodian healthcare institution and the response delay depends on their country legislation (e.g. 10 days in Portugal [5], 21 days in England [6] and 30 days in USA [3]). We believe that the latest developments in digital communications and information technologies should provide the patients a simpler and more secure way to access their medical records and at the same time provide a better collaboration and interaction experiences with the healthcare professionals [7].

In the healthcare domain, patients digital data is normally collected into what is called the Electronic Health Record (EHR). The EHR encompasses many functions that can include different types of data items such as diagnoses, medications and operations [8,9]. The EHR is nowadays indispensable for health institutional purposes and could be used to empower patients by giving them the necessary information to play a more active role in their own health and in their families health as well [10].

Unfortunately, by opening up the access to the EHR with inadequate access control mechanisms and policies carries some substantial risks as illustrated by the grim statistics observed during the period of 2006 to 2007, where in the USA, over 1.5 million names were exposed during data breaches that occurred in hospitals [11]. One of the most important and complex requirement for eHealth systems [12] is to keep patient's information private and secure. The EHRs are daily accessed by a diversity of health professionals that have different objectives according to their functions. Appropriate access control mechanisms and policies are essential to provide a good balance between usability and confidentiality. These procedures constitute the core of the authorization process on eHealth systems, in other words, they are responsible to manage the EHR access by granting access only to previously authorized persons [13].

The patient authorization model proposed by *Santos-Pereira et al.* [7] is to be used and customized by the patient. This model effectively combines the characteristics of Role Based Access Control (RBAC) model [14], ISO 13606-4 [15], temporal constraints (GTRBAC) [16] and break-the-glass mechanism (BTG-RBAC) [17]. The access permissions of a role to a specific EHR component is dependent on the previously mapping made by the administrator of the model (usually the patient). A customized role can have access to an EHR record component if the administrator defines any of the create, read, update, delete or break-the-glass operations to be part of the record access permissions.

Tacconi et al. [18] states that smartphones are revolutionizing many sectors and aspects of our economy, including social networks and healthcare. Based on this we decided to employ the smartphone as the tool to establish a more interactive relationship between the system and its users, since the smartphone by its own very nature as a personal communication device usually follows their owners everywhere. They constitute an ideal platform to develop and provide any-time and any-where fast user interactions.

Our aim is to define a patient-centric infrastructure to manage medical data access in a reliable and secure way. To realize our objective we rely on the: (a) patient authorization model defined by *Santos-Pereira et al.* [7] to define patient centered access control and administration; (b) Extensible Messaging and Presence Protocol (XMPP) to establish the communication between the mobile devices and the healthcare institutions; (c) usage of dynamic web services in order to create the necessary communication nodes. To this infrastructure we call OFELIA (Open Federated Environments Leveraging Identity and Authorization). OFELIA provides the means to build a secure web based service infrastructure where the patient can access and customize access permissions to his/her own EHR in a complete patient-centric way using his own smartphone as an authorization broker [19].

In OFELIA access control is exercised by the means of a secure mobile identity digital wallet, secured by a Public Key Infrastructure (PKI) with keying operations provided by a smartcard for mobile devices. This secure mobile identity wallet allows the patient to exercise a flexible based access control over their EHR thus disclosing its data only to pre-authenticated and previously authorized users, for certain well defined periods of time at the data owners discretion.

The rest of the paper is organized as follows. In Section 2, we review the system mechanisms and technologies, describing how they constitute the OFELIA architecture. In Section 3 we describe the necessary steps to establish a trust connection in order to request an EHR access. In Sections 4 and 5 we present an usage case scenario and then discussed some issues and their possible solutions. In Section 6 we present a preliminary conclusion about our proposed architecture and delineate our plans for future work.

2 Security Mechanisms and Technologies

In this section we present the mechanisms and technologies employed to implement the OFELIA authorization infrastructure. Each mechanism/technology is presented in some detail and then we explain how the functionalities can be integrated to the proposed authorization model.

