CURRENT ISSUES AND SOLUTIONS IN IDENTITY MANAGEMENT

By Malcolm Crompton and Robin McKenzie

This work has been supported by funding from National ICT Australia (NICTA)
www.nicta.com.au

A BACKGROUND PAPER FOR

Identity systems: Informational self determination Panel

32ND INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS – "PRIVACY: GENERATIONS"

JERUSALEM, ISRAEL

OCTOBER 2010

TABLE OF CONTENTS

1 INTRODUCTION

The need to create trust and security in the digital world is currently a preoccupation of governments and private sector organisations globally.

The digital world and the internet in particular were built on the assumption that using the internet was almost risk free. It was originally developed to be a closed environment and the information exchanged did not need protection or sharing restricted. As a consequence, mechanisms to manage risks, such as a trust framework were not built. A key element missing was any means of identifying who was connecting with whom.

In the absence of mechanisms to establish trust in the digital world and in the face of rapid expansion and the increasing value and availability of information about people, the criminal element has moved in.

There has been increasing concern that there could be a major trust crisis that might threaten the vibrant digital economy.

2 IDENTITY IN THE DIGITAL WORLD

Organisations in both the private sector and the public sector seeking to manage risk in the digital world have usually tried to solve the problem on an individual basis. In the real world there have been a range of mechanisms to establish trust. However, in the digital world, the choice has most often been to adopt mechanisms that rely on claims about identity. This has been so even in circumstances where this approach would not have been adopted in the equivalent kind of transaction in the real world. For example, payments in the digital world have almost universally required the authentication of identity claims where in the real world, the anonymity of payment by coin or notes would be regarded as sufficient because other means of trust are in place.

The mechanism in the digital world has most commonly involved:

- an enrolment or registration process which requires a person to provide a number of identifying claims about themselves, such as name, address and date of birth, which may be checked with a credible authority to establish their identity
- the issuing of a credential as a way of avoiding having to repeat the enrolment process each time a person interacts with the other entity. The credential has consisted of something that is based on:
    - something that you know (user name or password, secret questions) or
    - something that you have (a card with a magnetic strip or chip) or
    - something that you are (a photograph or biometric such as a finger print, iris scan etc) or
    - an agreed combination of these and

- presentation of the credential when a person is asked to authenticate their identity at which point the credential is checked for whether it has been revoked and whether it is in the control of the entity to which it was issued.

Trust in the digital world has therefore become increasingly dependent on the authentication of identity claims than ever was the case in the real world.

3 RISKS OF SOLUTIONS – THE POWER IMBALANCE

As the solutions to the problem of digital identity management began to emerge in the 2000s, the flaws in the approaches also began to emerge. From a privacy and security point of view these include:

- that mechanisms for representing identity have relied too much on managing organisational risk and not enough on managing the individual's privacy and other risk – mechanisms are not providing for two way trust, so individuals are vulnerable to phishing and other online fraudulent activity

- that individuals have lost control over their digital identities and digital life through some identity management systems that may give too much power to a government or an identity provider or that do not provide for sufficient control once the information has been transferred to third parties

- lack of interoperability which means that individuals cannot transport their identity to another identity provider if they are not happy with the way information is managed

- a failure to recognise that, as in the real world, people have a number of digital identities and how each is being represented needs to be appropriate to the context

- that more information about an individual than necessary is being exchanged through identity management systems (and between more parties) and so organisations that do not need to are holding identifying information about individuals and potentially using it for purposes unrelated to the management of their trust relationship with individuals

- that organisations are being enabled to track the movements of individuals in their digital lives in a way that is not related to identity management

- that systems may be designed in a way that individuals do not understand and so they cannot easily evaluate the parties they are interacting with or detect irregularities or fraud

- that single source of truth or centralised identity management systems create a honey pot of information about individuals which is valuable enough for criminal elements to make significant efforts to breach even highly secure defences.

These flaws revealed that a key reason why trust is still missing in the digital world is that many of the initiatives place too much power in the hands of entities other than the individual. In some cases, there is too much power in the hands of a government, or in other cases, in the hands of a private sector identity provider, claims authenticator or a trusted intermediary.

