An Internal Enterprise Framework for Identity based Management

Peter White, Irfan Altas, Jason Howarth, John Weckert
Charles Sturt University, Wagga NSW
Email: peter.white@lands.nsw.gov.au

Abstract

The use of Identity based Management for applications and resources is emerging as a key concept in meeting the requirements of an information security architecture. This paper looks at some of the current models for Identity Management and proposes an internal framework for an enterprise to develop an Identity based Management system. This paper describes the two major components of identity based management: identity administration and identity based access management and the processes they contain. The paper discusses the use of processes as chokepoints to enhance identity and authentication security and proposes the minimum requirements for an effective framework within an enterprise. This paper proposes that the framework should be implemented by an enterprise that intends to move towards a federation with other external enterprises. This work should contribute to the further development of identity based management models.

1 Introduction

The basis of any information system is the data and information that it holds. Information security is employed to protect these valuable assets and resources and some enterprises spend considerable amounts of money in dealing with perceived security problems. But, the security of the data relies, in part, on who has access to the data and "…anyone who steals the identity of one of your users becomes that user and has access to your most sensitive systems and data. If just one user's identity is compromised, your systems are vulnerable" (Wood 2005, p.12).

The Australian standard AS/NZS ISO/IEC 27001:2006 (Standards Australia & Standards New Zealand 2006), details the requirements for human resources security in order to conduct verification of identity: for provisioning of user accounts as well as the de-provisioning of user accounts on termination or change of employment; for access to operating systems; for access to network services and resources; for user access management; for change control. An identity based management system will provide many of the internal controls that will facilitate compliance with the standard.

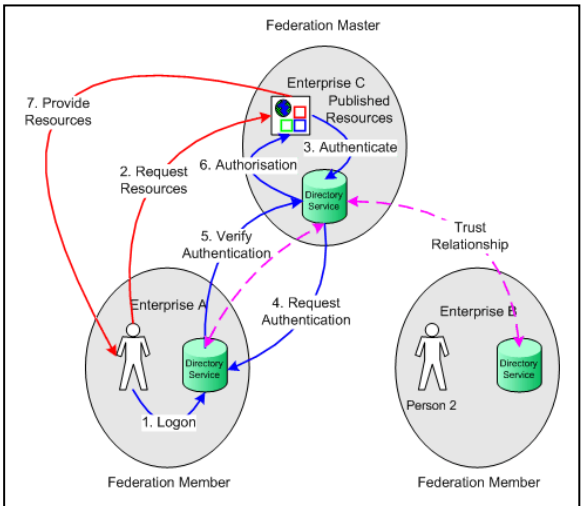

Figure 1: The Federation Model

Identity based Management systems are often implemented when an enterprise decides to join a federation (Fig. 1). A federation may be created when an enterprise has resources that it wishes to publish and which other enterprises wish

to consume. The enterprise that publishes the resources is known as the federation master, while enterprises that consume those resources are known as federation members. Typically, a federation is created when the federation master allows users in a federation member enterprise to authenticate and consume the published resources using their own internal federation member identity and authentication credentials.

The business need that leads to federation also extends the requirements of both the Threat and Risk Assessment (TRA) and the Information Security Management System (ISMS). These must now consider any external federation needs as well as any possible external threats.

It is unlikely that an enterprise will be able to impose its ISMS policies on an external enterprise in a federation. However, an enterprise may be able to negotiate, as part of an Information Exchange Agreement, that a particular framework be used for authentication, authorisation and access management within the federation. A key stipulation of any such framework should be that it is not tied to any particular technological solution, but must be capable of being implemented using existing systems. The framework should also offer a verifiable method of auditing authentication. This will act to add assurance that the risk of intrusion coming from an enterprise partner, as the result of a chain of trust, has been reduced to an acceptable level (Day 2003).

There has been considerable research and development into the models for use in a federation between enterprises or for use on the Internet (Cameron 2005; Casassa Mont 2004; He & Zhang 2005; Josang et al. 2005), but there has been little research into the basic enterprise framework. The Open Group (2002, p.25) states that there is no standard enterprise Identity Management architecture, and that enterprises define individual architectures to meet their specific needs. However, the increasing importance of compliance with standards, combined with the need to operate with procedures that can be verified and audited, means that this stance can no longer be adopted.

