Role-based Access To Portable Personal Health Records

Robert Steele and Kyongho Min
Discipline of Health Informatics
The University of Sydney
Sydney NSW 2006 Australia
{robert.steele, k.min}@usyd.edu.au

Abstract—**Electronic health information systems (e.g. health record systems, clinical information systems) can assist in the provision of better health care services for patients and help doctors and other health care workers treat and diagnose patients more effectively and efficiently. One of the most important issues in health-related information systems is high information security and stringent access control for patient's health data to protect the patient's privacy and to prevent the use of data harmfully or illegally. Carrying health records with a patient, for example in a personal digital assistant (PDA) or a mobile phone, could provide greater control of the patient's health data and privacy. It can also facilitate exchanging this health data with health care workers at the point of care and only to the level desired. In this paper, we propose a portable personal electronic health record architecture which natively supports a greater level of privacy using an extended digital certificate-based approach. Other challenges to security accompanying a portable device-based approach are also considered.**

Keywords: electronic personal health records, portable health records, role-based access control

I. INTRODUCTION

Health care has increasingly seen the introduction of electronic-based support systems such as health information systems, clinical information systems, and picture archiving and communication systems. These systems can support improved health care services for patients and help doctors and other health care workers treat and diagnose patients more effectively and efficiently. Various information technologies including hardware and software have been applied to the health care field along with computing approaches such as sensor networks, security and privacy approaches, image processing and archiving, database management and access control approaches [5].

At present health care organizations employ clinical information technologies in helping to care for patients and keep electronic records which store patient's details and health-related information, called electronic health records. The electronic health record requires a high level of security and access control because it can provide great accessibility (wired or wireless and local or remote) according to the various roles of health workers in terms of the organization's defined access policy (e.g. role-based access control [7], attribute-based access control [2] and declarative and secure access control model for health data based on XML representation [10]) and can use various security implementations including key-based approaches [6, 9, 14].

The most important reason for high security and stringent access control for patient's health data is to protect the patient's privacy and prevent the data being used harmfully or illegally. If a patient's health data is kept in a shared space in the network that can be accessed by predefined users, then it requires stringent access control management for every health care worker involved in the system.

The control of a traditional electronic health record is under the management of the health care organization (e.g. a hospital or general practice) rather than the patient and the accessibility of the electronic health record is also decided by the organization keeping the health record. In addition, if any changes occur, for example, adding of new health care workers or update of the access policy in a hospital with health records of tens of thousands of patients with potentially thousands of staff, then it can require complex management to handle those changes.

Alternatively, a way to support greater privacy of every patient's health data is by keeping their data with the patient in a device the patient uses and may often take with them, like a PDA or a mobile phone. If a health record is kept in a personal device, then it could enhance the patient's ability to control their data securely and privately. It could also help patients use their information for better health care for him/herself. Of course, portable health data does imply certain security challenges itself – this is discussed in Section 3.

Carrying health records with a patient, for example in a PDA, a mobile phone or a portable encrypted USB [15], could provide greater control of the patient's health data [1, 4, 8]. It can also facilitate exchanging this health data with health care workers (e.g. general practitioners (GPs), staff in a hospital, pharmacists) just to the extent required. In this paper we describe an extended digital certificate-based approach for patient control of their personal health records (PHRs) kept in a mobile device. The mobile device such as a PDA or a mobile phone provides portability, greater privacy, and multi-functionality with a digital certificate approach to authentication and access control [11, 12, 13].

However, as mentioned above there are also challenges in using the mobile or other portable device for storing private and sensitive data like health records. If a patient loses his/her mobile device, then it raises problems such as privacy and

978-1-4244-4639-1/09/$25.00 ©2009 IEEE

security of the data in the mobile device and recovery of the data, etc. Garson and Adams [3] discuss approaches for encrypted storage, biometric access and other device-integrity approaches and these will not be discussed in detail in this paper. Instead we will focus on the mechanisms for trusted and patient-controlled access control for the patient's health data stored in their mobile device.

Section 2 describes the proposed architecture for role-based access of portable personal electronic health records. Section 3 describes how patients can control their health data access when they have interactions with health workers and the Conclusion follows.