4 KEY PRINCIPLES FOR DIGITAL IDENTITY

There have been a number of academic, public and private sector initiatives to develop frameworks aimed at a consistent and comprehensive approach to address achieving trust in the representation of digital identity. These approaches specifically address the importance of placing more power in the hands of the individual or 'user' and have come to be described as providing for a 'user-centric' approach to digital identity.

Early thinking on digital identity includes the work by Roger Clarke[1] in the mid to late 1990s in which he looks at the digital persona and explored identified, anonymous, pseudonymous transactions and choice. Perhaps the most influential thinking on digital identity and how to address the privacy and security risks associated with it came with the publication of Kim Cameron's Law of Identity in May 2005.[2] However, at roughly the same time, a number of others also developed sets of principles including 'Proof of ID Required', as published by Malcolm Crompton, March 2004[3], the London School of Economics[4] in its assessment of the UK identity card bill, Jøsang and Pope on Use Centric Identity Management in 2005[5], the '7 Laws of Identity' assessment of the Kim Cameron work by the Information and Privacy Commissioner, Ontario[6], and later on the Prime White Paper: Privacy and Identity Management for Europe, May 2008[7].

More recently, in June 2010 the United States Department of Homeland Security published a draft National Strategy for Trusted Identities in Cyberspace[8].

These sets of principles and thinking have been developed in a number of different contexts and have influenced each other. However there are some core features in common. They emphasise the importance of:

- user control over their digital identities
- minimising the identifying or other information about a person in a digital identity to only the information needed for the occasion
- minimising the number of parties having access to identifiable information through a digital representation
- developing systems that prevent unnecessary linking of information about individuals via their digital identities

[1] (www.rogerclarke.com/DV/DigPersona.html) on digital data persona in 1994, and 'Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice' http://www.rogerclarke.com/DV/UIPP99.html.
[2] (http://msdn.microsoft.com/library/en-us/dnwebsrv/html/lawsofidentity.asp).
[3] (www.privacy.gov.au/news/speeches/sp2_04p.pdf)
[4] 'The Identity Project: an assessment of the UK Identity Cards Bill and its implications', June 2005 (http://is.lse.ac.uk/idcard/identityreport.pdf), report on the UK identity card initiative
[5] http://persons.unik.no/josang/papers/JP2005-AusCERT.pdf
[6] '7 Laws of Identity: The Case for Privacy Embedded Laws of Identity in the Digital Age' prepared by the Information and Privacy Commissioner, Ontario, Ann Cavoukian (www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf)
[7] (https://www.prime-project.eu/prime_products/whitepaper/)
[8] (www.dhs.gov/xlibrary/assets/ns_tic.pdf)

- allowing individuals to have multiple digital identities that are suitable for the context
- mechanisms that establish two way trust, not just an organisation's trust in the user, including system support for users in managing the identity of service providers
- having a number of different operators and technologies and the ability to 'port' digital identities
- providing a consistent and easy to use human experience for users of digital identity systems.

In short, a strong global consensus is emerging on the importance of building trust and privacy into the design of digital identity management systems from the beginning, particularly at the technology layer[9] [10].

5 KEY ISSUES FOR THOSE SEEKING TO ADDRESS TRUST ISSUES IN THE DIGITAL WORLD

A range of issues face governments and other organisations seeking to establish trust in the digital world particularly in the area of identity management. These do not just relate to privacy and security. There are also a number of practical issues. The most important are addressed in this section, along with a selection of examples of solutions already available.

5.1 USABILITY

5.1.1 CONVENIENT AND TRUSTED 'ENROLMENT'

To gain the full benefit of the convenience and efficiency of the digital world, governments and other organisations are seeking to eliminate or minimise the need for face to face enrolment to establish the link between a claim and a real person. So far most online transactions that require a high level of assurance involve a face to face interaction and strong evidence of physical identity, followed by the issuing of a credential that can then be used online. This is a major inhibitor of the expansion of online service into transactions requiring higher levels of trust. Governments and organisations are seeking ways to establish this higher level of confidence without having to constantly repeat face to face enrolment processes or to resort to complex federated arrangements which have their own governance, privacy and security challenges.

