Trust Requirements in Identity Management

Audun Jøsang[1], John Fabre[2], Brian Hay[2], James Dalziel[3] , Simon Pope[1]

[1]Distributed Systems Technology Centre
{ajosang, simon.pope}@dstc.edu.au

[2]Telstra Research Laboratories
{john.fabre, brian.hay}@team.telstra.com

[3]Macquarie University
james@melcoe.mq.edu.au

Abstract

Identity management refers to the process of representing and recognising entities as digital identities in computer networks. Authentication, which is an integral part of identity management, serves to verify claims about holding specific identities. Identity management is therefore fundamental to, and sometimes include, other security constructs such as authorisation and access control. Different identity management models will have different trust requirements. Since there are costs associated with establishing trust, it will be an advantage to have identity management models with simple trust requirements. The purpose of this paper is to describe trust problems in current approaches to identity management, and to propose some solutions.

1 Introduction

Being able to represent and recognise entities in computer networks is fundamental to electronic interaction and collaboration by providing a basis for other security constructs, such as authorisation, access control, and reputation ownership. In the simplest case when a set of users accesses a single service provider, the traditional approach is to let users identify themselves through unique identifiers, and authenticate themselves using security credentials such as passwords. In this model the trust requirements between user and service provider are well understood in the form of specific security and privacy assumptions. In addition, the industry has had several decades of experience with this model, and users are familiar with it. What we have here is an *isolated identity management model* because each identifier that a user possesses can only be used for one isolated service. This model, which is used for all types of access to online services and resources, as well as for digital rights management, is relatively simple for service providers but is rapidly becoming unmanageable for users. The rapid growth in the number of online services based on this model now results in the users being overloaded with identifiers and credentials that they need to manage. For this reason, and also for the purpose of coordinating related services from different service providers, new identity management models are being proposed and implemented. Some of these models have relatively complex trust requirements, and the user groups have so far had little experience with them. The contribution of this paper is to analyse some of the trust requirements resulting from the various identity management models. The paper first discusses the general concepts of identity and trust. Subsequently, models for user identity management are described and compared. Finally some trust issues in the existing paradigm for service provider identity management are discussed.

The work reported in this paper has been funded in part by the Co-operative Research Centre for Enterprise Distributed Systems Technology (DSTC) through the Australian Federal Government's CRC Programme (Department of Education, Science & Training).

2 Entities, Identities and Identifiers

A person's or an organisation's identity consists of the individual characteristics by which that person or organisation is recognised or known. These elements can be acquired, such as name, address, nationality, registration numbers and memberships, or can be inherent, such as with biometrics. For organisational identities, most of the characteristics must be considered acquired.

Any characteristic element can be called an identifier when it is used for identification purposes. It is assumed that identities are unique, i.e. no two human beings or organisations have the same identity. However, the same person or the same organisation can have different identities in different contexts, and each identity is reflected by a different set of identifiers. An identifier is

usually only unique within a given context. The different types of identifiers can be quite varied in their characteristics, and may be transient or permanent; inherent or applied; self-selected or issued by an external authority; interpretable by humans, computers, or both, etc. The name space for identifiers must be carefully chosen in order to guarantee the unique mapping of each identity to a single entity. Biometric identifiers are usually not sufficient for this purpose for more than a limited set of entities, and other identifier types can suffer from similar weaknesses under particular sets of conditions. The relationship between identifier, identities and person/organisation entities is illustrated in Figure 1 below.

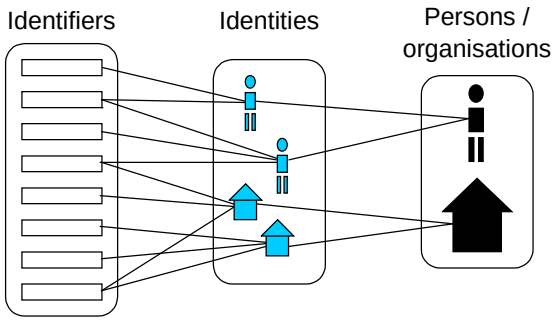

Figure 1 Relationships between identifiers, identities and entities

The set of identifiers is larger than the set of identities, which again is larger than the set of persons or organisations. An identity can be seen as a unique subset of identifiers.

Digital identity is a form of identity resulting from the digital codification of identifiers in a way that is suitable for processing and interpretation by computer systems. A digital identity is commonly represented by a unique identifier such as an account name or number. Protected services typically require that users identify themselves with this type of unique identifier. E-authentication is about verifying the correctness of a user's claim of holding a particular unique identifier.

It should be noted that in common language, the separation between identity and identifier is blurred, and that the term "identity" often is used in the sense of "identifier". This is quite common when an identity is recognised by a single unique identifier within a given context. For clarity, the terms "identity" and "identifier" will be used with their separate specific meanings throughout this paper.