2.1 Patient Authorization Model

Santos-Pereira et al. [7] proposed an authorization model where the concept of Patient Healthcare Network (PHN) is defined and is composed by all the healthcare institutions that the patient may attend and where his medical records are kept (e.g. hospitals and healthcare facilities). The knowledge of which healthcare institutions belong to the patient's PHN is very important, because if the patient wishes to access his medical records he should have been previously enrolled within all these institutions. In our vision each healthcare institution deploys its institutional EHRs together with an OFELIA web service that is described in subsection 2.7. The concept of PHN and the need for the patient to access his medical information, within multiple healthcare institutions, is very important however is not contemplated in this paper because we are only focusing in the authorization process architecture. Nevertheless, the PHN concept and implementation in all its extent is a fundamental step to be addressed as future work.

Santos-Pereira et al. model integrates a set of functional roles that categorizes the accesses to the patient EHR into three main groups: subject of care (SC) (Group I), healthcare professionals (Group II) and administrative staff (Group III) (see Figure 1).

In this work we focused in Group I to explore the idea of patient empowerment by deploying an infrastructure that allows patients to access and share their EHR record components based on functional roles.

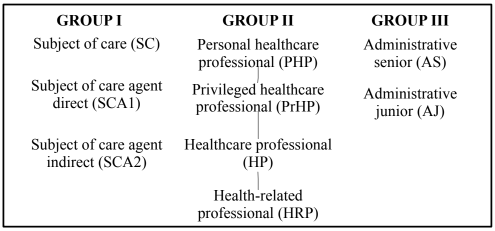
GROUP I
Subject of care (SC)
Subject of care agent direct (SCA1)
Subject of care agent indirect (SCA2)
GROUP II
Personal healthcare professional (PHP)
Privileged healthcare professional (PrHP)
Healthcare professional (HP)
Health-related professional (HRP)
GROUP III
Administrative senior (AS)
Administrative junior (AJ)

Fig. 1. Functional Roles groups and Hierarchies [7]

2.2 Quick Response Code

The Quick Response codes (QR codes) are two-dimensional square shapes that encode a reasonable amount of digital information (several Kilobytes of chars) in a small amount of space. The encoding is achieved with the careful positioning of varying size black and white smaller squares within the 2D space defined by the QR square. These 2D codes are normally displayed within web pages or printed in paper posters and are employed to quickly exchange digital information with mobile devices that would otherwise had to be entered by hand. This is accomplished by having the mobile device to digitally scan and decode the displayed QR code with its built-in optical camera [20].

In OFELIA, QR codes are displayed at computers displays for an auto-enrollment process of smartphones into the healthcare institutions. QR codes are a very convenient way of conveying a reasonably amount of secret shared information to a smartphone that would otherwise be very cumbersome to input by hand by the user. The usage of QR codes to share secret information between ehealth systems and smartphones, can in a way, be seen as the establishment of a rather new special security layer by taking advantage of the analog security properties of the optical channel that is employed during the scanning of the QR codes by the smartphone. In other words, the QR codes can be used to simplify and make practical the enrollment process between the OFELIA web service (within the healthcare institution) and the user smartphone.

2.3 Extensible Messaging and Presence Protocol

The Extensible Messaging and Presence Protocol (XMPP) is a widespread open technology, employed for almost real-time messaging style communication, that takes advantage of the eXtensible Markup Language (XML) as a base format for exchanging information [21]. XMPP provides a complete standard set of services [22] like certificate based authentication and asynchronous one-to-one and many-to-many messaging services that are extensively employed in our propose as the network transport layer infrastructure.

Arguably, in the mobile world an implicit direct Internet communication with a personal device is generally not possible due to the shortage of public IP (*Internet Protocol*) addresses faced by Internet service providers. In the near future, the IP version 6 (IPv6) is supposed to solve this problem, however we believe that the mobile telecommunications operators will not allow for directly addressable mobile devices from the Internet due to their less flexible business plans which regard mobile devices, smartphones in particular, as a strict consumer device, not as a service provider.

Towards this end, XMPP is proving to be an almost ideal communication infrastructure for our propose to circumvent these communication restrictions because of its ability to efficiently operate over HTTP (*Hypertext Transfer Protocol*) by the means of the BOSH (*Bidirectional-streams Over Synchronous HTTP*) [23] protocol, where two non directly addressable devices, located on private closed intranets and with minimal Internet access, can locate each other over the Internet and then freely exchange messages between themselves in a reliable and secure way [24].