5.1.1.1 INDUSTRY SOLUTIONS

Edentity

Recently, other techniques of digital identity management have been explored based on using evidence that a respected third party online entity can authenticate a person's identity to establish the trustworthiness of a person and their identity claims. This kind of system allows a person to

[9] White Paper: Privacy and Identity Management for Europe, May 2008 https://www.prime-project.eu/prime_products/whitepaper/ p 16 The Prime design principles.

[10] See for example, Ann Cavoukian 'Privacy by Design' www.ipc.on.ca/images/Resources/privacybydesign.pdf, and Malcolm Crompton in 'Privacy by Design: An Oxymoron, An Impossibility or The Way To Go?', a NICTA Big Picture public seminar, June 2010 www.nicta.com.au/nicta_events/big_picture/qrl_seminars/archives/malcom_crompton

authenticate their identity without presenting a credential and relying instead on the high integrity digital identity management processes of others.

There are a number of digital identity systems of this kind. One such system operating in Australia called Edentity[11] asks an individual to log into the web site of a particular service provider such as the Australian government's Medicare system and on the basis that the person is able to authenticate their identity with the Medicare site, Edentity is willing to authenticate the person's identity to a third party.

Experian

A further development has been online identity management systems such as that provided by the UK company Experian[12] which relies on the evidence of a person's interactions with a number of digital sources of information over a significant period to establish and authenticate an individual's identity.

This online identity management system searches a wide number of digital databases to establish evidence of a person's existence and to confirm identity details. It does not rely on third party enrolment processes to establish the existence of a 'real' identity. It does not require a centralised holding of personal information about a digital identity and it does not require a person to have one identifier that is used to authenticate identity. The sources of data do not disclose information about the person seeking to establish identity. It is a 'yes / no' process which contributes to a rating or finding about the likelihood that the person is who they say they are and has a real world identity.

5.1.2 MULTIPLE CREDENTIAL PROBLEM

A key issue is how to eliminate the many user names and passwords, smartcards and other credentials which individuals must currently manage in seeking to authenticate their identities online. These are inconvenient for users who are always forgetting or losing them and costly for organisations to administer. Users adopt many insecure strategies for managing their many user names and passwords. The two main solutions developed so far have been to either:

- centralise identity management into one system and one credential; (for example, the failed UK identity card initiative) or
- develop federated identity management systems, in which the individuals can 'sign on' once and authenticate once and then that authentication is relied on by a number of other parties.

However, these initiatives each potentially raise a number of issues.

- In the case of centralised identity systems this could be:
    - too much power in the hands of one party including the power to bring a person in and out of digital existence
    - the ability to track and form a whole picture of a person's life

[11] www.edentiti.com/edentiti-id/index.php
[12] eg https://www.experian.com/whitepapers/precise_id_whitepaper.pdf

- creation of a honey pot of information attractive for internal or external attack
- the lack of portability of a digital identity

- In the case of federated identity management systems this could be:
  - the ability of one of the parties, for example, a third party mediator to track a person's identity management transactions
  - security and trust issues relating to having a range of identity providers, relying parties and other intermediaries involved.

5.1.2.1 INDUSTRY SOLUTIONS

Some key initiatives have focussed on enabling individuals to manage multiple credentials more easily and to have direct control over which identity claims they will provide to a particular relying party. These provide 'meta systems' for digital identity management and are called 'identity selectors' or 'card selectors'[13].

These card selectors enable an individual to manage 'information cards' that allow an individual to present a set of claims (or units of data). These information cards can be self issued (called Personal Cards) or can be managed cards that present data or claims that are authenticated by an 'authority' that is an identity provider (for example, a driver license issuing authority). Very importantly, the information card is a pointer to data, not the actual data itself. When a person wants to access a restricted website, or pay for something online, for example, the card selector software client prompts the user to choose one of the information cards he or she has in his or her selector space that could be used to validate the particular claims required by the website or other relying party. The software client brokers the transfer of the claims between the identity provider (for example, a driver license issuing authority, or it could be the user if it is self issued card) and the website or other relying party. The software client helps the person choose which information card they might use based on the claims that the relying party is seeking to validate. The client only brokers the particular claims that the relying party asks to be validated.

