Identity Management for a Spatial Data Infrastructure

S. Woodhouse & P. White
Department of Lands

Abstract- **The Spatial Data Infrastructure (SDI) raises problems for enterprises accessing resources in federations. The integrity and availability of this SDI is a prime concern for the custodians and managers of these SDI's. This paper proposes the development of an Identity Management (IdM) system for assuring the security of the SDI. The IdM system would ensure that only positively identified entities are authorised to access and update GIS datasets that are part of the SDI. In this paper a new Federation Cluster Framework (FCF) is proposed to enhance the security and availability of the SDI. This paper also proposes the use of an Identity Management Framework (IdMF) for use within the SDI framework.**

I INTRODUCTION

Geospatial information systems (GIS) encompass information about natural resources, the environment, land ownership and use, transport, communications, utility services, demography and socio-economic factors, in fact any information that can be related to location.

The members of every community, through their government agencies, depend upon access to spatial information as a foundation for planning and managing their environment. Using geospatial technologies such as mapping, surveying, aerial photography, remote sensing, global positioning technologies and satellite imagery unique databases of geospatial information about the world we live in are compiled[1].

"Sometimes the visual language of GIS allows us to communicate without saying a single word, which is the essence of effective communication"[14]. Access to this knowledge gives us the ability to manage our current environment and plan our future environment. It also has the potential to provide our enemies with more information about our critical infrastructure than they have ever been able to obtain[1].[1]

This geospatial information is made accessible to organisations and the community via a collection of policies, people, administrative arrangements, and technologies called the Spatial Data Infrastructure (SDI)[2]. The identity of who is consuming and updating these spatial information systems is an important information security issue for the managers of these SDI's. The development of an Identity management (IdM) system would seem the most logical step. The IdM system would ensure that only positively identified entities are authorised to access and update GIS datasets that are part of the SDI.

II SPATIAL DATA INFRASTRUCTURE

The Spatial Data Infrastructure (SDI) provides a basis for spatial information discovery, evaluation, and application for users and providers within all levels of government, the commercial sector, the non-profit sector, academia and by citizens in general[2].

The term Global-Spatial Data Infrastructure (G-SDI) is used to encourage the concept of a reliable, supporting environment, analogous to a telecommunications network that, in this case, facilitates the access to geographically-related information using a minimum set of standard practices, protocols, and specifications.

More succinctly it means ready access to spatial information at the global level, organised by region clusters, sponsored by participating nations where the sources-of-truth are maintained by custodians of clearinghouses (agencies) and where State nodes aggregate agency metadata. Ready access to spatial information is now a global concern and is reflected in the growing interest in the concept of a G-SDI.

The SDI exists at four levels, a G-SDI which is a super-set of the Regional-SDI (R-SDI) which is a super-set of the National-SDI (N-SDI) and which is a super-set of the State-SDI (S-SDI). The intent of the SDI is to seamlessly link spatial information so that it appears, to the user, as a virtual data resource.

This linkage will occur via an intra-regional institutional framework that provides mechanisms for sharing experience, technology transfer and coordination of the development of the regional fundamental datasets.

The S-SDI is a physical, organisational, and virtual network designed to enable the development and sharing of the state's digital geographic information resources. Each S-SDI will be aggregated with all other state jurisdiction SDI data into a N-SDI framework.

III INFORMATION SECURITY

The purpose of information security is to protect valuable assets, such as geospatial information and its supporting infrastructure, such as hardware, software and people. Information security should support the business objectives or mission of the organisation, it must be cost effective,

[1] Steven Woodhouse (steven.woodhouse@lands.nsw.gov.au) is the Manager Technical Services and Peter White (peter.white@lands.nsw.gov.au) is the Information Security Architect for the NSW Department of Lands. They are both currently completing Doctor of Information Technology degrees at Charles Sturt University, Wagga Wagga, NSW Australia.

ICITA2008 ISBN: 978-0-9803267-2-7

must be holistic, and fit into the organisation's culture seamlessly[3].

The aim of planning, designing and implementing security in and around geospatial information systems is to ensure not only the confidentiality and integrity of the information produced, stored and used but also the continued availability of both the geospatial information and supporting infrastructure[3-5].

