RFID enabled smartcards as a context-aware personal health node

D.T. Parry, A. Narayanan
School of Computing and Mathematical Sciences, Auckland University of Technology,
Private Bag 92006, Auckland, New Zealand

Abstract

Smartcards for the storage of medical information are not new [1]; however, their use has been constrained. The major problems are that cards have limited memory, may use a non-universal framework and are liable to loss or theft. When dealing with a single health provider these disadvantages outweigh potential advantages, such as availability at many points of care and reassurance of confidentiality. This work focuses on the requirements for a smartcard that acts as a personal health node, controlling access to data rather than holding the data itself. This approach allows interaction with multiple health provider systems, potentially complex data sharing and access control requirements, and emergency needs. Previous work has emphasised the need to use structured data sources in limited data space [2]. The data stored on the personal health node smartcard will comprise an encoded XML document that includes pointers to the location of clinical data, access control rules concerning that data and a minimum emergency subset of this data. The use of radio-frequency identification (RFID) technology allows increased flexibility, both in the ability to read data without contact and the opportunity to make data reading conditional on other factors. One particularly important aspect is the ability to make data accessible only when another card – e.g. that of a trusted clinician or advocate, is also within range of the reader. The readers may be incorporated in mobile devices, giving assurance of control of access to data anywhere and improving the acceptability of data sharing [3].

1. Introduction

Sharing information between health providers and providing appropriate information at the point of care have become increasingly important aspects of health information systems. However, as patients move, systems for sharing are becoming increasingly connected to developments in mobile health. Mobile health, or M-health, has been defined as “mobile computing, medical sensor, and communications technologies for health-care” [4]. In this paper, the mobility of the patient is emphasised over the mobility of the care. This paper is concerned with the need to access patient data in a timely, effective and secure manner at the point of patient care. Based on the idea of the “Hippocratic database” model of access control [5] it also tries to demonstrate a method of health information access that can support patient and health provider preferences in terms of access control.

Sharing of health data can be accomplished in two main ways. Firstly all health providers may be encouraged or forced to share data and provide access to a central data repository. This approach is very attractive in many ways, especially for universal health care systems. There are potentially economies of scale, the ability to perform audit and research, and equity of access. It can be argued that this approach has been adopted by the NHS in the UK, but problems of confidentiality and mechanisms for opting out of an universal system [7] continue to dog the “connecting for health” [6] project. Particular issues arise with the nature of confidentiality and the mechanisms needed to opt-out of a universal system.

Secondly, health data can be shared between health providers and patients using a messaging protocol such as HL7. In this approach, the patient needs to be identified and the access control rules identified, often on a case-by-case basis. Data is then transferred between health providers as part of the health care pathway. The existence of such messaging systems and infrastructure to support them has been a major cause of the high level of computerisation of the New Zealand primary care system [8]. Ambitious grid computing approaches [9] have also been proposed for data sharing and analysis.
Smart card technology has been used for many secure applications, such as credit and debit card systems and has also been used as a means of holding and securing personal medical data [10]. Smart cards generally contain an authentication mechanism along with a minimal data set. Linking smart cards to web-based records is not new in the context of health information management [1].

Recent developments in Radiofrequency identification (RFID) and auto identification technology [11] offer a number of advantages over traditional electrical-contact, or magnetic stripe-based smart cards:

1. Contactless and non-line-of-sight reading is possible
2. Multiple cards can be read in a reader at the same time

Advantage 1 allows cards to be located on unconscious or unresponsive patients in an emergency situation. Advantage 2 allows multiple-card authentication methods and the potential, to modify access to records in the physical presence of trusted professionals. This proposal describes a set of systems and approaches that will allow people to define access to their data in a natural, accessible and secure way, as well as supporting healthcare providers and allowing them to fulfil their legal and clinical obligations.

In practice we believe this approach will allow patients to be assured of the privacy and availability of their personal health information and simplify the access control and auditing.

2. A vision of personal healthcare

Healthcare systems are moving from the generation of systems that lock health data into organisational silos to ones that allow individuals to access data across many systems. In order to implement this vision a number of assumptions have been made:

- Health data management is based around the person
- Each person deals with multiple providers of health, and multiple users of data, all health data will not be in the same place.
- Each person has individual rules for who gets access – this includes the health sector, NGOs and family and friends – and these rules may also depend on personal trust relationships.
- Healthcare takes place in many settings, including the home.
- Access technology will be open but auditable and secure.