CardSpace

CardSpace is a card selector that runs on Microsoft Windows and can participate as an Identity Selector within the framework of an Identity Metasystem. CardSpace uses standard web services protocols to communicate claims between three parties: the Identity Provider (IdP), the Relying Party (RP), and the Identity Selector[14].

Higgins active client and data stores

Higgins has also developed an active client and data store that provides a card selector function.[15] It is open source and runs on a range of platforms.

[13] Examples include: Microsoft's CardSpace (http://Cardspace.netfx3.com) and the Higgins project (www.eclipse.org/higgins)
[14] See explanation at http://eternallyoptimistic.com/information-cards/cardspace-quickstart/
[15] See explanation at www.incontextblog.com/?cat=11

A card selector in the Cloud

Most of the card selectors developed to date have been platform or device specific at least to some extent and in the case of Windows CardSpace, locked to the one device in one software environment involving a serious effort to transfer an information card from one device to another.

With the mobile environment rapidly taking over the everyday user experience and backed by 'cloud' based services, the need for a platform independent, cloud based card selector has become an imperative. One of the first is the Avoco Secure CloudCard Selector which is very promising from a user experience and organisation deployment perspective.[16]

5.1.2.2 Benefits of these system

The benefits for users in this kind of system is that they can use already issued credentials to validate claims rather than having to get yet another one, they can control what credential they will use to validate the claims and they can reduce the number of user names and passwords they have to keep track of.

Importantly, these kinds of systems also seek to avoid many of the other trust issues identified here. For example, they aim to avoid any one identity provider from being able to control a person's digital existence. However, they often involve the use of trusted intermediaries. As such, careful design is needed. Otherwise the trusted intermediary can become the actor that is all seeing.

5.1.3 Control and appropriate human experience

User centric identity management principles also require that individuals have as much control as possible over what information they disclose and in what circumstances. A key conundrum is how to give individuals that kind of control in an easy to use, understandable and trustworthy way. Not all of these issues can be resolved by technology alone. For example although card selectors help a person to have control of this through enabling a person to select from a series of information cards, there is still potentially a whole range of governance and other issues particularly where there are a large number of third parties involved including:

- trust between the parties involved in these mechanisms;
- the need to be able to establish, in some cases, a high level of trust in a claim, including that the person is who they say they are
- enabling relying parties to measure the level of trust that can be placed in a particular claim
- security in the transmission of claims
- allocation of responsibility when things go wrong.

5.1.3.1 Industry solution

Open Identity Trust Framework

One initiative seeks to address these governance and trust issues by developing the Open Identity Trust Framework (OITF) model. It provides a detailed, but flexible governance system for all the participating types of entities, including identity providers and relying parties. [17] It enables large scale networks of trust to develop. The OITF provides a set of technical, operational, and legal

[16] https://www.secure2cardspace.com

requirements and enforcement mechanisms for parties exchanging identity information. The framework establishes additional actors to look after these requirements. These are:

- **policy makers** decide the technical, operational and legal requirements for exchanges involving identity information among a group they govern;
- **OITF providers** translate the requirements of policy makers into their own blueprint for a trust framework that they then proceed to build;
- **assessors** evaluate identity service providers and relying parties and certify that they are capable of following the OITF Providers' blueprint;
- **auditors** may be called on to check that parties' practices have been in line with what was agreed for the OITF; and
- **dispute resolvers** may provide dispute resolution services for disagreements of a legal nature.

Any entity may carry out these functions, as long as they meet specified criteria. Mechanisms for implementing the framework include:

- criteria for measuring a party's ability to meet technical, operational and legal requirements for OITF;
- a set of certification processes for evaluating a publishing whether parties are capable of meeting the OITF requirements;
- a set of legally binding agreements that together constitute the legal structure of the OITF.

To further promote trust and accountability, the framework is underpinned by principles of openness. All participants must incorporate them into their agreements. The principles address lawfulness, open reporting and publication, ombudsmen, anti-circumvention and open disclosure, non-discrimination, interoperability, open versioning, participant involvement, data protection, accountability, auditability and redress.

5.2 Privacy

5.2.1 Information limitation

For privacy and security reasons, individuals, governments and organisations may be seeking to limit the information they collect through identity management to that which is necessary for their function or activity. They may also seek, where possible, to limit the ability to link information about a person held in different domains, and as a result, form a whole of life picture of an individual that is not relevant to the service provided or function.