2.4 The Trust Infrastructure

The management of trust between the healthcare institutions and the smartphones is essential to our scenario. To establish this trust we rely on a Public Key Infrastructure (PKI) that is responsible for the management of the certificates that are at the core of the privacy, trust, non-repudiation and authentication infrastructure mechanisms that we need to put in place to secure our architecture.

To establish a stronger and therefore more trustworthy identity and authentication between the different actors (personal smartphones and healthcare institutions), we rely on the deployment of a well managed standard compliant PKI that can also sign PGP (*Pretty Good Privacy*) and X509 certificates. These certificates are then used as securely vouched identity credentials that can be employed to establish highly secure communication channels, with a reasonable degree of non-repudiation properties and trust between the parties involved in the communication.

2.5 MicroSD Mobile Security Card

Due to the pivot role played by the smartphone in our vision, it is vital to guarantee a more trustful patient identity and assure strong authentication for the communication mechanisms. A more traditional file based keystore to protect the keys of the identity certificates would not be secure enough because a regular file can be easily copied and the smartphone can be a target of attacks where this keystore file can be compromised. It is reasonable to put the encrypted file based keystore security in tandem with the security provided by a much simpler login/password based scheme. In fact, an attack on a password protected keystore file involves a password guessing attack completely analogous in terms of complexity to what happens with an attack directed towards a login/password scheme.

To solve this weakness we rely on the security properties of the mobile security card (MSC) [25] for mobile devices. These security cards are composed by a flash memory and a smartcard component that provides the necessary crypto components and device physical non tampering security features [26]. This allows us to guarantee a two factor authentication required for sensitive data exchange scenarios. To also encourage and provide for a greater level of user responsibility and trust in the system, we also employ identity certificates (X509, PGP) [27] for MSC internally generated crypto-key pairs. These certificates are signed by the users citizen card (eID) [28] to further ascertain the smartphone authenticity to the network and by the healthcare institution to establish the possibility of federation between healthcare institutions in a future work.

2.6 The OFELIA Secure Access Authorization Token

An authorization token (AT) can be seen as a secure digital object that an authorized person needs to present in order to have direct access to another person's resources. In other words the authorization token looks like a valet key for data access, the one who possesses the key has temporary restricted access to the valet key emitter data.

These authorization tokens are also very hard to falsify and take the form of a small base64 encoded XML excerpt, containing elements for a large pseudo-random number [29], and a simple statement describing the authorization validity restrictions which apply to a particular authorization. This statement can express for example temporal restrictions. The XML excerpt is then digitally signed by the smartphone MSC private key and the resulting XML document is then encoded into a base64 string which constitutes the OFELIA authorization token.

The ATs provide a flexible security mechanism for EHR access control, allowing the EHR requesters a restricted and controlled access to the selected EHR record components and discarding the necessity of sharing and managing other types of credentials like login/passwords. In our scenario, these ATs are directly linked with a specific access role, defined by the EHR access control administrator, the subject of care, to the requester at the moment of the authorization. These tokens are only shared with the requesting healthcare institution since the EHR requesters are always associated with a specific identity. It is also important to clarify that in our vision the EHR access control administrator, the subject of care, also maintains the revocation rights by being able to unconditionally revoke these tokens at any given moment.

2.7 OFELIA Web Service

As illustrated in Figure 2, the OFELIA web service (OWS) is responsible for the management of the EHR authorization access process. The OWS is structured into three main component nodes: a XMPP server, an External Web Application (EWA) and an Internal Management Service (IMS).

The XMPP server grants a strong patient authentication method due to the mandatory usage of PGP certificates at the login process and a secure and asynchronous communication between smartphones and the EWA. The patient enrollment process with the XMPP server is illustrated by Figure 3 on step 4.

The External Web Application (EWA) is the service responsible for answering the HTTP(s) external requests, in other words, every time a patient wants to access his or other previous authorized EHR data, he must make a request to the EWA by using a computer with Internet access. When requested the EWA replies with an invalid session key encoded as a QR-code, which is then scanned and decoded by the patient smartphone that in turn sends a request to the XMPP server to validate the session key. This process is presented in Figure 5 in steps 1 to 4. After the patient's request, the XMPP server communicates with the EWA confirming the patient authenticity and requests the session key validation by presenting the patient certificate. Now the EWA can validate the session key by annexing the appropriate identity to it and finally establishing a valid session to the patient.