In Section 2 we propose the *internal enterprise framework* and describe its components and minimum requirements. In Section 3 we present the advantages and issues of the proposed internal enterprise framework. The current view of Identity based Management, the proposed internal enterprise framework and suggestions directions for further research are discussed in Section 4.

2 The internal enterprise framework

The literature describes three basic models of federation:

- A federation model where a local enterprise will allow the identities from a remote enterprise to have access to certain resources within the local enterprise, based on the authentication of that identity within the remote enterprise (Casassa Mont, Pearson & Bramhall 2003).
- A distributed model where the management of identities and control of access to resources is distributed amongst a number of trusted repositories. Each repository is responsible for the management of its own identities and resources. Each repository also trusts the identities from other repositories that it has trust relationships with for access to its resources (He & Zhang 2005).

- An Internet model where a trusted authentication provider certifies the digital identity of an entity. This digital identity can then be trusted by third parties who also use that authentication provider as a means of authentication (Cameron 2005; Josang & Pope 2005; Wason 2003).

Each of these models implies that there is an enterprise level framework that underlies and supports the described models within each enterprise. Without an underlying framework, the models described above must be considered at risk. The one common factor between these described models is trust. Each enterprise that enters into a federation must trust that all other parties are diligent and consistent in their approach. If one party cannot trust another then the federation is doomed to failure.

Currently there is no single agreed enterprise level framework. It is assumed that an enterprise framework exists, but there is considerable confusion over what it contains and even of the definition of terminology. Possibly the best single definition is as follows: "Identity Management has two principal components — management *of* identity and management *by* identity. Management of Identity is the process of issuing and using digital identities…Management by Identity combines the proven identity of the user with their authorisation, in order to grant access to resources" (Wood 2005, p.12). This definition means that the usual term Identity Management is simply not precise enough to describe what is actually meant. It is therefore proposed to use the term *Identity based Management* to more accurately describe the combination of both components. *Identity based Management* (IbM) gives a more intuitive understanding of how these two components interact.

An internal enterprise framework can be defined as one that combines the *identity administration* of entities and their identities with *identity based access management* to control access to the resources of an enterprise. It is the base on which all subsequent models must rely.

The internal enterprise framework is proposed as a solution to the lack of an agreed enterprise framework. This framework details the minimum requirements for an effective IbM solution for an enterprise.

In the internal enterprise framework each enterprise is responsible for the management of its own internal identities which is to be conducted in a verifiable manner. An enterprise may enter into contractual information exchange agreements with other enterprises in order to share resources and these contractual agreements will lead to the creation of a trust between the two enterprises. An information exchange agreement should also include an assurance that the identities of the enterprise have been verified.

The administrative burden of external user management for a resource can be reduced if the enterprise enters into a federation with other enterprises that wish to consume the resources on offer. Each enterprise joining a federation would complete an Information Exchange Agreement (IEA) which then forms the legal basis for a trust relationship between them. The federation master can now allow entities from federation members to access its resources based on their internal identities and authentication credentials. The federation master has effectively moved the administrative burden of managing external identities from itself to the federation

members that own those identities. As a result, all requests for authentication and access are sent to the relevant directory service in the originating enterprise. All authentication requests are SASL (Simple Authentication and Security Layer) Bind requests to the appropriate LDAP server (Arkills 2003; Wahl et al. 2000).

However, the danger for an enterprise in a federation, particularly the federation master, is that one of the member enterprises may allow its internal identities to be compromised by a third party. This situation may be countered by an information exchange agreement which includes an assurance that the internal verification of identities and their authentication is in accordance with an agreed framework and is subject to audit by all parties to the agreement.

It should be noted at this stage, that the internal enterprise framework is designed to be technology agnostic. The internal enterprise framework is really more about process and process management than technological implementation and as such should be easily implemented in any LDAP based directory service system.

The internal enterprise framework consists of two major parts — *Identity Administration* and *Identity based Access Management* as shown in Fig. 2.