3 The Concept of Trust

A wide variety of definitions of trust have been put forward [McKnight & Chervany, 1996], many of which are dependent on the context in which interaction occurs, or on the observer's subjective point of view. A general definition that can be extracted from McKnight and Chervany's survey can be summarised as follows:

Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible. [McKnight & Chervany, 1996].

Although relatively general, this definition explicitly and implicitly includes the basic ingredients of trust that are 1) *dependence* on the trusted party, 2) *reliability* of the trusted party, and 3) *risk* in case the trusted party does not perform as expected. The implication of this definition is that trust requirements are directly correlated to risk exposure [Jøsang & Lo Presti 2004]. It is useful to keep this interpretation in mind when considering particular trust assumptions for identity management.

4 Isolated Identity Management

4.1 Isolated Identity Architecture

The current practice is for online service providers to act as both credential provider and identifier provider to their clients. They control the name space for a specific service domain, and allocate identifiers to users. A user gets separate unique identifiers from each service/identifier provider he transacts with. In addition, each user will have separate credentials, such as passwords associated with each of their identifiers. This situation is illustrated in Figure 2 below.

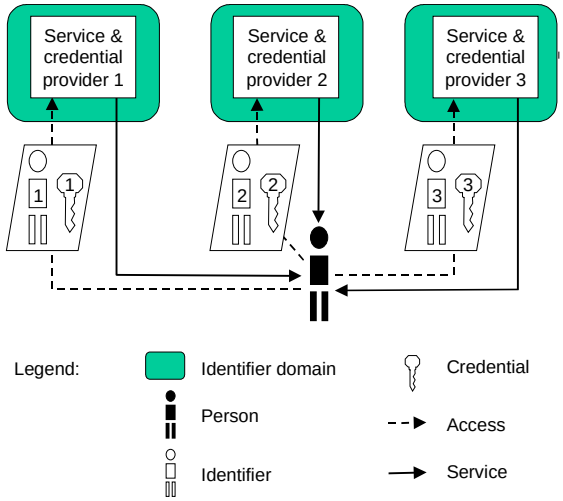

Figure 2 Isolated identifier domains

This approach might provide simple identity management from the service providers' point of view, but is problematic for users as the number of service providers that they transacts with increases. Users routinely forget passwords to infrequently used service providers. Forgotten passwords or fear of forgetting them create a significant barrier to usage, resulting in the services not reaching their full potential.

For important sensitive services, where password recovery must be highly secure, forgotten passwords can also significantly increase the cost of client service.

4.2 Trust Issues in Isolated Identity Management

The simplicity of the isolated identity architecture makes it relatively easy to understand and solve the trust issues involved. Trust complexity is greatly simplified when the same entity acts as identifier provider, credentials provider and service provider. Under these conditions, the client and service provider only need to trust each other for a small set of purposes.

The assurance level (i.e. the strength) of the processes and mechanisms used for identity registration and authentication will be defined by the service provider according to their assessment of the risks and sensitivity of the offered service. For example, stronger mechanisms will normally be needed for online banking than for online library access. See e.g. [US OMB 2003] and [NIST SP800-63 2004] for procedures for determining authentication assurance levels and mechanisms.

4.2.1 Client Trust in Service Provider

The need for clients to have *identity trust* in the service provider is described in Section 9 below. In addition, the client needs the following trust in the service provider:

- **T1:** *The service provider protects client privacy*, and
- **T2:** *The service provider has implemented satisfactory user registration procedures and authentication mechanisms (from the client's perspective).*

Failure to protect personal information can cause distress and inconvenience to clients. Inadequate authentication procedures and mechanisms can result in authentication failure as well as financial loss to both service provider and clients. By authentication failure is meant that a misrepresented and unauthentic identifier is erroneously determined to be authentic by the verifier. It can also mean that legitimate users are unable to authenticate themselves, but this type of authentication failure poses less risk than the former type.

T1 trust can for example be established by publishing privacy policies, by having a history of following those, and/or by using the P3P platform [W3C 2004]. T2 trust is established by implementing the right procedures and mechanisms; by having a history without authentication failures; and by reducing clients' exposure through alternative risk mitigation strategies in the event of actual or implied losses as a result of fraud.

4.2.2 Service Provider Trust in Client

The service provider needs to trust the client so that:

- **T3:** *The client handles their authentication credentials with adequate care.*

Poor management of credentials can result in their theft, possibly leading to authentication failure and identity theft. In cases of credential theft, service providers often place the burden of liability on clients in their terms of service. In these cases the provider does not need T3 trust. Instead, the client needs to trust themselves for the purpose of T3 as they bear the liability in the event of identity theft.