The Internal Management Service (IMS) is responsible to: query the healthcare institution's EHR based on the requester role that was previous established on the RBAC model by the Subject of Care at the moment of the authorization process; manage the patient enrollment into the healthcare institution by directly communicating to the registration healthcare institution computer; and to manage the patient identity and his authorization tokens. So after a patient successfully authenticates based on his identity permissions the IMS sends the information of what EHRs are accessible to the patient and respective pre-defined roles are linked to each one of these EHRs. This procedure is illustrated in Figure 5 step 5. This process only involves the IMS and the healthcare institution EHR database since the ATs are stored in the IMS.

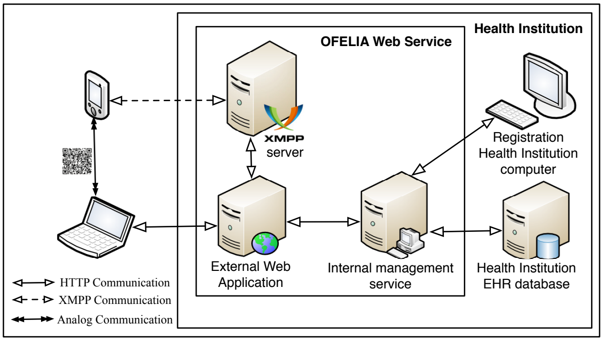

Fig. 2. Patient centric authorization architecture

2.8 OFELIA Mobile Application

The OFELIA Mobile Application (OMA) can be seen as an identity digital wallet to be deployed by the smartphone that is responsible to: strongly prove the patient identity within the healthcare institutions; create and manage the authorization tokens by providing the necessary means to its authorization and revocation; be the "unbreakable" bridge between the subject of care and the healthcare institution by constantly following their owners everywhere as the "de facto" personal mobile device.

To fulfill these objectives, OMA is composed by a database to store the ATs information, a MSC to guarantee patient's identity and authentication, and three service libraries: a XMPP client connector to establish the communication, the OFELIA secure access authorization token to provide the methods to generate the ATs in a secure way, and a QR-code library to read and interpret the QR-codes.

3 Enrollment and Authorization Processes

In this section we describe the enrollment process of a patient to a healthcare institution and all the necessary steps to realize the authorization process in order to gain access to his/others EHR record components.

3.1 Patient's Healthcare Institution Enrollment

Due to the patient's low knowledge about privacy, security and IT issues, this enrollment is done within his health institution provider, resulting in a physical security layer done by the responsible support member in service. Figure 3 presents the 6 steps to establish patient enrollment in a healthcare institution:

Step 1: The subject of care (the patient) accesses the registration healthcare institution computer and authenticates himself by using his citizen card (eID) on the pin pad machine of the registration healthcare institution computer.

Step 2: A pair of QR codes is presented one by one by the registration healthcare institution computer. The patient now reads the first QR code with his smartphone for the installation of the OFELIA Mobile Application (OMA) (could be skipped if the user have already installed OMA). Then, by using the OMA, the patient reads the second QR code for an auto-enrollment on OMA of his healthcare institution. This second QR code brings 3 components: an OFELIA web service (OWS) XMPP credential composed by a JabberID and a password, the OWS XMPP address configuration and a session key for the establishment of a session with the OWS.

Step 3: The OMA accesses the OWS XMPP by authenticating with its PGP certificate (generated by the OMA using the MSC). It then sends the previously exchanged session key obtained from the QR code in order to establish a link between the mobile session and the registration healthcare institution computer. Now the OWS pre-registers the patients certificate.

Step 4: To verify the patient authenticity the OWS sends via XMPP to the OMA a four digit one-time password encrypted with the patient pre-registered PGP certificate.

Step 5: The OMA decrypts the one-time password and presents it on the smartphone monitor requesting the patient to handily insert it on the registration healthcare institution computer. This process guarantees that it was the patient's smartphone who read the QR-code, in other words, the correct patient PGP certificate was exchanged.

Step 6: The OWS finishes the registration by sending via XMPP to the OMA the patient PGP certificate signed by the patient's citizen card (eID) and the healthcare institution itself. This PGP certificate is stored by OMA.

