Who Would You Trust To Identify You In Accessing Your Health Record?

Prof William J Buchanan[2], Cassie Anderson[1], Adrian Smales[2], James Varga[1], Niall Burns[2], Omair Uthmani[2], Dr Lu Fan[2], Owen Lo[2], Alistair Lawson[2],

Contact Email: w.buchanan@napier.ac.uk

[1]miiCard, 5 Gayfield Square, Edinburgh EH1 3NW 5EA
[2]School of Computing, Edinburgh Napier University, 10 Colinton Road, Edinburgh EH10 5DT

Abstract. Within health and social care there is a strong need to provide access to highly sensitive information, and one which requires high levels of identity assurance. This paper outlines a joint project between Edinburgh Napier University and miiCard [10], and which aims to provide trusted identities in order to support both the access to health records, and also support the requirements to share information across domains. It provides an overview of some of the key issues involved in proving identity within the access to health care records, and also the proposed framework, safi.re, that is being used in the joint project.

The paper also includes the results from a survey on the attitudes to the access to electronic health records, and shows that users in the survey often require high-levels of assurance in the identity provision that is used in health record access. A key finding is that users mostly prefer to use an identity provision method that they control, along with one which has high levels of assurance, and this re-enforces the viewpoint that LOA (Level of Assurance) 3+ should be used to control the access for public access to electronic patient records. The paper outlines the differing levels of assurance and proposes that LOA 3+should be the minimum requirement for health record access for citizens.

Keywords: Information sharing, trust, governance, miiCard, online identity verification

1 Introduction

Current information architectures have been designed to keep data within well-defined confines, where every user must authenticate themselves into the domain and gain rights for that specific domain. This has meant that users end-up with a whole range of user names and passwords. Fortunately this approach is changing for many reasons, including:

- **Bring-Your-Own-Device**. The idea of all network connections being constrained by an organisational firewall is now fading as users bring their own devices to work, and where they can breach the firewall by using an alternative network connection, such as over 3G.

- **Bring-Your-Own-Identity**. This concept starts to define the identity that users are willing to use when they authenticate into systems.
- **Hybrid IT and Cloud Infrastructures**. Before the advent of Cloud Computing many organisations setup their own network and server infrastructure, employing their own authentication servers. The current trend is to start trust cloud services, such as for network storage, identity and Web provision.
- **Trust-based Web Provision.** A key factor in the access to Web-based services is the concept of trust, where users can define their own trust relationships with on-line service providers.

The core of the Internet provides little in the way of proving the identity of anything, which makes it difficult to prove identity online. Traditional methods rely on risk-based approaches that do not provide the high level of trust needed to enable us to access and share highly sensitive information like healthcare records. The identity infrastructure that we have created, though, is based on digital certificates – known as the PKI (Public Key Infrastructure), which is flawed as very few people actually understand how it works. With PKI, users are meant to prove their identity by electronically signing something with their private key, and then use their public key to identify themselves. This normally requires access to digital certificates, which few people understand how they are actually used to verify identity. For example, Zissis [7] interviewed 121 IT-literate young people and found that the most of them did not understand even the basic concepts of cryptography, and he concluded that the majority could not effectively manage digital certificates.

2 So who do we trust?

Within health and social care there are often major barriers for users in gaining access to their health records, especially in the fact that existing systems were built to identify users who have formal roles within the health care infrastructure, with very little methods for external users to authenticate themselves. One way to support external user access is to use organisations which can identify the user, such as from their email access, or from social networking activity. Google and Microsoft are in a strong position in providing identity through their cloud-based email system, while Facebook, Twitter and Linkedin can provide identity verification for their social network infrastructure.

Whilst these companies have fairly good security infrastructures, through things like one-time passwords and for providing usernames and passwords, they are normally used for low-risk access to documents. There is a strong need for enabling identity proofing purely online, to the same standard as an in-person passport/ photo ID check. Thus, in the cases of access to highly sensitive information, especially within health records, there is a strong need to provide multiple factors to prove someone’s identity.