II. ARCHITECTURE

Personal health records can contribute to improving the quality of health services and the safety of a patient. For example, the portable personal (electronic) health record (PPHR) can include a patient's information related to his/her medications and allergies and can be used to improve clinical decision-making at the point of care. However, the interaction between a patient's personal health record and a health care service provider's system requires a trusted and secure connection and it also needs flexible and dynamic processes between them. The previously published MobiPass architecture [11] can form a basis for creating a trusted interaction under a dynamic and unpredictable mobile computing environment and this PPHR architecture builds closely on and adapts the MobiPass architecture.

To briefly recap, in the MobiPass architecture a policy (MobiPolicy) is used to capture the attributes of mobile entities participating in using that particular service (i.e. each service has its own policy and each policy facilitates setting of a user's preference for services used or provided by a mobile entity). A MobiPass is a certified record of a mobile entity's particular attribute values for that service (signed by the ECA - Extended Certificate Authority). In this architecture each mobile entity would need to register manually with the ECA to have its attributes for a service certified [11].

The portable personal health record (PPHR) architecture requires secure and private management of patient health data in a portable/ mobile device. This architecture will control access of the health record through a policy for certified entities requesting access permission of part or all of the health record and the access control is defined by a patient as the owner of the health record. As such the patient can control and manage his/her health records securely and privately under their own control. Figure 1 shows the overall proposed architecture for a portable personal health record using a mobile device (e.g. a PDA or a mobile phone) for storage, and the issuing of a HealthPass, the certificate to be used by the PPHR service, under a HE (Health Entity) Policy.

Generally the approach is to have all providers and patients registered with a relevant authority. This could be the Department Of Health and Ageing (DOHA) for example in Australia, or an agency of it, and such a body would equate with a HCA (Health Certificate Authority) in this architecture. The architecture is composed of four major components: the HE (Health Entity) Policy, HealthPass, HCA (Health Certificate Authority), and PHR Manager (Personal Health Record Manager). We will now describe each component in the portable personal health record architecture (Fig. 1).

HE (Health Entity) Policy describes attributes of health (mobile) entities and its representation uses an XML schema format to allow extensible description of services and dynamic evaluation of mobile entities with high flexibility. The HE Policy would include a globally unique ID (e.g. issued by a HCA, for example DOHA) and the mobile entity describing attributes (e.g. a GP or a pharmacist's provider number, a patient number, an area of medical expertise) with other policy-related information.

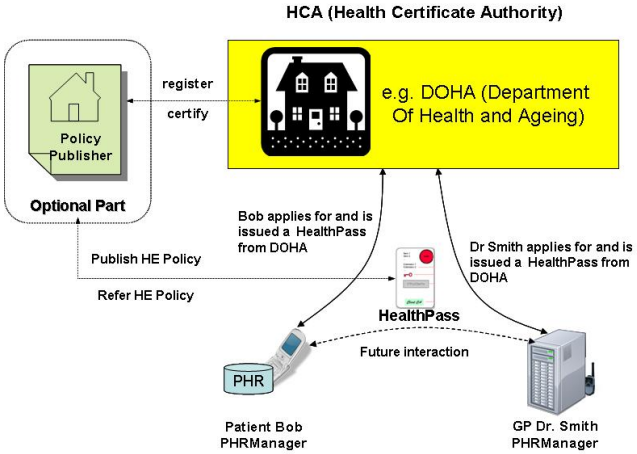

Figure 1. Overall Portable Personal Health Record (PPHR) architecture – PHR certificate/ HealthPass issuing

HealthPass, migrated from a passport concept (as per the MobiPass architecture) and issued by a HCA, it is a digitally signed description of a particular health entity's attributes (an extended digital certificate) and enables trusted and flexible interaction in a dynamic mobile environment. The HealthPass representation is like an XML instance (e.g. attribute and value pair) and it has information such as the identity of the HCA (e.g. HCA-ID), identification of the HE Policy (e.g. HE Policy-ID) and signed health entity attributes, digitally signed digest value by the HCA (e.g. a public key), digitally signed digest value of the whole HealthPass by the HCA, and description of valid time of the HealthPass (see [11] for details of the extended certificate approach).