5.2.1.1 Industry solutions

There is a raft of initiatives underway which aim to give users more control over their digital identity claims by enabling individuals to authenticate identity claims without the relying party receiving

[17] See for example The Open Identity Trust Framework (OITF) Model, March 2010 http://openidentityexchange.org/frameworks

identifying information about the individual. A number of the initiatives identified earlier contribute to meeting these objectives.

Other initiatives are seeking to prevent disclosure of private login information held by identity providers in a federated login system. Minimising the audit logs generated by individuals will need to be a conscious process.

Pseudo ID

PseudoID is a privacy enhancement for federated login systems that is backward-compatible with OpenID (a popular federated login system[18]). PseudoID is designed to protect users from disclosure of private login data held by federated identity providers. It is based on a cryptographic tool called a blind signature, which is similar to the untraceable payment scheme developed by David Chaum[19].

In cryptography, a blind signature is a form of digital signature in which the content of a message is disguised (blinded) before it is signed. The resulting blind signature can be publicly verified against the original, unblinded message in the manner of a regular digital signature.

An often-used analogy to the cryptographic blind signature is the physical act of enclosing a message in a special write-through-capable envelope, which is then sealed and signed by a signing agent. Thus, the signer does not view the message content, but a third party can later verify the signature and know that the signature is valid within the limitations of the underlying signature scheme.

U-prove

U-Prove allows the creation of secure ID tokens, which are pieces of data that incorporate only the information a person needs for a given task along with cryptographic protection to ensure that they cannot be forged, reused, traced back to the user, or linked to other tokens that a person has issued.

It builds on existing public key cryptography concepts, but adds to them the important ability to hide data. In effect, public key cryptography normally requires knowledge about the data to prove that a particular piece of data was encrypted by a particular person. U-Prove allows that proof to take place without revealing all the data.

If a credit card company or online music service both support U-Prove, the user can create a token that allows a single limited electronic money transfer from the users card to the music company, without disclosing his or her name, address, or date of birth, and without that token being usable to make further purchases. Similarly, a user who wants to buy a computer game from an online store that is rated for adults only can reveal his or her age, as well as the money transfer, to the online store. U-Prove lets a user do this, but does not require the user to reveal name, address or other irrelevant detail.

U-Prove can ensure that a user can, if appropriate retain anonymity, or pseudonymity when using a card selector[20].

[18] See http://openid.net/
[19] See www.pseudoid.net/
[20] See UProve (Brands) https://connect.microsoft.com/content/content.aspx?contentid=12505&siteid=642.

Identity Mixer

As consumers hand over personal details in exchange for downloading music or subscribing to online newsletters, they leave a data trail behind that reveals pieces of information about the size, frequency and source of their online purchases that can be traced back to the user. IBM's Identity Mixer software eliminates the trail by using artificial identity information, known as pseudonyms, to make online transactions anonymous. For example, the software allows people to purchase books or clothing without revealing their credit card number. It can confirm someone's spending limit without sharing their bank balance, or provide proof of age without disclosing their date of birth.

Identity Mixer works by allowing a computer user who has the appropriate software to obtain an anonymous digital credential, or voucher, from a trusted third party, such as a bank, insurance company or government agency. A health insurance company, for example, could provide a credential confirming that a user has certain health insurance benefits. If the user wishes to consult their healthcare provider's online portal for medical information, the Identity Mixer software digitally seals the credential so the user can send it to the healthcare provider and get access to the online service. By using sophisticated cryptographic algorithms, the Identity Mixer software acts as a middleman so that the user's real identity is never exposed to the health-care provider. The next time the user consults the service, a new encrypted credential would be used[21].

Identity Mixer and U-Prove offer solutions to similar challenges in identity management but not in quite the same way.

5.2.2 Control over information handling

Some work has focussed on giving individuals more control over those receiving digital identity claim information including by enabling individuals to negotiate information handling policies and to control and keep track of information disclosed as part of digital identity management.[22] Identity management mechanisms will need to come to grips with the need to be transparent about the information held through the identity management system, and who has accessed any information and for what purposes as required by privacy principles. Some countries provide individuals with an online portal that gives them greater control over who has access to their credentials and helps them track their identity usage. These include Norway's MyPage www.norway.no/minside/, France's Service Public www.service-public.fr/, the UK's Directgov www.direct.gov.uk/en/index.htm and Australia's http://australia.gov.au/.