The C.I.A triad represents the basic, industry accepted, principles of information security. Confidentiality is the practice of preventing unauthorised disclosure of information. Integrity ensures the security and trustworthiness of systems. It does this by ensuring that changes to information can only be made in a specified manner and by specified people or processes. Availability allows the accurate and timely access to the organisation’s information systems and dependent processes when required. It has been argued that the classic triad of "C. I.A." is inadequate to describe the requirements of information security for the modern enterprise[6].

Geospatial information is now critical to business operations and decision making activities for governments at all levels and private organisations, allowing these organisations to survive and grow in competitive and tough economic environments, and governments to provide services and infrastructure to their constituents.

As organisations have evolved management has applied the sophistication of new technology without due regard to the shortcomings and risks inherent in its application. Advances in technology, especially the Internet, have allowed organisations to expand rapidly by utilizing e-business. Unfortunately, the development of security tools has lagged behind and as e-business and Internet applications continue to grow it has become more difficult to protect organisational assets [7].

IV Identity Management Models

Identity Management has been defined as having "…two principal components --- management *of* identity and management *by* identity [8]. An Identity Management Framework can be defined as *a structure of processes and workflow that implements a digital identity infrastructure* [9]. This definition allows a better understanding of the standard federation models, as it shows that Identity Management must occur both within the enterprise as well as being a method of external authentication and authorisation.

A federation model is one where a local enterprise will allow 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[10].

A distributed federation model is one where each enterprise is responsible for the management of its own identities and resources. Each enterprise also trusts the identities from other enterprises that it has trust relationships with, for access to its resources[11].

An Internet model is one that allows an entity to certify an identity with a trusted authentication provider[12-15].

Each of these models implies that there is an enterprise architecture that exists within each enterprise and thereby underlies and supports the described models.

V Federation Cluster

It is proposed that a federation cluster be developed for use within the SDI framework.

A federation cluster can be defined as a group of federations that are united in order to share resources between individual members of each of the federations as shown in Fig. 1.

The federation cluster architecture calls for a directory service to be located in each federation. This allows for the aggregation and the publication of resources and services that are published by any of the member enterprises. A directory service within the top level federation cluster then allows the definition of a single namespace for the entire federation cluster. This would allow a member enterprise of a member federation to discover all the resources and services that are available within the federation cluster.

A federation cluster may also aggregate user attributes. This will also work to simply authentication as it will allow the federation cluster to identify which enterprise that the identity claim originates from.

Each enterprise that is to join a federation should complete a formal Information Exchange Agreement in order to fully detail the extent of the federation and information that is to be exchanged as part of the federation.

External identity providers may also be invited to access the federation cluster in order to allow individuals access to the resources of the cluster. The identity provider would need to have an Information Exchange Agreement in place that is similar to the agreements with each of the enterprises in the federation cluster.

The federation cluster allows resources from multiple enterprises in multiple federations to be aggregated and published at a single point. This allows these resources to be organised and published in a coherent manner so that all resources can be quickly located and accessed regardless of their original location.

The federation cluster now provides a method that allows the organisation and publishing of resources throughout the federation cluster as well as providing access mechanisms that allow the resources to be accessed externally and internally through an IdMF.

VI Identity Management Framework

In order for a federation to be created, the enterprises intending to federate must agree to a form of Information Exchange Agreement (IEA) that details the basis of the federation along with the resources that are to be available to members of the federation [16]. It should also include an assurance that each enterprise maintains an enterprise level framework that describes the internal process of control and management of processes, identities authentication and authorisation. This agreement forms the basis of the trust agreement that will allow entities from one enterprise to access resources in another enterprise[16].