HCA (Health Certificate Authority) issues digital certificates (HealthPasses) to registered, accredited, and trusted parties previously unknown to each other (e.g. the HCA could be the Department Of Health and Ageing (DOHA) in Australia). Its functions are evaluation of mobile entities based on the HE Policy and production of digitally signed results of each entity evaluation (e.g. a HealthPass for the entity). The HealthPass can have certified and non-certified sections.

For the present architecture, HCA will only issue a HealthPass for a mobile entity by an offline application and authentication process for the applicant. In addition the HCA can also play a policy publisher role. Alternatively a separate policy publisher can exist, optionally as in Fig. 1. If a real business model requires a separate policy publisher, then the

optional element will be involved in the PPHR architecture to play its characteristic role (e.g. create and publish policies).

PHR Manager (Personal Health Record Manager) is software present on the mobile device, and is invoked if and only if two mobile entities are *physically linked* together for interactions involving PPHR access but can be invoked for wireless interactions that do not involve the potential for private information access (see Section 3). It performs all necessary trust establishment operations in the PPHR architecture as follows:

1) Validity checking and retrieving the public key of a HCA
2) Verification of an incoming HealthPass
3) Enabling its HE Policy
4) Setting service preference rules to HE Policy
5) Applying the rules to allow the desired access to a personal health record or other wireless interactions

Detailed steps from 1 to 5 were discussed in [11] and we will focus on description of the access control of personal health records using HE policy in steps 2 to 5. In the PPHR architecture, the PHR Manager verifies an incoming HealthPass to determine whether it is a registered entity (e.g. a GP, a dentist, or a pharmacist) or not. Then the PHR Manager allows access to the PPHR to the access level determined by the patient's preferences (e.g. a GP can see all of the health record including personal information, medication, and diagnosis, etc).

At this step, the architecture requires a way to map a given health care worker's role to parts of the record that they should be able to access. Describing this in detail is beyond the scope of this paper, but can make use of the XML-based role-based access control framework discussed in [10].

III. Patient Control of Access to Their Portable Personal Health Record

The MobiPass architecture [11] creates dynamic and flexible interaction between unknown mobile entities under an unpredictable wireless environment. However, the PPHR architecture handles sensitive and private health records in a variant way to the MobiPass architecture and it makes use of two different modes: (1) PPHR access mode is invoked *only* when two mobile entities are *physically linked* together as discussed in the previous section; and (2) wireless mode is invoked when the patient mobile entity recognizes a wirelessly incoming HealthPass which is health service related but not related to *accessing* of any personal health record data (e.g. medicine availability information from a pharmacy). Physical device docking is required for any interaction with any possible outflow of individual PPHR-related data to further enforce privacy and security. We will describe the application of the architecture for example purposes, between a patient and 1) a GP, 2) a dentist and 3) a pharmacist.

A. Example 1: Bob consults a general practitioner

Bob is a patient and Dr. Smith is a GP. Bob with his mobile phone goes to see Dr. Smith at his surgery or this could be in an out-of-office (e.g. emergency situation). In his mobile phone with the PHR Manager, Bob has his HealthPass, previously registered with the HCA (e.g. could be DOHA in Australia). Bob's mobile phone also contains his actual personal health record. Let's ignore the administrative flow of GP appointments here (e.g. Bob sees a receptionist, Dr. Smith opens Bob's file from his database for consultation at his office). Instead, Bob physically links his mobile phone to Dr. Smith's device that can then enable the respective PHR Managers to interact in the PPHR architecture whether Dr. Smith is at his office or in an out-of-office scenario (e.g. an emergency situation for Bob in any location).

Next Dr. Smith's PHR Manager sends Dr Smith's HealthPass to Bob's docked mobile phone and Bob's PHR Manager sends Bob's HealthPass to Dr. Smith. After exchanging their HealthPasses with each other Bob's PHR Manager authenticates Dr Smith as a doctor and accordingly allows Dr Smith to access Bob's personal health record saved separately in Bob's mobile phone (e.g. applying Bob's rule for Dr. Smith's access to Bob's personal health record in terms of Dr. Smith's role). The steps from Step 1 to 7 in Fig. 2 show Dr. Smith's access process of Bob's personal health records via the PHR Manager and HE Policy and HealthPass. In this way Bob has a certified basis to trust the GP and grant data access whether the GP is at his office or in an out-of-office scenario and can then authorize access of his PPHR according to Bob's rules.