T3 trust can be established for clients through assurances that they follow the recommended practices of the SP for handling authentication credentials, and by having a history with the service provider that is free of security incidents.

5 Federated Identity Management

5.1 Federated Identity Architecture

One of the purposes of identity federation is to address the type of inefficiencies described in Section 4.1. Identity federation can be defined as the set of agreements, standards and technologies that enable a group of service provider to recognise user identifiers and entitlements from other service providers within the group. The basic idea is to link different identifiers, and thereby their associated identities, owned by the same user across multiple service providers, and allow the user to authentication himself with a single identifier to one of the service providers, and thereby be considered identified and authenticated by all the other service providers as well. This is in effect a Single Sign-On (SSO) solution similar to that described in Sec.6.1.3 below, and the isolated identifier domains within a federated group become a single federated identifier domain. This approach is illustrated in Figure 3 below.

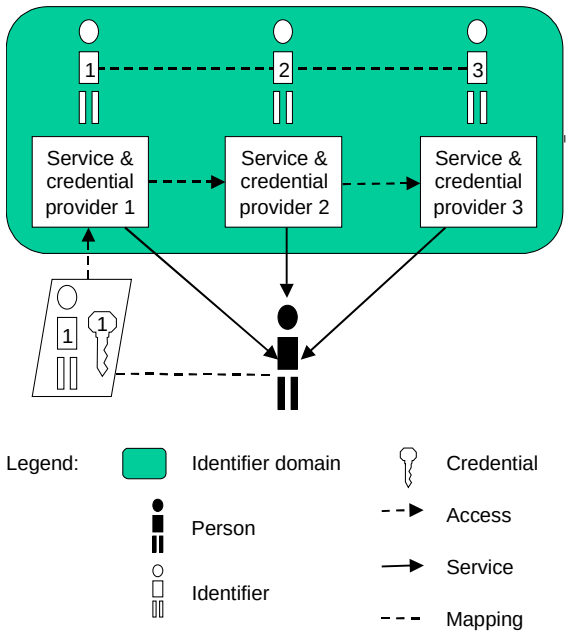

Figure 3 Federated identifier domain

In a federated identifier domain, each service provider still provides a separate identifier and credential to the same client, but the client does not necessarily need to use them all. The most likely implementation is that access will happen through a single service provider, allowing a single set of identifier and credential to be used for accessing all service providers within the federated domain.

5.2 Trust Issues in Federated Identity Management

While identity federation is aimed at simplifying the user experience, it creates considerable trust complexity both for the service providers and their clients, as will be explained below.

5.2.1 Trust between Federated Service Providers

As illustrated in Figure 3, access to a service provider can occur indirectly via other service providers. Assuming that the client uses separate digital identities with the different service domains, each service provider would then need to know the mapping between the identifiers owned by the same user. While the primary access method of direct access requires the client's digital identifier and credentials for that domain, indirect access is a secondary access path that does not require the client's authentication credentials. This indirect access path simply requires the passing of security assertions, such as e.g. SAML assertions [OASIS 2004], between service providers. Service providers need to trust each other for the purpose T2 described above, as well as:

- **T4:** *Service access by assertions between service providers on behalf of users will only take place when legitimately requested by the client.*

Client authentication by a third-party service provider (SP) is based on these assumptions. Authentication failure at the third-party SP can occur (for example) if the second-party SP suffered an authentication failure, or sent a fraudulent access request to the third-party SP (i.e. not on behalf of the client). OASIS [OASIS 2004] considers this to be a serious risk, as expressed by:

"When determining what issuers to trust, particularly in cases where the assertions will be used as inputs to authentication or authorization decisions, the risk of security compromise arising from the consumption of false but validly issued assertions is a large on."

The suggested method for establishing T4 trust is through agreement to a common set of policies and procedures, and possibly by establishing a contract that defines the obligations and responsibilities of the federated parties. The Liberty Alliance Project[1] uses the term "*Business Trust"* [Liberty Alliance 2003] to describe mutual trust between companies that emerges from formal agreements that regulate the interactions between them.

The distinction between symmetric and asymmetric trust relationships between service providers is worth noting. Where two service providers need to trust each other as part of their day to day business – e.g. banks transacting regular business – they would have similar exposure in the case of failure, and would likely have symmetric trust requirements. This kind of agreement has worked within the Liberty Alliance frameworks. However, asymmetric trust relationships between federated parties are harder to establish – e.g. a bank providing services to an airline. In this case, the different roles played by the two parties means that they are exposed to different risks in the case of failure (e.g., the failure of timely financial processing of online bookings could causes the airline to lose clients worth thousands of dollars, whereas the bank only loses commission fees worth a few dollars). The problem with asymmetric relationships is that one party has significantly higher risk exposure than the other, and hence business and legal agreements become more complex.