3. Problems with current healthcare systems

Healthcare costs and expectations continue to rise. In addition, even in countries with a “universal” health care system such as New Zealand, each patient may deal with large numbers of different healthcare providers and funders. Figure 1 shows some of the organisations that a people with spinal injuries deal with.

The corollary of this is that each of these providers may have information systems, which store information needed for patient care in incompatible “silos”. It may be that many health providers are completely unaware of the presence of potentially critical information held in another system.

At the same time, the fact that information sharing between organisations takes place at all is relatively poorly understood by many patients [3]. Currently systems are rarely able to record patients’ preferences for sharing information at a useful level of detail. This consent may need to be updated quickly, for example when a new referral is being made, or after discussion with clinical staff.

Security systems for health computing systems have very wide variations in the level of authentication required. Many health providers are based in very small organisations, and upgrading security can be a relatively large burden. In addition, there exists the danger of patients and clinicians ending up authenticating themselves with many different methods to many different systems simply in order to access critical data. Additionally, if relatively secure health providers share data with insecure health providers, then the potential for more general security breaches becomes more serious.
Access to critical information about a person’s health may not be available if the patient is unable to communicate, and away from their regular health providers. A national minimum dataset is available linked to the National health index (NHI). However this requires identification of the patient and their NHI. In addition some people may require additional information to be provided in an emergency – for example pregnant women.

4. Methods

4.1. Design principles

The RFID-based smart card must provide a number of features. It should allow patients to provide access to health data held in different systems, it should allow patient’s preferences for information sharing to be recorded and altered, it should support a simple and secure authentication and audit process, and it should be able to be accessed in many different locations, by all health providers and legitimate consumers of health information.

4.2. Technology

Generally, smart cards have relative small memory spaces. Readily available UHF RFID cards have a read range of between 50cm and 2 metres. Cards include different areas of memory, including permanent data such as a unique identification number, secure data area and read/write data. Such tags are relatively cheap- in the $1-10 NZD range. Card readers tend to be more expensive at around $500-$1000 NZD. Card readers can be battery or mains-powered and are starting to become available integrated with mobile devices and phones.

In terms of implementation each area where health data needs to be accessed would have an RFID card reader which implemented suitable security algorithms (described below).

Each person who would have contact with the New Zealand health system would be issued with a card with the following data:

- Encrypted PIN (to allow personal access to and control of card contents)
- Authentication keys (to allow others to access card contents)
• Minimum emergency dataset e.g. allergies, current medication
• Pointer to data storage areas – GP, ACC, DHB and other providers, based around HL7 CDA
• An XML-based store of data sharing preferences of patient

As part of the system, clinicians and other employees of health organisations will also be issued with cards. When cards of those requiring information and the card of the patient are both present in the reading field of the RFID reader, the reader would authenticate access at the appropriate level (Figure 2). This approach could also be extended to multiway approval for example if a support person needs to be present. It would also be possible to use the reader infrastructure to read e.g. “smart” pill boxes, that record compliance with treatment, but only in the presence of authorised people.

The data retrieved from the cards would be a pointer to health data held in a health provider’s system along with the necessary access procedures, which may include confirmation of biometrics. If preferences of the user are set at a less permissive level, a bloom filter approach [12] will allow the health provider to check if a particular health provider holds any information about the patient. Bloom filters widely used in spell-checking applications. They allow checking to see if a string exists within a coded list, without allowing an easy decoding of that list. In this application, it means that a provider can send a string to the coded list, without having the presence of any other provider information being revealed. This is superior to a traditional string-matching approach which would reveal all of the providers listed, if a search was performed on it. In an emergency situation, health professionals could access the minimal dataset and potentially other data that the patient is willing to share without PIN entry by the patient, but this access would be recorded.

As RFID tags can also be written to by certain readers, the data sharing preferences of the patient and the pointers to health data can be updated during the consultation, along with an audit log on the card. Data may also reside in such personal health record systems as “Google Health” or Microsoft’s HealthVault.