The end game, though, is that citizens will take much more control of their own data, and personal storage providers, such as mydex [8], and for personal health records, such as with Sitekit’s e-Red Book [9], could show the way for a future where the citizen will have more control of their own health records. With a more citizen- focused approach, the citizen might actually own their data, and then can define who they trust to get access to it. This type of approach overcomes many of the concerns around security and privacy, and might actually see us progress from the electronic health record (EHR) to personal health record (PHR).

Within new information architectures the definition of federated identity provision is likely to become a key factor, especially within application areas which span different domains, such as for information sharing across the public sector, and in systems which integrate with the citizen and third sector organisations. The integration of identity providers such as Microsoft Live, LinkedIn, Twitter, miiCard, and so on, are likely to be one method which will allow the wide-scale adoption of services within the trust infrastructure. So, with the large-scale adoption of the OAuth 2.0 protocol [6], there are now many identity and services providers integrating their systems to form an overall trust framework.

A feature of any trusted infrastructure is that the owner of the data is clearly defined, and this entity can differ from the actual governance of it. For example, in a health care system, the owner of the data could be the citizen, and the governance of the data is defined by the health care provider (such as the National Health Service (NHS) in the UK). In a full trust infrastructure, the citizen could have full rights to define who had access to their data, and within a health and social care infrastructure, the requirement for highly trusted identity information is key, providers such as Google and Windows Live can only give a small amount of assurance on identity. It is important to use trusted identity providers such as miiCard to establish a user is who they say they are, to the level of an in-person identity check. This high level of assurance in identity is required for high-risk document access.

3 High Assurance Levels

Figure 1 outlines a current architecture in which Edinburgh Napier University and miiCard[1] are working on, and which has been used in several health-care related projects [1-5]. It is named safi.re (Structured Analysis and Filtering Engine), where users query a **Trust Framework** for the claims required to gain access to a service. They will then go and collect the required identity and attribute claims from the trusted providers, and give these back to the **Governance Engine**, which contains rules which define whether that user, based on role, relationship, consent and delegation, has access to the service.

Within health and social care there is a requirement from both the health care infrastructure, and from the user, that there is a strong level of security involved. Having

[1] **miiCard** (My Internet Identity) is a global Identity as a Service solution that proves ‘you are who you say you are’, purely online, in minutes and to the same level as a physical passport or photo ID check. Through a patented process that leverages the trust between an individual and their financial institution, miiCard establishes identity to Level of Assurance 3+ and meets Know Your Customer and Anti-Money Laundering identity guidelines.

strong authentication and assurance in identity of all users will increase the trust in the system/service.

As Figure 2 illustrates the levels of assurance range from LOA (Level of Assurance) 1, with the validation of an email address, up to LOA 3+, which verifies identities to a passport/ photo ID standard and uses strong, multi-factor authentication to ensure the true assertion of that identity. As will be seen in the survey in Section 4 there is a strong requirement for the usage of an LOA 3+ identity proofing service like miiCard for high-risk areas, and that the checking method should conform to:

- **Verified Attributes**. This provides the accessing of personal identities such as date of birth, phone number, address, device, signatures, qualifications and professional memberships. Each verified element, or attribute, should have been checked with a third party data source to ensure its integrity.
- **Active Revalidation and Bank-level Security.** Active Revalidation is a key factor, which should update the information on a regular basis, to ensure the identity information is always up-to-date to provide traceability. Within a health care service, users are accessing high sensitive information, thus bank-level security and a number of member-set features are required to protect access and ensure true assertion of the identity, including: multi-factor authentication, Enhanced Security Icons, strong passwords, Individualised Strong Encryption (ISE^{TM}), Enhanced SSL Certificates, auto session locking, device based security, activity alerts and detailed activity logging.
- **Strong Authentication**. This requires that the identity provision is provided in the form of hard and soft tokens, biometrics, location and device authentication are added as required to protect member accounts and ensure the true assertion of the identity.