The detailed access control for health care service providers has not been discussed here in detail. The access authorization of personal health data like read, write and delete would be provided for security and privacy of the health data and is set by each user for their own data. In addition, the access and transaction logs should be audited to a portable personal health record system. These issues have been studied broadly and we will not discuss them in detail in this paper.

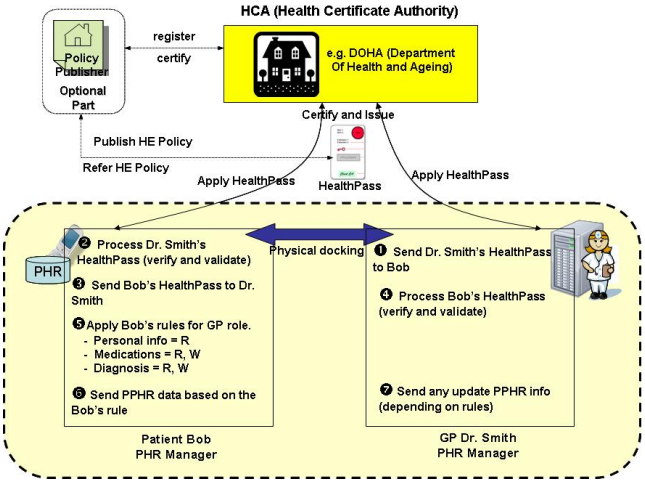

Figure 2. Personal health record interaction between a patient and a doctor (a general practitioner).

B. Example 2: Bob consults a dentist

Bob is a patient who needs dental care and Alice is a dentist. Bob goes to see the dentist Alice with his mobile

phone. In his mobile phone with PHR Manager, Bob has his HealthPass registered with the HCA and Alice likewise has a HealthPass certifying her dentist role and relevant attributes. The process of both mobile entities, each with a HealthPass, is the same as an Example 1 but Bob's rules for a dentist role would be different from those for a doctor, as a dentist does not need to access Bob's full detailed personal health record such as medications, diagnosis, medical history, and GP notes.

Bob's rules for Alice's role would be {personal info = Read, dental history = Read, Write}. With the rules, Alice can access just Bob's personal health record information relevant to dental treatment. The steps from step 1 to 7 in Fig. 2 show the same access process of Bob's personal health records except for a different HealthPass in this example.

C. *Example 3: Bob receives information from a pharmacist*

After Bob visited his doctor, he goes shopping to a shopping centre where there is a pharmacist that has registered with a HCA to obtain their HealthPass. The pharmacist sends any medication information through the local wireless network so that nearby shoppers with a mobile phone can detect it. At this time, Bob's PHR Manager verifies and validates an incoming HealthPass from the pharmacist and sends back his HealthPass to the pharmacist when the pharmacist's HealthPass is verified to be a trusted one. Then in terms of his preference settings for the pharmacist's service (e.g. rules might be set to only receive information on medications for which Bob has a current prescription), Bob can receive inflow information from the pharmacist without giving any access privilege to his personal health record information. As there is no physical docking to a PPHR-enabled device, no access to Bob's personal health records for information outflow is possible, hence ensuring PPHR security.

However, if Bob had a prescription in his personal health records from his doctor and he wanted to purchase medication in the pharmacist, then Bob needs to physically link his mobile phone with a PPHR-enabled device in the pharmacist to interact together. The authentication and authorization of the pharmacist is the same as both Examples 1 and 2. After the interaction, the pharmacist provides Bob's medication and may update the prescription in Bob's personal health record with a 'filled' status – for example, "medication A was dispensed to Bob as prescribed on April 5 2009".