4.3. Authentication

An authentication PC (APC) attached to the reader verifies card (Internal authentication) using the following procedure:

• APC sends a random number to card encrypted using card’s public key.
• Card deciphers using its private key.
• Card return the random number encrypted using APC’s public key.
• APC deciphers using its private key. If random number is the same, APC knows card is authentic since only card’s private key could have decrypted the random number.
• Card verifies APC (External authentication)
• Card sends a random number to APC encrypted using APC’s public key.
• APC deciphers using its private key.
• APC returns the number encrypted using card’s public key and APC’s private key
• Card decrypts using APC’s public key and card’s private key. If random number is the same, card knows that APC is authentic.

Unique random numbers used safeguard against ‘replay attack’ Current RFID enabled Passports use a similar approach and although there has been some debate about the robustness of the security, recent work suggests that they are able to support an acceptable standard of security [13].

5. Implementation approach

Mrs. S goes to see her family doctor about her type 1 diabetes. At the physician’s office she and her family doctor Dr. H, place their smart cards within range of the reader. The authentication computer identifies the presence of both – in future systems biometric data may confirm this - and searches through Mrs. S’s XML access document on the card to identify data classes which are available to Dr. H.
The card also has an XML document that contains details of where data is available on other provider systems that Mrs. S would like to share with Dr. H.

One of these items is a laboratory test that reveals that Mrs. S is pregnant. Dr. H. asks if she can get access to her past obstetric history. Mrs. S. decides that while she is happy for Dr. H. to have access, other members of the practice will only see a limited view of the data but all of the practice can see administrative information concerning her visits to her obstetrician Dr. Y.

Mrs. S.’s Smart card is updated with this new access rule, and a bloom filter hash table reconstructed so that other people reading the card are allowed to check to see if they are allowed access but not what it is they cannot access. In addition the fact that Mrs. S. is pregnant is added to the minimum data set on the card, accessible to all readers. A log entry for the access and update is added to Mrs. S.’s dataset located on a secure data repository, and this replaces one of the log subset items on her card.

At the pharmacy, Mrs. S. authenticates herself to the pharmacy system with her card. The pharmacist is able to confirm her identity, and that of the prescribing doctor, along with the minimal dataset, but does not have access to any other records. The co-payment system checks her insurance policy via the administration document on the card and the approval occurs.

6. Discussion

Using RFID-enabled smartcards, a “personal health data repository” could be implemented using current infrastructure, and new services and models of care – for example data sharing within families – to be defined. In some ways it can be seen as an “electronic wallet” for all the data sharing rules and data locations that currently patients and clinicians have to navigate. Although strong security is necessary, this approach does not put any patient-critical data at risk, it simply points to where the data is and who can see it. By basing access controls and data locations around XML documents, the schemes can be as complex or as simple as the patient wants, and it may be that a “menu” of access rights may be presented and made available from the card vendors.
6.1. Advantages over current systems

This system enables data sharing and transfer to be simplified and controlled. Most importantly the control mechanism is transparent to and owned by the patient. For the health provider, this allows efficient transfer of critical data without allowing intrusive access to systems or building complex interfaces.

6.2. Challenges

The main challenges to adoption include cost including the cost of replacement cards – a back-up of the current state of the card should be stored in a secure repository. The level of take-up by patients and providers, particularly for the reading hardware, may be an issue as standardised approaches would be best. Security of RFID cards is still an active area of research [14] and problems such as ensuring a digital credential infrastructure exists, along with issues of local caching of biometric data and potential eavesdropping need to be addressed.

7. Conclusion

The Patient Data home running on an RFID enabled smart card allows current infrastructure to be reused, and new services and models of care – for example data sharing within families – to be defined. In some ways it can be seen as an “electronic wallet” for all the data sharing rules and data locations that currently patients and clinicians have to navigate. Although strong security is necessary, this approach does not put any patient-critical data at risk, it simply points to where the data is and who can see it. By basing access controls and data locations around XML documents, the schemes can be as complex or as simple as the patient wants, and it may be that a “menu” of access rights may be presented and made available from the card vendors. The business opportunity lies in making the cards and data formats available and facilitating the development of systems to use them.

8. References