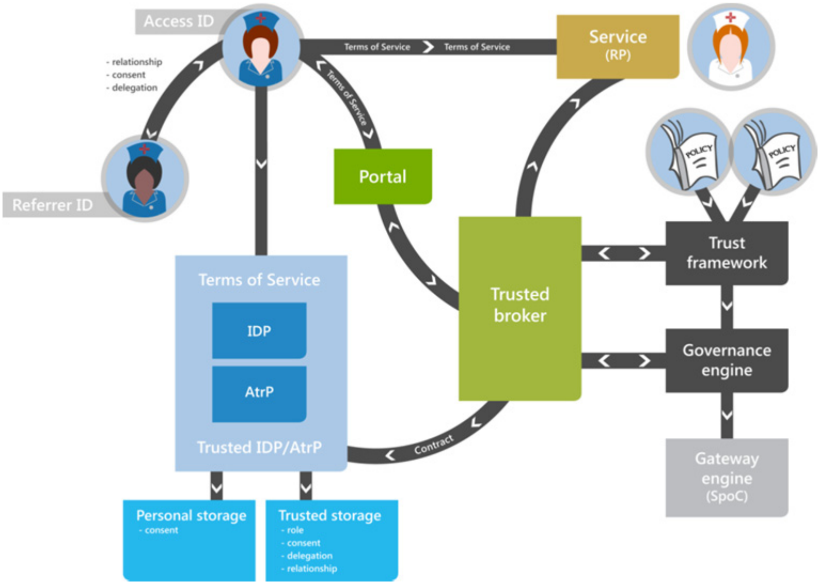

Fig.1. Trust, Governance and Access Framework

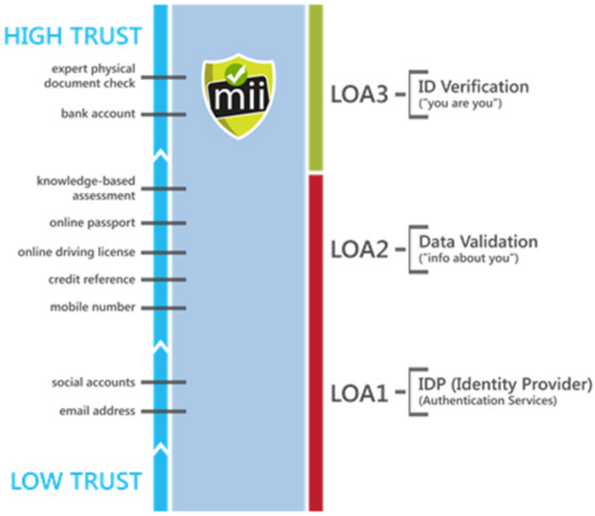
HIGH TRUST
expert physical document check
bank account
knowledge-based assessment
online passport
online driving license
credit reference
mobile number
social accounts
email address
LOW TRUST
mii
LOA3 - ID Verification ("you are you")
LOA2 - Data Validation ("info about you")
LOA1 - IDP (Identity Provider) (Authentication Services)

Fig.2. Levels of assurance in identity

3.1 Trust Levels

Safi.re defines trust levels within a trust framework and matching these to identity providers and attribute providers. A key factor is the definition of the identity checking properties of the associated providers (such as whether they support bank validation, passport checks, password cycling, geo-location verification, and so on). These can then be rated into levels for the access to services based on the level of trust. Table 1 and Figure 2 outlines some of these trust levels, where providers such as miiCard, along with Government Identity Services and EU e-Passport Schemes, can provide the highest level of assurance around a user's identity entirely online. These levels of assurance are important within a health and social care infrastructure, especially in the access to sensitive information, which would require the highest level of identity assurance.