Examples shown in this section describe the patient control of their personal health records in a portable/ mobile device. Compared to personal health records stored remotely or on a PC, this PPHR architecture supports greater patient control of access to their health records and provides a more secure level of privacy for the patient and their sensitive data.

However, there are other research issues to achieve stringent access control and a higher level of security and privacy for personal health records particularly in the case of device loss and these issues have not been discussed in this paper. But the issues would be 1) secure and consistent data backup when the mobile device is stolen, broken or lost, 2) encryption of health data while stored, 3) secure interaction with other health information systems (e.g. hospital information system) and 4) interoperability of health records.

IV. CONCLUSION

This paper has proposed a portable personal health record architecture to provide patients with greater control over third party access to their personal health data. This architecture achieves trusted interaction based on use of extended digital certificates (HealthPasses) issued by a health certificate authority (HCA). To support flexible interaction between mobile entities and extensibility of policy (HE Policy), in this architecture an XML-based representation is used for HealthPasses and to set access control preferences based on roles of health care service providers. In addition, this architecture supports two modes: trusted and flexible interactions between physically linked entities for secure access control of PPHR data and trusted wireless interaction for interactions not involving the outflow of private personal health record information.

REFERENCES

[1] S. Endsley, D.C. Kibbe, A. Linares, and K. Colorafi, "An Introduction to Personal Health Records," Family Practice Management, pp. 57-62, May 2006.

[2] K. Frikken, M. Atallah, and J. Li, "Attribute-Based Access Control with Hidden Policies and Hidden Credentials," IEEE Transactions on Computers, vol. 55, pp. 1259-1270, 2006.

[3] K. Garson and C. Adams, "Security and Privacy System Architecture for an e-Hospital Environment," Proceedings of the 7th symposium on Identity and trust on the Internet, Maryland, USA, pp. 122-130, 2008.

[4] J.D. Halamka, K.D. Mandl, and P.C. Tang, "Early experiences with personal health records," Journal of American Medical Informatics Assoc., vol. 15, pp. 1-7, 2008.

[5] R. Haux, "Health Information Systems – past, present, future," International Journal of Medical Informatics, vol. 75, pp. 268-281, 2006.

[6] G. Kambourakis, I. Maglogiannis, and A. Rouskas, "PKI-based Secure Mobile Access to Electronic Health Services and Data," Technology and Health Care, vol. 13, pp. 511-526, 2005.

[7] D. Kulkarni and A. Tripathi, "Context-aware role-based access control in pervasive computing systems," Proceedings of the 13th ACM symposium on Access control models and technologies, Estes Park, USA, pp. 113-122, 2008.

[8] C. Pagliari and B. Fernando, "Portable personal health records: can they improve patient safety?," Prescriber, vol. 18, pp. 9-10, 2007.

[9] U. Sax, I. Kohane and K.D. Mandl, "Wireless Technology Infrastructures for Authentication of Patients: PKI that Rings," Journal of American Medical Informatics Assoc., vol. 12, pp. 263-268, 2005.

[10] R. Steele, W. Gardner, D. Chandra, and T.S. Dillon, "Framework and prototype for a secure XML-based electronic health records system," International Journal of Electronic Healthcare, vol. 3 pp. 151-174, 2007.

[11] R. Steele and W. Tao, "MobiPass: A Passport for Mobile Business," Personal and Ubiquitous Computing, vol. 11, pp. 157-169, 2007.

[12] W. Tao and R. Steele, "Trusted Mobile Interaction via Extended Digital Certificates," The 2nd IEEE international Symposium on Dependable, Autonomic and Secure Computing (DASC06), USA, pp. 284-292, 2006.

[13] W. Tao and R. Steele, "A Local Broker Enabled MobiPass Architecture for Enhancing Trusted Interaction Efficiency," ACSC 2008, pp.55-61, 2008.

[14] F.K. Uckert and H. Prokoschl, "Implementing Security And Access Control Mechanisms For An Electronic Healthcare Record," Proc. AMIA Symp., pp. 825–829, 2002.

[15] A. Wright and D.F. Sittig, "Encryption Characteristics of Two USB-based Personal Health Record Devices," Journal of American Medical Informatics Assoc. vol. 14, pp. 397-399, 2007.