5.2.2 Trust in the Identity Mapping

The mapping of digital identities can be problematic as it requires a sufficient set of common identifiers to be matched between each pair of identities in order to establish that two separate identities actually belong to the same entity. All federated service providers need this trust which can be described as:

- **T5:** *The mapping of identities between service providers is correct.*

Incorrect identity mapping will unavoidably result in authentication failure.

T5 trust can be established by following thorough procedures for mapping identities, and by having a history that is free of incorrect mappings. In particular service providers must receive consent from each client before mapping their identities.

5.2.3 Client Trust in Service Providers

In addition to the trust purposes T1 and T2 defined in Section 4.2.1, the client also needs trust with the purposes T4 and T5. A stronger form of privacy trust is probably needed to satisfy T2 trust requirements as the identity mapping allows providers to correlate personal information about the client in a way that otherwise would not be possible. When the client consents to identity mapping, he must accept a given policy for how mapping can be used to correlate data linked to his different identities. This trust purpose can be expressed as:

- **T6:** *The service provider adheres to the accepted policy for correlating personal data about the same client from other service providers.*

The service provider's failure to adhere to the privacy policy for identity mapping can cause distress, inconvenience, and potential financial loss to clients.

T6 trust can be established by defining clear policies that are acceptable to the clients, and possibly by having a history without policy breaches.

[1] http://www.projectliberty.org/

6 Centralised Identity Management

6.1 Centralised Identity Architectures

In a centralised identifier domain, there is a single identifier and credentials provider that is used by all services. Centralised identifier domains can be implemented in a number of different forms. Below we describe *Common Identifier Domain*, *Meta-identifier Domain*, and *Single Sign-On* (SSO)

6.1.1 Common Identifier Domain

It is possible to nominate a separate entity or single authority as the Identifier and Credentials Provider. This architecture, which can be called the Common Identifier Domain, is illustrated in Figure 4 below.

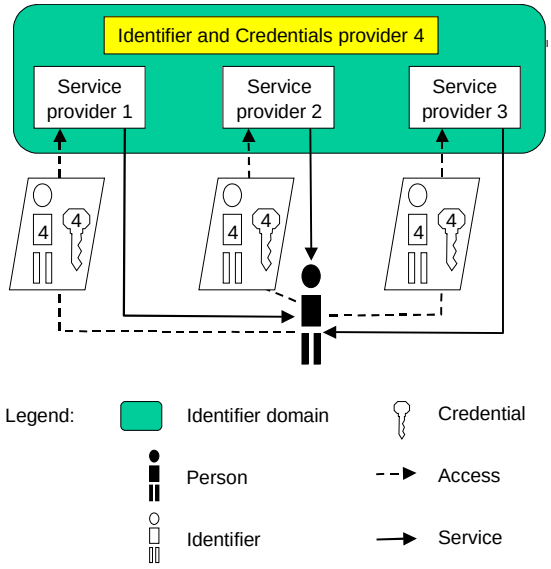

Figure 4 Common identifier domain.

Figure 4 indicates that the same identifier and credential are used for each service provider. This could for example be implemented by having a PKI, where a Certificate Authority (CA) issues certificates to users. The identifier name space can for example be the set of Internet email addresses that are globally unique. Each user can then use the same certificate to access different service providers, and all service providers authenticate the client through the same certificate before granting access to their services.

6.1.2 Meta Identifier Domain

Service providers can share certain identity related data on a common, or meta, level. This can be implemented by mapping all service provider specific identifiers to a meta identifier with which for example the credential can be linked. This is illustrated in Figure 5 below.

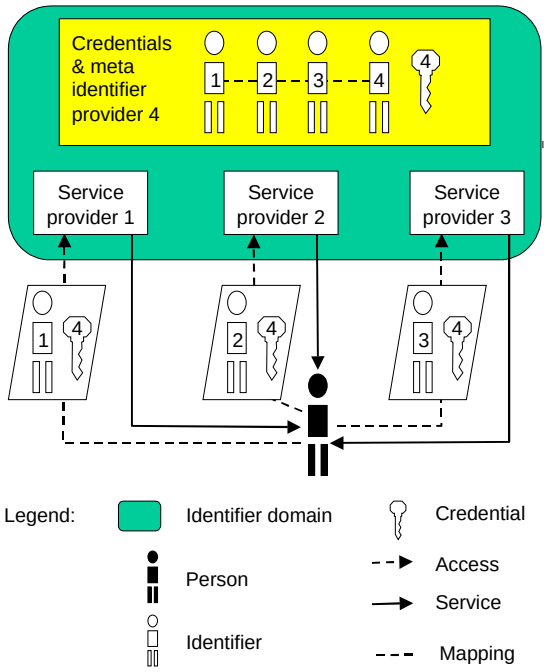

Figure 5 Meta identifier domain

The meta identifier approach is commonly implemented by a so-called meta directory, and is a popular approach for integrating legacy identity management systems in large enterprises. In theory it can also provide an integrated identity management approach for different service providers. The unique meta identifier is normally hidden from users, and is only used internally for identity management and service coordinating purposes.