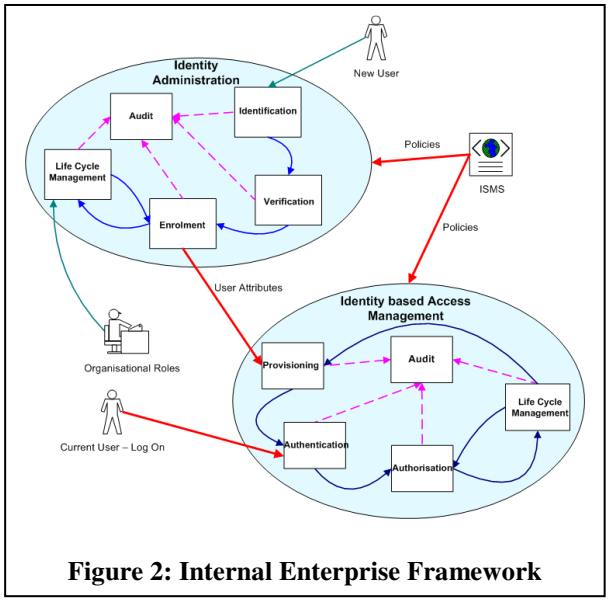

Figure 2: Internal Enterprise Framework

2.1 Identity Administration

Identity administration is the process of positively identifying an entity, determining the identifiers to be used and issuing credentials for future authentication. This process comprises a number of components: identification, verification, enrolment, life-cycle management and audit.

Fig. 3 shows how the *identity administration* components interact. A new entity first presents the formal identification documents that are required by the enterprise. The enterprise verifies the entity's identity according to its internal procedures. When the identity has been verified, the entity's digital identity is created in the enrolment process and the appropriate authentication credentials are assigned. Depending upon the enterprise's policies, the identity may also be assigned to an organisational role during enrolment. It should be noted that for many enterprises the procedures of

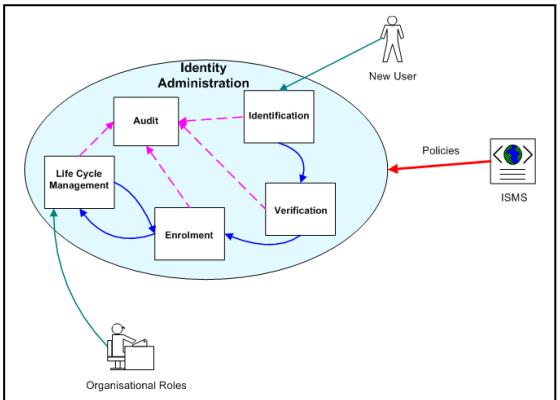

Figure 3: Identity Administration

identification and verification may well remain manual procedures. However, all of these procedures must be in accordance with the enterprise's ISMS and must provide a full audit trail.

The enrolment process in identity administration creates a chokepoint where all identities for the systems are created. Day (2003, p. 86) argues that a chokepoint enhances security by allowing much closer security focus, control and monitoring on a point of access. This chokepoint allows the verification of any identity that is created by using the processes of identification, verification and enrolment. These processes should ensure that all employee, contractor and service accounts that are created for use in the system can now be verified. These processes also ensure that the unauthorised creation of identities cannot occur without being audited and discovered. Real-time auditing and discovery are available through the use of various auditing tools which may also act to prevent unauthorised identity creation. This chokepoint and the associated processes provide an assurance to the business, as well as to any external federation partners, that the enterprise's identities are both valid and verifiable.

2.2 Identity based Access Management

Identity based access management (IbAM) is the process of authenticating an identity that is claiming access, authorising access to certain resources and auditing the authentication and use of those resources. *Identity based access management* (Fig. 4) has a series of components: provisioning, authentication, authorisation, life-cycle management, change control and auditing.

Fig. 4 shows how the *identity based access management* components interact. A new entity's identity is initially passed to the Provisioning module for provisioning of the account. This includes creating email accounts, database accounts and any other accounts that are required for the entity's role in the enterprise. Provisioning may also include Single Sign On (SSO) arrangements where the entity's authentication credentials are also accepted by some or all enterprise applications.

When an entity attempts to logon to the system, they are initially authenticated through the enterprise's LDAP directory service. The authenticated identity is then authorised to access certain enterprise resources using the enterprise's access control method. However, these procedures must be in accordance with the enterprise's ISMS (Fig. 4) and must provide an audit trail. Life-cycle management, which also includes change control, allows for any change of role for all entities in the system.