Table 1. Trust Levels for Identity

LoA in Identity	Identity Providers	Attributes Supported
LoA 1	Social accounts Email addresses	[Username], [Password]
LoA 2	Knowledge Based Assessment Upload scans of ID documents Data bureau checks	[Username], [Password], [Document Check]
LoA 3	miiCard Government Identity Services EU e-Passport Scheme Offline Physical ID Document Check	[Username], [Password], [Document Check], [Bank Check], [Geo-location], [Mobile Verification], and so on.

4 e-Health Survey

Many industries have embraced the Internet, especially in the usage of electronic mail, social media, and Web-based infrastructures. These have often transformed their operation, such within the banking sector and education, where electronic methods of communication have replaced traditional methods. One sector that has often lagged behind is in health care, who are often not up-to-date with their implementation of IT, where it is often unusual to have e-mail contact with a GP, or to be able to video conference with medical consultants. Thus, in May 2013, Edinburgh Napier University conducted a survey on the attitudes on the access to electronic health records in the UK. With 477 respondents, 79.04% of participants said that they wanted full access to their health record, while only 16.98% wanted a summary of their record, and only 3.98% wanted no access to their health record, at all. This shows that there is a strong demand from citizens to actually access their health records.

Of the reasons that citizens would most like access the main reasons were:

- Check its accuracy (36.07%).
- Recall key information (32.64%).
- Add comments (15.24%).
- Make amendments (11.45%).

There is thus a strong demand from citizens to make checks on their records, along with making their own notes on their record. When asked for who should own the health record, 60.80% reckoned that the citizen should own them, which goes against the limited access that many UK citizens have to their record today, whether it be electronic or paper-based. The two main barriers on allowing access to their health record, where identified as poor security within the health care infrastructure (55.56% quoting as a strong reason), and the cost of building the IT infrastructure to support citizen access (44.89% quoting as a strong reason).

As might be expected, the main services that users would like are to view their health record (29.52%), and, closely followed by, booking appointments on-line (29.19%). These perhaps highlight a growing requirement for citizens to interface with the health care infrastructure using electronic methods.

If there is a demand for online access to services, the survey prompted for the identity provider that they would most trust. For this the results in Figure 3 show that the traditional identity providers such as Facebook, Microsoft Live, Linkedin, and so on, are not the ones that users most trust to provide their identity. It can be seen that users are most keen on using a security tool that they control in some way, and one which has a strong security procedures, similar to online banking security measures. Thus it can be seen that users are demanding a higher-level of trust for the provision of their identity in the access to their health record. This is likely to be because they want to protect the security of their own record, while supporting a fairly easy method of access. A Government method of access, while trusted more than the traditional identity providers, trails behind these methods, which perhaps shows that, while trusting the identity provision, it might not be the easiest, or most controllable, method.

When asked about the identity provider that they least trusted (Figure 4), the majority of users identified that Facebook as the least trusted (56.2%). This perhaps shows that users are becoming more educated in the understanding of trust and the way that organisations use the data gathered on individuals. Thus a provider which does not focus on identity provision, may have other reasons for proving identity, such as determining the services that they are gaining access to, so as to push relevant advertising material to them. It can also be seen from Figure 4 that Twitter and Linkedin score highly on the least amounts of trust in identity provision, which could point to recent security problems within their infrastructure, where passwords have been compromised. It is thus a changing landscape of trust, and it can often end up being a 1:1 relationship that users have with their trusted organisations, and which can change quickly depending on changes in the environment.

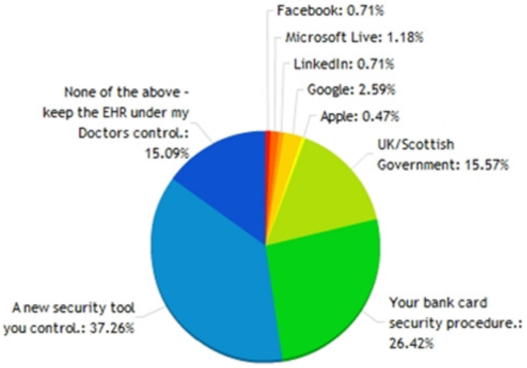

Fig. 3. Identity Providers that users would **most** trust to access their electronic health records