It is important to understand that this process of double signature grants a high level of identity and authenticity. The citizen card (eID) is issued by the government of the patient's country and its signature grants our proposal a real civil identity. The healthcare institution's signature is used to prove the patient's enrollment entity.

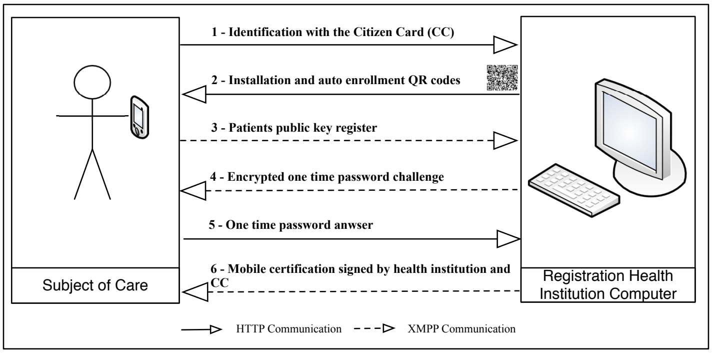
1 - Identification with the Citizen Card (CC)
2 - Installation and auto enrollment QR codes
3 - Patients public key register
4 - Encrypted one time password challenge
5 - One time password anwser
6 - Mobile certification signed by health institution and CC
Subject of Care
Registration Health Institution Computer
HTTP Communication
XMPP Communication

Fig. 3. Subject of care enrollment to a healthcare institution

3.2 EHR Authorization Request

In order to obtain access to other patient's EHR an authorization request must be triggered by a requester (e.g. subject of care agent direct or indirect) who was previously enrolled to the healthcare institution holding that EHR. This whole process is done by using XMPP communication and is described in Figure 4 in 4 steps:

Step 1: The requester, by using the OMA on his smartphone requests the OWS an EHR authorization access by inserting the desired patient JabberID.

Step 2: The OWS sends the EHR authorization request to the OMA of the EHR access control administrator, the subject of care (SC), including the descriptive information about the requester.

Step 3: The EHR access control administrator (SC) is notified on his smartphone by the OMA and based on the requester descriptive information he has to decide. If the subject of care agrees to give any access to his EHR record components, he has to select which functional role the requester will be attributed or to define a more specific role by subscribing any other functional role[7]. After the owner's authorization, the OMA generates an authorization token (AT), signs it and sends it to the OWS that stores the AT for possible later revocation.

Step 4: The OWS sends a report answer with the detailed information (the attributed role and the authorization expire date) to the OMA requester.

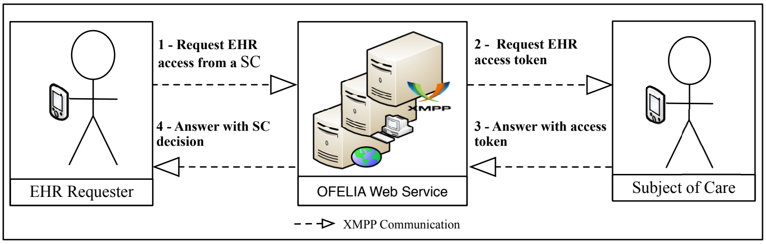
1 - Request EHR access from a SC
4 - Answer with SC decision
2 - Request EHR access token
3 - Answer with access token
XMPP
EHR Requester
OFELIA Web Service
Subject of Care
XMPP Communication

Fig. 4. Subject of care EHR authorization access request

3.3 EHR Access Request

The process to request an already authorized EHR data can be done by any computer with Internet access plus the usage of the user's smartphone to handle the authentication process. As we can see on Figure 5 this process is described in 7 steps:

Step 1: The user requests, via a web-browser, the OFELIA healthcare institution website.

Step 2: A QR-code with an invalid session key is returned, in other word a session key without access permissions is returned.

Step 3: The user, using the OMA on his smartphone, reads the QR-code that contains the session key.

Step 4: The OMA sends via XMPP to the OWS the invalid session key signed with the PGP certificate from the mobile secure card (MSC). It is important to understand that the XMPP authentication method provides a strong non-repudiation method since the requester's PGP certificate is validated during the login process.

Step 5: The OWS links the presented user's identification to the session key and based on the requester access authorization tokens, returns a list of patients and their roles to the requester's computer web browser. Now the session key is validated on OWS.