6.1.3 Single Sign-On

A simple extension of the centralised identity management approaches described in Sections 6.1.1and 6.1.2 could be for service providers to allow a user who has been authenticated by one service provider to be considered authenticated by other service providers. This is commonly called a Single Sign-On (SSO) solution because the user then only needs to authenticate himself (i.e. sign on) once to access all the services. There will normally be one party responsible for allocating identifiers, issuing credentials and performing the actual authentication as illustrated in Figure 6 below.

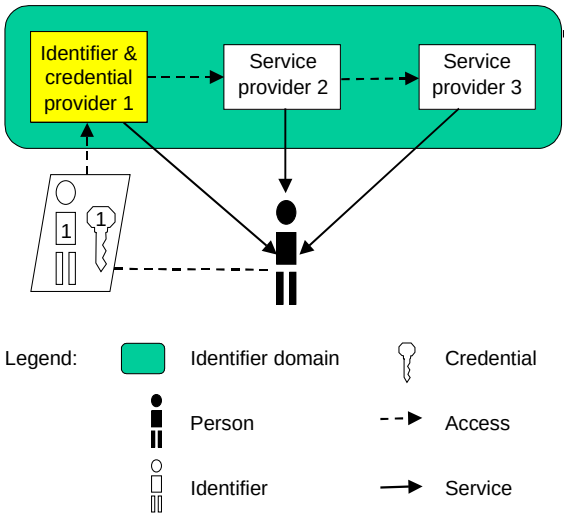

Figure 6 Single Sign-On identifier domain

The SSO scenario is very similar to the federated identifier scenario described in Section 5, except that no mapping of user identifiers would be needed because the same identifier is used by every service provider. Kerberos based authentication solutions are in this category, and Microsoft .Net Passport is a practical example of an SSO implementation for e-commerce.

6.2 Trust Issues in Centralised Identity Management

6.2.1 Client Trust in Service Providers

T1 is applicable as usual. When the service provider acts as a broker for issuing credentials in the registration phase, and verifies the credentials in the authentication phase, then T2 is applicable. T6 is also applicable because the centralised shared identity gives a service provider the ability correlate personal data about the same client from other service providers.

6.2.2 Service Provider Trust in Clients

T3 is applicable. However, if the risk and burden of liability is placed on clients in cases of credential theft, clients need to apply T3 to themselves.

6.2.3 Service Provider Trust in Credentials Provider

The existence of a separate credentials provider requires trust in the way credentials are issued to the users:

- **T7:** *The credentials provider has implemented adequate procedures for registering users and for issuing credentials.*

The credentials provider's failure to fulfil the requirements expressed in T7 can cause distress, inconvenience and financial loss to service providers as well as to users.

T7 trust can be established by implementing adequate procedures for registering users and for issuing credentials, and by having a history without registration error. User T7 trust can also be enhanced by reducing the users' exposure to risk through alternative risk mitigation strategies in the event of losses caused by registration error.

7 Personal Authentication Management

7.1 Personal Authentication Management Architecture

An authentication solution must take into consideration how the identifiers and credentials are to be handled by the user. In the simplest case, the user records identifiers on a suitable medium such as a paper notebook, and memorises the corresponding password credential. However, this becomes problematic with the increasing number of identifiers and credentials a user needs to manage.

The problem of managing multiple identifiers and credentials can be alleviated by storing them in a tamper resistant hardware device which could be a smart card or some other portable personal device. Because its main purpose would be authentication, the device can be called a personal authentication device (PAD). This is illustrated in Figure 7 below.

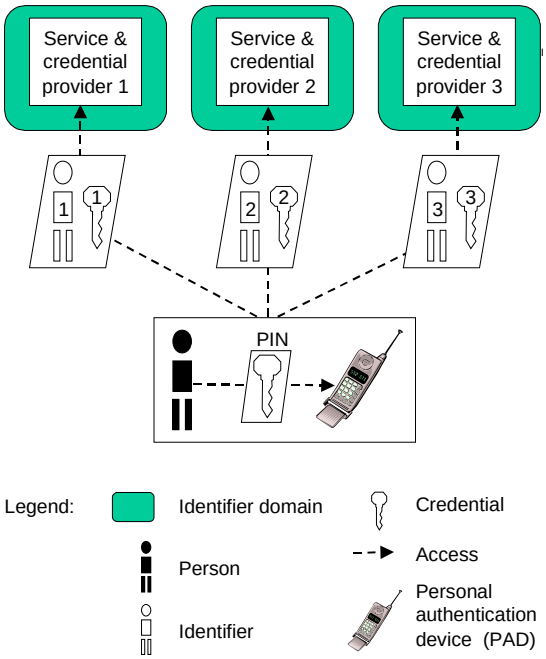

Figure 7 Personal authentication management

The term "Personal Authentication Device" has been in use within the context of computer security at least since 1985 (Wong, et al., 1985). While the details of the operations and limitations of the devices have varied significantly since that time, the key concepts remain the same. A more recent incarnation of the same concept can be found in the form of the Personal Trusted Device defined in [MeT 2002].