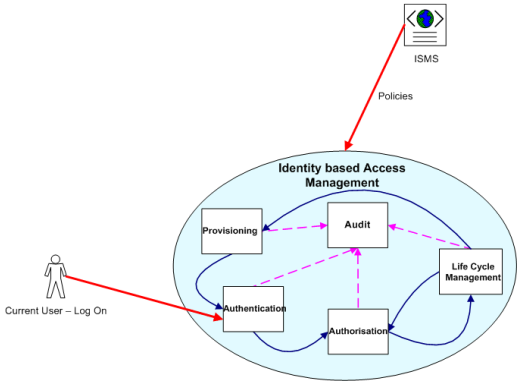

Figure 4: Identity based Access Management

The provisioning process also creates a chokepoint. The traditional method of provisioning identities into a system requires the administrator of the system to manually add an identity and an authentication credential, usually a username and

password combination, to the system user database. This allows two separate entities to have access to the same digital identity and its authentication credential. This may raise security issues if it occurs without proper authorisation or documentation.

The manual provisioning of identities into individual systems can still occur under the internal enterprise framework. But this process must now be documented, verified and audited. The ideal situation occurs when the provisioning process is automated and all provisioning into individual systems occurs as the result of a policy-driven event. The provisioning process should be tied to a robust access control system, such as a role based access control system. This would then act to ensure that a digital identity would only be provisioned into an individual system when the identity's role required it and that the identity would then receive only the level of access that the role required. This chokepoint would act to remove the possibility of unauthorised identities being created in individual systems, as well as removing the possibility of two entities knowing the credentials of a single digital identity.

The creation of chokepoints at the points of enrolment and provisioning will act to prevent the creation of chains of trust in a federation. These chokepoints ensure that only verified identities are provisioned into the applications authorised for that identity. This will act to prevent untrusted identities gaining access by masquerading as a trusted identity.

A third chokepoint is created in the process of authentication. As an enterprise implements provisioning through its individual systems, it creates, in effect, a system of Simplified Sign On for identities where the authentication for all the individual systems now occurs through the main enterprise authentication system. This removes the requirement for each individual system to have its own set of identities and authentication credentials.

The use of a single method of authentication based on the enterprise's LDAP directory service means that a single, consistent authentication policy can be applied across the enterprise. The authentication strength can be increased as there is now a single method of authentication that is employed at each system boundary. This authentication chokepoint, when combined with the enrolment and provisioning chokepoints, provides a layered security approach that enhances information security and effectively reduces the chance of "back door" access being available in strategic systems and resources.

2.2.1 Access Control

The purpose of authorisation, or access control, is described as follows: "… to limit the actions or operations that a legitimate user of a computer system can perform. Access control constrains what a user can do directly, as well as what programs executing on behalf of the users are allowed to do. In this way access control seeks to prevent activity that could lead to a breach of security."(Sandhu & Samarati 1994, p.40). The major forms of access control are:

- **Discretionary Access Control** (DAC). DAC policies control access to resources based on the proved identity that requests the access and on access rules stating what certain requestors are, or are not, allowed to do.
- **Role-based access control** (RBAC) assigns access rights to a series of roles rather than individual users. Users are granted membership of roles based on

their competencies and responsibilities in the organisation (Hu, Ferraiolo & Kuhn 2006, p.7). Users then receive access rights based on the role that they are assigned. RBAC allows a user to access all the resources that are authorised for that particular role.

- **Rule based Access Control** (RUBAC). RUBAC allows users to access systems and information based on pre determined or configured rules.
- **Attribute based Access Control** (AbAC). AbAC allows access based on certain attributes of the identity requesting the access (Lang et al. 2006; Wang, Wijesekera & Jajodia 2004).
- **Usage Control** (UCON). Usage control encompasses traditional access control, trust management and also digital rights management.

The authorisation component of *identity based access management* can use any of the major access control models. This is a decision that can only be made by the individual enterprise after it has completed its TRA and ISMS. The internal enterprise framework does require that the enterprise specify which model it is using and that its operation be audited. An enterprise that is planning to implement an internal enterprise framework must seriously consider whether the standard model of discretionary Access Control Lists is satisfactory and in accordance with its ISMS.