Step 6: The requester by using his web browser, consults the returned list and chooses the patient he wishes to consult by sending a request to the OWS.

Step 7: The OWS returns to the requester's computer web browser the selected patient's EHR data based on the requester's authorized role.

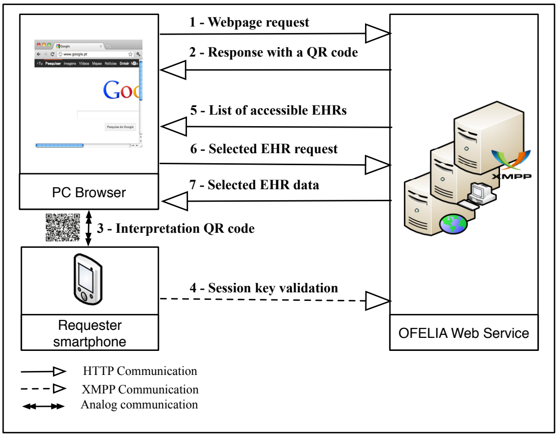

Fig. 5. Subject of care EHR access request

4 Storyboard

To better understand the capabilities provided by our authentication and authorization architecture, we have defined a storyboard to exemplify how the presented patient centric authorization architecture behave on a real healthcare scenario.

Katherine, a 50 years old woman that resides in Mystic Falls, has recently finished her radiotherapy treatments after being diagnosed with breast cancer. Her daughter, Agnes, who lives in a different city 400km away, desires to monitor her mother's follow-up consultations.

Assuming that both mother and daughter are already enrolled at the same healthcare institution, Agnes, the EHR requester, requires Katherine, the subject of care, an authorization to access Katherine's EHR with her smartphone as the subject of care agent direct functional role. Katherine, also using her smartphone decides to grant access to her daughter. However, Katherine wants to customize some of the access control rules of the subject of care agent direct functional role since she desires to omit the treatments' record component, creating the specific role "Patient's Daughter" for that purpose. Now Agnes accesses her healthcare institution website (that triggers the External Web Application from the OWS) with her browser and a QR code is returned and read by the OMA that handles the authorization process with the XMPP server into the OWS. After that, Agnes browser automatically refreshes with a list of the patients for which she has permissions to access. Now Agnes selects her mother assuming her assigned role, "Patient's Daughter", allowing Agnes to read the wished follow-up consultations record component.

Figure 6 illustrates the use-case of the above described storyboard. This use-case shows an example of the EHR folder regarding the Breast Pathology components [15]. The user Agnes accesses Katherine's EHR, with the "Patient's Daughter" role, attributed by her mother, which gives Agnes permissions to only read the following components: *demographic data*, *family history*, *consultations* and *complementary diagnostics tests*. Due to the role restrictions made by her mother, Agnes cannot access the *treatments* component.

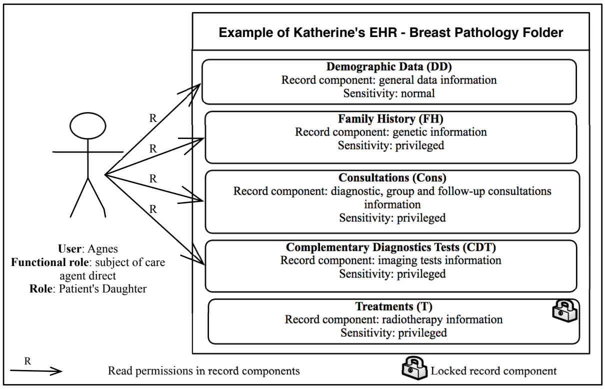
Example of Katherine's EHR - Breast Pathology Folder
Demographic Data (DD)
Record component: general data information
Sensitivity: normal
Family History (FH)
Record component: genetic information
Sensitivity: privileged
Consultations (Cons)
Record component: diagnostic, group and follow-up consultations information
Sensitivity: privileged
Complementary Diagnostics Tests (CDT)
Record component: imaging tests information
Sensitivity: privileged
Treatments (T)
Record component: radiotherapy information
Sensitivity: privileged
R
R
R
R
User: Agnes
Functional role: subject of care agent direct
Role: Patient's Daughter
R
Read permissions in record components
Locked record component

Fig. 6. Use Case related to the storyboard

5 Discussion

Regarding the proposed architecture, the storyboard and use case present a common scenario where a patient's relative, in this case a daughter who is far located from her mother, wants to follow her mother's consultations. This scenario shows how simple it can be for the patient's daughter to request and obtain access to her mother's EHR. Due to the flexibility of our architecture, any previous enrolled user can easily request for an EHR access depending only on the acceptance of the access control administrator, usually the patient.