Because the PAD holds the user's various identifiers and credentials, and because it is a personal device, this architecture can be called personal identity management. It can be combined with any identifier model described in Sections 4, 5 or 6 above, where Figure 7 represents an example illustrating how it can be combined with the isolated identifier domains of Section 4.

The user must authenticate himself to the PAD, e.g. with a PIN, before the PAD can be used for authentication purposes. Many different authentication and access models can be imagined with a PAD. In case the PAD has a keyboard and display, a very simple solution could for example be to retrieve from PAD memory a static password, or let the PAD generate a dynamic password, that the user then can type into the login screen of the service provider. A more advanced solution could be to connect the PAD to the client platform via a PAD terminal such as a smart card reader, and let the authentication protocols run end-to-end between the service provider and the PAD. The functionality of a PAD could be integrated into other devices such as a mobile phone or personal digital assistant (PDA) because many people already carry with them such devices anyway. Using a mobile phone would also allow advanced solutions such as registration and challenge-response authentication through out-of-band channels such as a voice or SMS. With a PAD connected to the client platform, virtual SSO solutions are possible. This could be implemented by letting the PAD automatically authenticate itself on behalf of the user as long as the PAD is connected to the client platform.

The advantages of the personal identity management architecture are e.g. that 1) the user only needs to remember one credential (e.g. the PAD PIN), 2) that SSO is possible, and 3) that the existing paradigm of having a separate identifier for each service provider does not have to change. At the same time, all the disadvantages of for example federated identifier management, such as high trust requirements and complex security protocols between service providers, can be avoided.

For example, Mozilla provides single sign-on capabilities for users so they do not have to remember their usernames or passwords for websites. A master password protects the PKCS#11 security device, which can be either a software or hardware device that stores sensitive information associated with their identity, such as usernames and passwords, keys and certificates. Later releases of Mozilla have a software-based security device, and can also use external security devices, such as smart cards, if the user's computer is configured to use them. The master password for the browser's built-in software security device protects the user's master key which is used to encrypt sensitive information such as email passwords, web site passwords, and other sensitive data [Mozilla Project, 2004].

The PAD should be under the control of the user, and not under the control of the identifier providers, the credential issuers or the service providers. The latter would result in a proliferation of PADs which would defeat the simplification of a client's identity management. In order to gain full advantage of the PAD, it should be a general security devise which would be able to manage many types if identities and credentials. At the same time, some service providers might have to adapt the process of registering identities and issuing credentials to suit the PAD model. Some level of standardisation, as for example described in [MeT 2002] might be needed for that to be practical.

7.2 Trust Issues in Personal Authentication Management

Being able to trust the PAD is the main trust requirement in this approach. The PAD solution provides two-factor security for using the credentials it contains by: 1) the user must possess and control

the device, and 2) the user must know the PIN for accessing and unlocking the device. The device must be tamper resistant so that, should the PAD get stolen, the thief would not be able to use it. This can be formulated as follows:

- **T8:** *The Personal Authentication Device is tamper-resistant.*

Should the PAD fail to be sufficiently tamper resistant, an attacker with physical access to the PAD could be able to extract and/or use the credentials, and thereby access service providers by masquerading as the legitimate user and owner of the PAD.

T8 trust can be established by security evaluation of the PAD according to the Common Criteria or similar, and by having a history devoid of successful attacks.

T3 trust should be considered by service providers as they would be completely dependent on users and PAD technology to authenticate themselves. T8 trust may be attainable, but trust in consumer use of the PAD may be unacceptable to providers in a similar way that lack of mediation support in formal agreements is unacceptable (ie T1 is a greater issue). In a federation model, where references are linked to form an Identity, providing "history", is a better trust-creating model.

8 Comparison of User Identity Management Models

An analysis of the various models with respect to trust requirements involved is summarised in Table 1 below.

	T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**
Isolated	✓	✓	✓					
Federated	✓	✓	✓	✓	✓	✓		
Centralised	✓	✓	✓			✓	✓	
Personal	✓	✓	✓					✓

Table 1: Comparison of client identity management solutions

As can be seen from the table, isolated trust management requires the least trust assumptions whereas federated identity management requires the most. To satisfy trust requirements is costly, and the less requirements the better. In that respect, personalised trust management seems to have relatively low trust requirements. When selecting any particular architecture, the cost related to satisfying trust requirements must also be balanced against the cost and usability of the implemented solution.