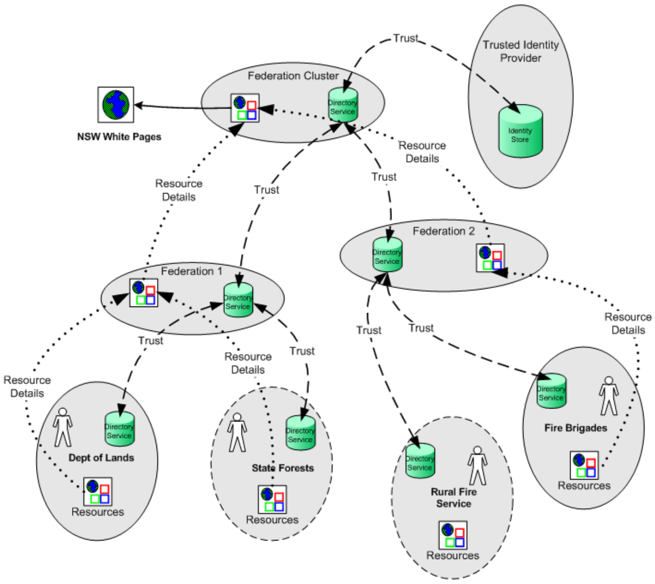

Figure 1: The Federation Cluster

The Australian standard AS/NZS ISO/IEC 27001:2006[17] requires that, for external parties to access an enterprise's information or information processing facilities, there must be an assessment of the risk; an identification of the information security requirements and a formal agreement between the parties[16].

An IEA that provides these assurances will be the basis of the formal contract trust relationship between enterprises that will allow the sharing of information and resources in a federation.

Currently, there is no model or framework available that can provide the verifiable assurance that is required under an IEA.

An IdMF has been defined as one that concentrates the internal management of identities and control of access to the resources of an enterprise [9]. The IdMF details the minimum requirements for an effective enterprise solution and would form part of an enterprise Identity Management Architecture[18].

In this framework each enterprise is responsible for the management and verification of its own internal identities. 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 is the document that defines the contractual trust arrangement. The IEA may be created under the AS/NZS ISO/IEC 27001:2006 standard. It should also include an assurance that identities are verified in accordance with an agreed framework. Each local enterprise using the framework is responsible for managing the identity of any other remote enterprise with which it has an Information Exchange Agreement.

The IdMF is technology agnostic. The framework should be implemented using any LDAP based directory service. The IdMF is really more about process and process management than technological implementation.

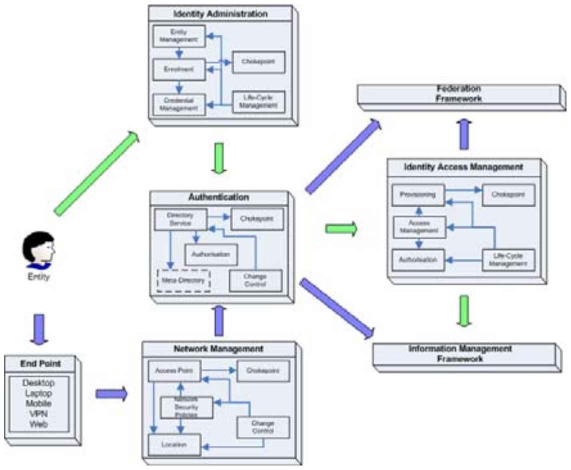

Figure 2: Identity Management Framework

This framework consists of four components: *Identity Administration, Authentication, Identity Access management* and *Network Management* as shown in Fig. 2.

The Entity Management module deals with entity identification and verification. It handles all enrolment of entities into the system and the creation of their identities. This module is also used to change an identity’s role in the enterprise. The Credential Management module deals with the issue, updating and replacement of authentication credentials. This can include passwords, smartcards, One Time Password tokens or biometrics. Both of these modules operate within a workflow that is defined in the Life-Cycle Management module. The Change Control module ensures that all changes to identities and their credentials have been approved prior to the change being implemented.

It should be noted that for the vast majority of enterprises the procedures of identification and verification will probably remain as manual procedures. However, these procedures must be conducted in accordance with the enterprise's Information Security Management System (ISMS) and an audit trail must be provided.

The Identity Access Management component contains a Provisioning module. This module creates the access rights for an identity in a specific system. Provisioning is the dynamic process of establishing the specific access rights for a specific identity. The creation of an identity triggers a series of policy driven events such as the creation of a network account, an email account, various database accounts, and so on. In effect, the provisioning process creates all the accounts and access rights that an entity will require to complete their role and responsibilities within the organisation [19, 20]. The provisioning process must be in accordance with the enterprise ISMS and give the new identity access to only those resources that it actually requires. Traditionally, provisioning is done manually by the administrators of a system, but this is being gradually replaced by automated systems that provision entities based on their role or requirements in the enterprise.

Authentication is the process of checking the identity claim and credentials of an identity that is claiming access to the system. An LDAP directory service is required for authentication as it allows for a single authentication policy to apply a set of defined criteria to be applied to all identities that request authentication. This removes the different types and levels of authentication that can be found in silos of data and replaces them with a single authentication policy that can still apply different levels of authentication.