2.3 Minimum requirements

There are certain minimum requirements for the implementation of this framework. These are:

- **Entity identification and verification process**. This is a business process that must formally verify the identity of an entity requesting access to enterprise resources.
- **Identity enrolment process**. This process must determine the identifiers to be used to identify an entity, enter the entity into an authoritative source and issue credentials to allow the entity to authenticate its identity.
- **Identity life-cycle management**. This process must follow the life-cycle of the identity and its credentials and ensure that they are updated, maintained and validated or revoked as required.
- **Directory Service.** Directory services provide the major method of authenticating and applying security policies within an enterprise. A functional directory service covering the entire enterprise is a minimum requirement for an effective *identity based access management* system.
- **Provisioning**. The provisioning process creates all the accounts and access rights that an entity will require to complete their role and responsibilities within the organisation.
- **Access Control**. Access control provides the method of ensuring that only properly authenticated identities are provided with access to just those resources that they are authorised to access.
- **Life-cycle management**. This process monitors the life-cycle of an identity and ensures that the changing role of the identity is correctly maintained. It must also contain a revocation policy to ensure that the identities of entities that leave the organisation are correctly decommissioned. A system of change control is required as part of the life-cycle management process. This ensures that all proposed changes are checked and authorised before implementation.
- **Audit process**. This process must audit each process of the identity administration and identity based access management components. The audit

process must include a method of regularly reviewing these logs for anomalies.

An identity based management system developed using the internal enterprise framework should provide a sound solution within the enterprise that will be consistent with the enterprise's information security architecture. The identity based management system is then capable of being extended into a Federation with other enterprises.

3 Advantages and Issues

The implementation of an internal enterprise framework gives an enterprise a number of advantages.

The internal enterprise framework works with the existing enterprise authentication, and access control system. It ensures that the current system is fully documented, but allows for improvement and the implementation of new technologies.

The internal enterprise framework assures an enterprise that its identity based management system is managed in accordance with a known framework and has been included in the enterprise ISMS. This framework also assures potential federation partners that it has an identity based management system that can be verified and audited. This will increase the level of trust between federation partners.

The set of minimum requirements that is proposed also clarifies the scope of any identity based management project. It also allows the enterprise to implement an identity based management solution in phases. The implementation of identity administration neatly fits as the first phase for any implementation project. The implementation of identity based access management then naturally follows for all or part of the enterprise.

The internal enterprise framework creates three chokepoints which act to check and verify that:

- All identities are created in through a documented, verified and audited process for all systems and each identity that is created can be verified;
- All provisioning of identities to allow access to systems and resources now occurs through a documented and verifiable process that can be automated;
- All identity claims are authenticated through a single strong authentication system that allows verification and audit;

Although the chokepoints add layers of security to the system, they also add single points of failure that can cripple the system if successfully attacked, or in the case of loss of system resources. These chokepoints need to carefully assessed and monitored.

A move from simple password based access to a more sophisticated access control system gives the enterprise a number of advantages. These include:

- The management of authorisation. An enterprise can set up a series of policies that determine the rules for access to resources. These rules can then be applied by the selected access control system to give a more granular approach

to access control that can be applied consistently. This allows users whose organisational role has changed to be quickly given the correct security rights.

- A hierarchy of policies can be established where policies can be arranged according to the principles of generalisation, specialisation and inheritance. This will allow users appointed to a specialised role to inherit rights and privileges associated with more general roles.
- Least Privilege. The use of least privilege policies requires users to act with the least amount of privilege required for a particular task. Users who are authorised to use powerful roles do not need to exercise them in all situations. This acts to prevent inadvertent damage and errors and also acts to prevent intruders masquerading as legitimate users.
- Separation of Duties. There are many organisational roles where a single user is not allowed sufficient privilege to misuse the system, for example the person authorising payments should not be the same person who prepares the payment. This separation of duties can be enforced by policies which define those conflicting roles that cannot be held by a single person, or by enforcing that separation dynamically at run time.

4 Conclusion

The use of Identity Management is often proposed without a clear understanding of what is implied or what constitutes an identity management framework. There has been considerable research and development into frameworks and models for use in a Federation and on the Internet, but there has been little research into the basic Enterprise framework.