Despite the annoyance caused by the initial healthcare institution enrollment and the difficulties associated with the usage of our model mechanisms, we believe our approach has dealt with the persistent problem of the patients EHR access. Not only for solving the long wait for the EHR access but also for solving the problem of the outdated EHR record components since the access in our model is processed as requested. In other words the patient can access and administer at any moment and anywhere the most recent EHR record components.

However, in some cases the patients do not have the capability to administer their own EHR access control, due to problems like minimal required age or mental illness. To circumvent this kind of problems our model suggests an enrollment of a legal guardian with the functional role of *subject of care agent direct* granting the legal guardian full access control over the ward's EHR.

Since the smartphone is the key for opening the access to the EHR, its loss or malfunction could bring some substantial problems. These types of problems are usually related with the user's identity proof in order to allow the re-enrollment on the healthcare institution and the certificate revocation. To solve this identity issue, we relied on the signature functionality of the citizen card since this is emitted by the patient governmental entity. This signature usage assures a strong identity proof in order to allow a revocation or a re-enrollment process.

The trust between healthcare institutions is a real problem, bringing communication limitations into healthcare information systems. This weakness limits the users to their own healthcare institution, in other words, it is not possible for two different users enrolled within different healthcare institutions to give authorization permissions between them.

6 Conclusion

With the enormous growth of technologies, the world legislation concern about health data access and the arising of patients' interest to be in control of their medical records, the authors feel it is the right time for an architecture that can give the patients the means to securely and easily access and define access control permissions to their medical records. Our proposed architecture provides for this need by granting the necessary security means as well as promoting the patient empowerment concept.

In order to allow the patient to access and manage his medical data, future work includes the implementation and evaluation of our proposed architecture within a specific case study in a real healthcare institution, more precisely on São João hospital centre, which is the second biggest hospital in Portugal; and a research about federation networks in order to solve the problem of the communication trust between healthcare institutions, as already mentioned in section 5.

Acknowledgments. This work is funded by the ERDF through the Programme COMPETE and by the Portuguese Government through FCT - Foundation for

Science and Technology, project Open Federated Environments Leveraging Identity and Authorization [PTDC/EIA- EIA/104328/2008]. and is being conducted with the institutional support provided by FMUP and DCC/FCUP and the facilities and research environment gracefully provided by the CINTESIS and CRACS (Center for Research in Advanced Computing Systems) research unit, an INESC TEC associate of the Faculty of Science, University of Porto.

References

1. Ebadollahi, S., Coden, A.R., Tanenblatt, M.A., Chang, S.-F., Syeda-Mahmood, T., Amir, A.: Concept-based electronic health records: opportunities and challenges. In: Proceedings of the 14th Annual ACM International Conference on Multimedia, MULTIMEDIA 2006, pp. 997–1006. ACM, New York (2006)
2. Council of Europe. Protection of medical data - recommendation no r (97) 5 (1997)
3. U.S. Department of Health & Human Services. Health insurance portability and accountability act (1996)
4. Pereira, C., Oliveira, C., Vilaa, C., Ferreira, A.: Protection of clinical data - comparison of european with american legislation and respective technological applicability. In: HEALTHINF 2011, pp. 567–570 (2011)
5. Republica Portuguesa. Lei acesso aos documentos da administraçao 46/2007 (2007)
6. NHS choices. How do i access my medical records (health records)?, 15/09/2010 (2012)
7. Santos-Pereira, C., Antunes, L., Cruz-Correia, R., Ferreira, A.: One way to patient empowerment - a proposal for an authorization model. In: Proceedings of the HealthInf 2012 - International Conference on Health Informatics, pp. 249–255 (2012)
8. Hyrinen, K., Saranto, K., Nyknen, P.: Definition, structure, content, use and impacts of electronic health records: A review of the research literature. International Journal of Medical Informatics 77(5), 291–304 (2008)
9. Peleg, M., Beimel, D., Dori, D., Denekamp, Y.: Situation-based access control: Privacy management via modeling of patient data access scenarios. J. of Biomedical Informatics 41(6), 1028–1040 (2008)
10. Dept. of Health & HS. The office of the national coordinator for health information technology (2011)
11. Kroll Fraud Solutions. Healthcare information and management systems society (himss) analytics report: Security of patient data. Technical report, Kroll Fraud Solutions (2008)
12. Watts, J., Yu, H., Yuan, X.: Case study: Using smart cards with pki to implement data access control for health information systems. In: IEEE Southeastcon 2010: Energizing Our Future, pp. 163–167 (2010)
13. ISO/TS 22600-2. Health informatics - privilege management and access control (2006)
14. Kuhn, R., Ferraiolo, D., Sandhu, R.: The nist model for role-based access control: towards a unified standard. In: Proceedings of the Fifth ACM Workshop on Role-Based Access Control, pp. 47–63 (2000)
15. CEN/ISO EN 13606-4. Health informatics - electronic health record communication - security (2009)