In the context of this comparison, it is also useful to see whether federated and centralised identity management solutions have clear advantages to balance the cost of increased trust requirements.

One of the main purposes of federated and centralised solutions is to simplify the identity management for clients by reducing the number of identifiers and corresponding credentials they need to manage. It should be recognised that there can not be a single federated or centralised identifier domain, and that even when federated and centralised identifier domains are available, there will still be isolated identifier domains. There will for example be existing domains that can not be migrated across, and there will be service providers with specific requirements that federated or centralised identifier domains can not meet. Even with federated and centralised identifier domains, the clients will thus still be faced with having to manage multiple identifiers and credentials. It therefore seems that personal identity management is the only generic solution which can solve client identity management complexity.

9 Service Provider Identity Management

The problem of how service providers are to be identified has received relatively little attention in the web services and e-commerce security debate.

There are some fundamental differences between identity management for clients and for service providers. Service providers usually have registers of all their clients and their digital identifiers, but the opposite is usually not the case. It is therefore often difficult to determine which digital identifiers should be used to represent a service provider.

Authentication requires a unique identifier with which the authentication credentials can be associated. Service providers that operate in a global environment like the Internet need global identifiers. Unfortunately, there exists no reliable and practical global name space for people and organisations, so that it is questionable how meaningful service provider authentication really is in the current web security paradigm.

Telephone numbers, email addresses, IP addresses, Internet domain names and OID[2] actually represent global identifiers but because they often change, they are not suitable as stable and reliable identifiers for persons or organisations. There are examples of service provider identity domains with stable and reliable unique identifiers, but none of these identity domains are both global and comprehensive at the same time. National company registers used for tax purposes offer a comprehensive list of unique identifiers on a national level. The Australian Business Number Digital Signature Certificate [NOIE 2003] is an example of how this type of identity registers can be leveraged to allow strong authentication of organisations. The Dunn & Bradstreet company number register[3] offers a global list of unique identifiers, but unfortunately it is not comprehensive, and also lacks the character of being authoritative.

9.1 Service Provider Identity Management Architecture

Despite the fact that no reliable global namespace exists for service providers in general, cryptographically strong authentication solutions have been implemented, e.g. in the form of the Web PKI. Several identifiers, such as company name, street address, domain name etc., that are provided by different name space authorities, are used in Web PKI certificates The identifiers are sent as part of the server certificate in the initial phase of the SSL protocol. The client is unable to verify the credential himself, and relies on the computer to do it for him. On successful verification the computer can display identifiers on the interface. This is illustrated in Figure 8 below.

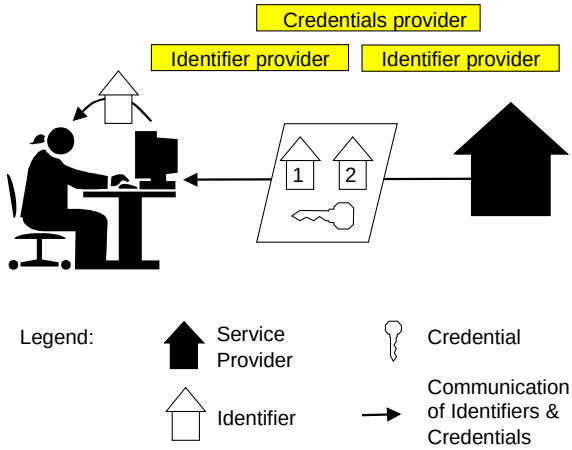

Figure 8 Service provider identity management**.**

The critical issue is how clients, and not computers, can reliably identify and authenticate the service providers. In order for the client platform to be able to authenticate the service provider on behalf of the user in a meaningful way, it needs to know the identifier of the provider that the user actually wants to access. In practice, the user types a URL, clicks on a hyperlink, or selects a URL from the local list of bookmarks/favourites, but as mentioned above, the domain name of the URL can be unreliable.

[2] Object Identifier. A standardised form of unique global identifiers. [X.500]

[3] http://www.dnb.com/us/

Recent security attacks[4] based on so-called *password phishing* have demonstrated how unreliable the service provider identification process is. A typical attack is based on sending email messages asking people to confirm their login details to their online bank by connecting to a specified URL that looks like the URL of the genuine online bank. In reality, the URL belongs to the attackers who have set up a web page that looks exactly like that of the genuine bank. The attackers can even have a server certificate that allows them to describe their web site as a "secure site" with SSL protected communication and the padlock symbol displayed on the browser. Many unsuspecting clients have disclosed their identifiers and credentials to attackers in this way.