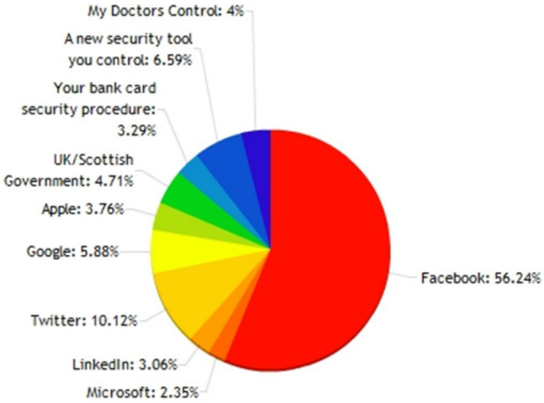

Fig. 4. Identity Providers that users would **least** trust to access their electronic health records

5 Conclusions

In health and social care, a key element is high levels of assurance for identity checking, as a lack of this will compromise the whole system. safi.re integrates the concept of levels of assurance for the access to health and social care services. The integration of miiCard as a trusted online identity provider, gives the highest level of trust, assurance and traceability to enable users to gain the highest levels of access to their health and social care services. A key proposal in the paper is the usage of LOA 3+ for citizen access to electronic health records, and this is re-enforced in the survey where respondents preferred methods in which they had a high-level of personal assurance in providing their own identities. Within a health care system which only used LOA 1, there could obviously be many risks, and this exposure to risks could, ultimately compromise the whole infrastructure. The dislike of service providers such as Facebook in verifying identities for the access to health records shows that users are becoming more educated in how their data is being used.

At present, there is a great deal of debate around what level of assurance users will get to access their health and social care records, and it is important that the governance of it provides ways to define different levels of access for users. This is likely to increase both human and digital trust. Thus within this Information Age, it is human trust that often counts more than digital trust, and thus strong governance and identity checking are essential. The checking of identity will be important in defining this human trust, and where there is no one method that can completely define all the accesses that are likely to be required. A modern health and social care infrastructure should map the requirements to consume services to the requirements to the identity provision. Along with this a health care infrastructure requires a completely defined trust infrastructure for identity and attribute checking, and one which not only scales to citizens, but to health care professionals too. Only with this can we have a completed trusted and integrated infrastructure, and one which can respond in real-time to any changes.

6 References

1. L Fan, W Buchanan, C Thuemmler, O Lo, A Khedim, O Uthmani, A Lawson, D Bell, DACAR Platform for eHealth Services Cloud, Cloud Computing (CLOUD), 2011 IEEE International Conference on, 219-226

2. Fan, Lu, et al. "SPoC: Protecting Patient Privacy for e-Health Services in the Cloud." eTELEMED 2012, The Fourth International Conference on eHealth, Telemedicine, and Social Medicine. 2012.

3. Ekonomou, E., Fan, L., Buchanan, W., & Thuemmler, C. (2011, November). An Integrated Cloud-based Healthcare Infrastructure. In Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on (pp. 532-536). IEEE.

4. Lo, O., Fan, L., Buchanan, W. J., & Thuemmler, C. (2012). Technical evaluation of an e-health platform. IADIS E-Health.

5. US Patent Application No 13/739074, The Court of Edinburgh Napier University, Short Title: Binary Decision Diagrams, IP Title: Improved Information Sharing, Submitted: 11 Jan 2013.

6. Hardt, D (ed.). The OAuth 2.0 Authorization Framework, IEFT RFC 6749, October 2012, Accessed from: http://tools.ietf.org/html/rfc6749.html

7. Dimitrios Zissis, Dimitrios Lekkas, Panayiotis Koutsabasis, Cryptographic Dysfunctionality-A Survey on User Perceptions of Digital Certificates, Global Security, Safety and Sustainability & e-Democracy, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Volume 99, 2012, pp 80-87

8. http://mydex.org

9. http://sitekit.net

10. http://www.miicard.com