The use of the term Identity based Management removes some of the imprecision and confusion that was attached to the more generic term Identity Management. The proposed internal enterprise framework offers a clear definition of the framework that is easily understood. It shows clearly that this framework must be implemented internally within an enterprise before it can be extended to a Federation model.

The framework consists of two major parts — *identity administration* and *identity based access management*. *Identity administration* is the process of positively identifying an entity, determining the identifiers to be used, enrolling and issuing credentials for future authentication. *Identity based access management* is the process of authenticating an identity that is claiming access, authorising access to certain resources and auditing the initial authentication and use of those resources.

An *Identity based access management* system developed using these requirements should provide a system that will provide a sound solution within the enterprise that will be consistent with the enterprise's information security architecture.

Further research on the *internal enterprise framework* is required to determine that it is suitable for implementation in a range of enterprises and in different federation architectures.

Reference List

Arkills, B 2003, *LDAP Directories Explained*, Pearson Education Inc, Boston, MA.

Cameron, K 2005, *The Laws of Identity*, Microsoft Corp., Redmond, WA, viewed 1 September 2006, <http://msdn.microsoft.com/webservices/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-us/dnwebsrv/html/lawsofidentity.asp>.

Casassa Mont, M 2004, *Identity Management: On the "Identity=Data + Policies" Model*, HP Laboratories, Bristol, UK, <http://www.hpl.hp.com/techreports/2004/HPL-2004-14.pdf>.

Casassa Mont, M, Pearson, S & Bramhall, P 2003, 'Towards Accountable Management of Privacy and Identity Information', *Lecture Notes in Computer Science*, vol. 2808, pp. 146-161.

Day, K 2003, *Inside the Security Mind. Making the tough decisions*, Prentice Hall, Upper Saddle River, NJ.

He, J & Zhang, R 2005, 'Towards a Formal Framework for Distributed Identity Management', *Web Technologies Research and Development - APWeb 2005*, Springer-Verlag, Heidleberg, Germany, pp. 913-924.

Hu, V, Ferraiolo, D & Kuhn, D 2006, *Assessment of Access Control Systems*, National Institute of Standards and Technology, viewed 4 October 2006, <http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf>.

Josang, A, Fabre, J, Hay, B, Dalziel, J & Pope, S 2005, 'Trust Requirements in Identity Management', *ACSW Frontiers*, vol. 44.
Notes: Viewed 09/02/2006.

Josang, A & Pope, S 2005, 'User Centric Identity Management', *AusCERT Conference 2005*.

Lang, B, Foster, I, Siebenlist, F, Ananthakrishnam, R & Freeman, T 2006, *Attribute Based Access Control for Grid Computing*, Argonne National Laboratory, Argonne, IL, USA, viewed 28 April 2007, <ftp://info.mcs.anl.gov/pub/tech_reports/reports/P1367.pdf>.

The Open Group 2002, *Identity Management Business Scenario*, The Open Group, San Francisco, <http://www.opengroup.org/bookstore/catalog/k023.htm>.

Sandhu, R & Samarati, P 1994, 'Access Control: Principles and practice', *IEEE Communications*, vol. 32, no. 9, pp. 40-48.

Standards Australia & Standards New Zealand 2006, *AS/NZS ISO/IEC 27001:2006 Information Technology - Security Techniques - Information security management systems - Requirements*, Standards Australia, Sydney.

Wahl, M, Sun Microsystems Inc, Alvestrand, A, EDB Maxware, Hodges, J, Oblix Inc & Morgan, R 2000, *RFC 2829: Authentication Methods for LDAP*, Internet Engineering Task Force, viewed 3 April 2007, <http://www.ietf.org/rfc/rfc2829.txt>.

Wang, L, Wijesekera, D & Jajodia, S 2004, 'A logic-based framework for attribute based access control', *Workshop on Formal Methods in Security Engineering*, pp. 45-55.

Wason, T 2003, *Liberty ID-FF Architecture Overview*, 1.2-errata-v1.0, Liberty Alliance Project, Piscataway. NJ, viewed 21 August 2006, <http://projectliberty.org/liberty/content/download/318/2366/file/draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf>.

Wood, P 2005, 'Implementing identity management security - an ethical hackers view', *Network Security*, pp. 12-15.