Phishing is possible because of poor usability of Web security, and not because of weak authentication mechanism. The task of inspecting the identifiers of a service provider can be quite challenging. The browser usually checks that the domain name in the certificate is the same as the domain name pointed to by the browser, and aware users might notice when an intruder's domain name is different from the expected domain name of the service provider. However, users do not usually inspect the URL for the domain name when browsing the Web, and many companies' secure Web sites have URLs with non-obvious domain names that do not correspond to the domain names of their non-secure Web sites. One example is the Norwegian bank Nordea which is accessed with the URL: *http://www.nordea.no*, but where the URL for secure on-line banking is: *https://ibank.bbsas.no/iBank/Dispatcher*. Another vulnerability is that distinct domain names can appear very similar, for example differing only by a single letter so that a false domain name may pass undetected. How easy is it for example to distinguish between the following URLs: *http://www.bellabs.com*, *http://www.belllabs.com*, and *http://www.bell-labs.com ?*

9.2 Trust Issues in Service Provider Identity Management

The critical issue for clients is to be able to trust that the service provider they are connected to is what they expect it to be. Even though this trust is not necessarily related to a specific identifier, but rather to an identity without any clearly defined unique identifier, the trust purpose can be described as:

- **T9:** *The service provider has the expected identity.*

If the service provider does not have the expected identity, people can be fooled to give away their credentials like the example of false online banks, or they can be fooled to transact with service providers that misrepresent their identity in order to attract clients.

T9 trust can be established by having a better user interface for authentication. The problem of finding suitable global unique identifiers seems to be extremely hard to solve. One possible method could be to base global identifiers on identifiers from national business registers, with a national qualifier added, similarly to the way telephone numbers are made globally unique by adding a national prefix. Although this has the potential of creating globally unique service provider identifiers, it represents a challenge to human users if the format consists of compact numbers and letters. A personal device like a PAD could be better suited to authenticate and interpret identifiers of this type.

[4] See e.g. "Latest e-mail bank scam targets Citibank" by Dennis Fisher, eWeek, 22 May 2003 http://www.eweek.com/article2/0,1759,1504146,00.asp

10 Conclusion

Adequate management of identities in open computer networks is crucial to provide security and to improve efficiency. Identity management requires an integrated and often complex infrastructure where all involved parties must be trusted for specific purposes depending on their role. The variety and complexity of the trust relationships required in the various identity management models can cause confusion for stakeholders. Satisfying the trust requirements also has a cost. Our study has tried to concisely express and compare the trust requirements related to each model, and thereby to allow these issues to be clarified. This comparison provides a basis for assessing the cost of satisfying the trust requirements, as well as for discussing and comparing identity management solutions. In particular, personal identity management seems promising because it provides great flexibility with relatively low additional trust requirements. Personal identity management is a user centric approach that can be combined with any of the described identity management models, and thereby improve the user experience in those models.

References

Cranor, L. *et al*.: *The Platform for Privacy Principles 1.1 (P3P1.1) Specification.* W3C, 2004. www.w3.org/TR/2004/WD-P3P11-20040427/.

A. Jøsang and S. Lo Presti. *Analysing the Relationship Between Risk and Trust*. In T. Dimitrakos (editor) the Proceedings of the Second International Conference on Trust Management, Oxford, April 2004.

CCITT: *The Directory --- overview of concepts, models and services*. X.500 Series Recommendation, 1993.

Liberty Alliance: *Liberty Trust Models Guidelines*, Draft Version 1.0-15, 25 July 2003.

McKnight, D. and Chervany, N.: *The Meanings of Trust*. Technical Report MISRC 96-04, Management Information Systems Research Center, University of Minnesota,, 1996.

MeT: *Personal Transaction Protocol Version 1.0,* Draft Specification 01-11-2002, Mobile Electronic Transactions Ltd, 2002.

Mozilla Project: *Privacy and Security Preferences*, PSM 2.0 Help http://www.mozilla.org/projects/security/pki/psm/help_20/passwords_help.html

NIST: *Electronic Authentication Guideline*. NIST Special Publication SP 800-63, June 2004.

NOIE: *Australian Business Number Digital Signature Certificate (ABN–DSC), Broad Specification*. National Office for the Information Economy, September 2003.

OASIS: *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Committee Draft 01, 18 August 2004..

US OMB: *E-Authentication Guidance for Federal Agencies*. Memorandum M-04-04 to the heads of all departments and agencies, US Office of Management and Budget, 16 December 2003.

Wong, R., Berson, T. & Feiertag, R. (1985): *Polonius: an identity authentication system*, Proceedings of the 1985 IEEE Symposium on Security and Privacy, pages 101-107, 1985. http://www.anagram.com/berson/abspolo.html