5.3 Interoperability

For many reasons, governments and organisations are seeking identity management systems that are interoperable at a number of levels including:

- at the technical level: providing for different technologies to communicate and exchange data based upon well defined and widely adopted interface standard
- at the semantic level: enabling each end point to communicate data and have the receiving party understand the message in the sense intended by the sending party

[21] See www.zurich.ibm.com/news/07/idemix.html
[22] Prime White paper.

- at the policy level: providing for identity solutions to have common business processes for the transmission, receipt and acceptance of data between systems.

5.3.1 The Government Hardwired Problem

Governments can have a particular challenge because political, constitutional and legislative barriers to change can be particularly high. Yet they are now beginning to seek identity solutions that use non-proprietary standards to ensure interoperability. Such mechanisms prevent governments being locked-in to particular solutions and to enhance systems without the need to start again from scratch. It also adds to user centricity and control by enabling individuals to move between identity providers as they choose.

5.3.1.1 Industry/Government solution

STORK

One project seeking a solution to interoperability of identity management systems is the STORK project (Secure Identity Across Borders)

The aim of the STORK project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID.

Cross-border user authentication for such e-relations will be applied and tested by the project by means of five pilot projects that will use existing government services in EU Member States. In time it is proposed that additional service providers will also become connected to the platform thereby increasing the number of cross-border services available to European users.

The aim is that in the future, a person will be able to start a company, get a tax refund, or receive university papers without physical presence. All the person will need to access these services is to enter their personal data using his or her national eID, and the STORK platform will obtain the required guarantee (authentication) from the person's government.

The project aims to offer a user-centric approach and is being designed to provide a privacy guarantee. The role of the STORK platform is to identify a user who is in a session with a service provider, and to send his or her data to this service. Whilst the service provider may request various data items, the user always controls the data to be sent. The explicit consent of the owner of the data, the user, is always required before his or her data can be sent to the service provider. The project is proposing two interoperability models:

- middle ware and
- pan-European proxy services[23].

5.4 Two way trust

A critical problem to solve is the need for two way trust. Governments and organisations have focussed largely on ensuring that they can trust individuals, but have focussed less on ensuring the individual can trust the entity or entities they are interacting with. Public Key Infrastructure and digital certificates have been the main solution proposed for this problem but it has proved

[23] See https://www.eid-stork.eu/index.php?option=com_frontpage&Itemid=1

expensive and there has been resistance to adopting it. Technologies discussed above such as U-Prove, IDMIX and PseudoID if widely adopted will help to solve this problem.

5.5 EASE OF ON BOARDING FOR ORGANISATIONS AND GOVERNMENTS

5.5.1 COPING WITH MULTIPLE PLATFORMS

A show stopper for many governments and organisations is the cost in establishing a new digital identity management system. The administrative and other costs of establishing a system that involves the more secure digital certificate approach, and resistance among relying parties to the bureaucracy involved, has inhibited the fast take up of more secure identity management systems. Other prohibitive costs have been the need to buy new hardware and software which must be kept secure and up-to-date. A further difficulty has been the need to accommodate a variety of platforms including iPads, iPhones, and laptops as well as fixed PCs.

5.5.1.1 INDUSTRY SOLUTION

One industry solution has capitalised on the capability of the Cloud to handle these issues.

Avoco

Avoco Secure offers a suite of solutions that are highly device and platform independent as well as cheap and easy for the enterprise to deploy. The suite centres around the card selector in the cloud mentioned earlier. The cloud card selector gives the user very visible and strong control over which claims about identity are being authenticated and presented to a relying party and applies a series of security measures to ensure safety. It goes on to provide document management and document signature using the information cards in the cloud selector that provides the ability to tie a security policy, using a digital identity, directly to information. In order to do so, it generates digital certificates 'on the fly' without requiring the expense and overhead of a Public Key Infrastructure[24].

[24] See www.avocosecure.com/