16. Joshi, J.B.D., Bertino, E., Ghafoor, A.: Temporal hierarchies and inheritance semantics for gtrbac. In: Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies, SACMAT 2002, pp. 74–83. ACM, New York (2002)
17. Ferreira, A., Chadwick, D., Farinha, P., Correia, R., Zao, G., Chilro, R., Antunes, L.: How to securely break into rbac: The btg-rbac model. In: Proceedings of the 2009 Annual Computer Security Applications Conference, ACSAC 2009, pp. 23–31. IEEE Computer Society, Washington, DC (2009)
18. Tacconi, C., Mellone, S., Chiari, L.: Smartphone-based applications for investigating falls and mobility. In: Proceedings of the International Conference on PervasiveHealth and Workshops 2011, pp. 258–261 (2011)
19. Augusto, A.B., Correia, M.E.: OFELIA – A Secure Mobile Attribute Aggregation Infrastructure for User-Centric Identity Management. In: Gritzalis, D., Furnell, S., Theoharidou, M. (eds.) SEC 2012. IFIP AICT, vol. 376, pp. 61–74. Springer, Heidelberg (2012)
20. Huang, H.-C., Chang, F.-C., Fang, W.-C.: Reversible data hiding with histogram-based difference expansion for qr code applications. IEEE Transactions on Consumer Electronics 57(2), 779–787 (2011)
21. Saint-Andre, P., Kevin Smith, A., Remko Tronon, A.: XMPP: The Definitive Guide Building Real-Time Applications with Jabber Technologies. O'Reilly Media, Inc. (2009)
22. Saint-Andre, P.: Xmpp: Core. RFC 3920, IETF (2004)
23. Paterson, I.: Xep-0206: Xmpp over bosh, http://bit.ly/xep0206 (verified on February 14, 2012)
24. Augusto, A.B., Correia, M.E.: An xmpp messaging infrastructure for a mobile held security identity wallet of personal and private dynamic identity attributes. In: Proceedings of the XATA 2011 XML: Aplicações e Tecnologias Associadas (2011)
25. Poitner, M.: G&D Secure Flash Solutions. Mobile security card, http://tinyurl.com/SDMSC (verified on February 14, 2012)
26. Maia, L., Correia, M.E.: Java jca/jce programming in android with sd smart cards. In: 7^a Conferencía Ibérica de Sistemas y Tecnologías de Informacións (CISTI 2012), Madrid/ Spain (2012)
27. Bakar, A., Ahmad, A.R., Ismail, R., Manan, J.-L.A.: Trust formation based on subjective logic and pgp web-of-trust for information sharing in mobile ad hoc networks. In: SocialCom 2010, pp. 1004–1009 (2010)
28. Santos, R., Correia, M.E., Antunes, L.: Use of a government issued digital identification card to secure interoperable health information systems. In: The 42nd International Carnahan Conference on Security Technology, ICCST 2008, pp. 1004–1009 (2008)
29. Eastlake, D.: Randomness recommendations for security, http://j.mp/rrsrfc (verified on February 14, 2012)