If the identity claim is authenticated, the authenticated identity is passed to the Access Management module. Directory services provide the major method of authenticating and applying security policies within an enterprise.

Authorisation, or access control, is the process of granting access to certain resources to an authenticated identity. The purpose of authorisation is described as "… 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"[21]. The Access Management module acts to ensure that only identities with the correct access rights are allowed access to each of the enterprise resources.

The Access Management component can use any of the major access control models. This is a decision that can only be made by an individual enterprise after it has completed its Threat and Risk Assessment (TRA) and Statement of Applicability (SoA). The IdMF 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 IdMF must seriously consider whether the standard model of discretionary Access Control Lists is really adequate for use in the framework.

The Life-Cycle Management module manages the life-cycle for enterprise roles or requirements in both Provisioning and Access Management. Again, changes to either module must be approved through a change control process.

VII FEDERATION FRAMEWORK

In order for a federation to operate effectively there must be a number of components in place. These include the Information Exchange Agreement that details the contractual arrangements between the enterprises. Another essential component is the Federation Framework. This framework allows an enterprise to determine and specify the requirements for access by external enterprises.

The federation component provides a method of detailing the requirements for federation with external partners as shown in Fig. 3. The Access Requirements module requires the enterprise to detail the requirements for external access to its resources. The Security Requirements module allows the enterprise to detail any additional security requirements for external access. The DRM module requires the enterprise to examine the issue of Digital Rights Management for resources that may be downloaded and consumed. The Information Exchange Agreement module allows the enterprise to consider the legal trust agreements that will be set up with enterprise partners. The final module, the Federation Service module, allows the enterprise to decide the type of federation and how it is to be implemented.

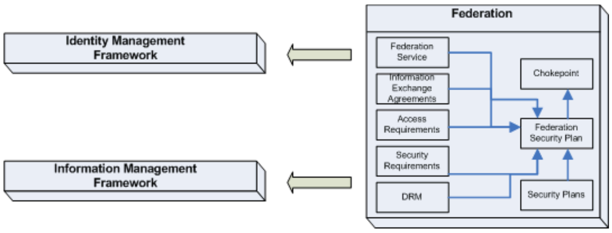

Figure 3: Federation Framework

The federation framework links to the enterprise's IdMF. This ensures that the federation is integrated into the enterprise Identity Management Architecture. Fig. 3 shows how the federation Framework links to the IdMF for Authentication and Access Management. It also shows how additional security can be included before allowing access to enterprise data and resources.

The details of the federation framework should also be included in the IEA as part of the enterprise trust agreement.

VIII CONCLUSION

The federation cluster offers a method of consolidating and publishing resources that exist in multiple federations from a single point. This framework also ensures that the authentication of a user that is requesting access to a resource is always handled by the originating enterprise of the user. This acts to prevent unauthorised or expired credentials being accepted. The federation cluster also allows for the authentication of external users, who are not part of the federation cluster, by allowing authentication from trusted third party identification providers.

The expanding use of federations to provide access to resources means that any enterprise joining a federation now needs to change the focus of its TRA and SoA to include its federation partners. The information exchange agreements that each enterprise must negotiate should now include references to the use of an IdMF. This will ensure that the enterprise is managing its internal identities in accordance with its ISMS and policies. It will also act to assure an external enterprise that the identities that seek to access its resources are correctly identified and authenticated.

The implementation of a federation framework assures any enterprise in the framework that identity management is managed in accordance with a known framework and has been included in the enterprise ISMS. This framework also acts to assure federation partners that a verifiable and auditable identity management system is in place. This acts to increase trust between federation partners.

A federation framework links into the enterprise IdMF. It ensures that the current system is fully documented, but allows for improvement and the implementation of new technologies. The federation framework is technology neutral.

A federation cluster allows resources from multiple enterprises in multiple federations to be aggregated and published at a single point. This allows these resources to be organised and published in an organised, logical manner so that all resources can be quickly located and accessed regardless of their original location. It also offers a method of providing access mechanisms to allow the resources to be accessed externally or internally through a federation and IdMF.

IX ACKNOWLEDGMENT

We would like to acknowledge the kind assistance of Dr. David Tien of Charles Sturt University in the preparation of this paper.

X REFERENCES

[1] S. Woodhouse, J. Howarth, and D. Tien, "A management approach to securing geospatial information systems," in *Fourth International Conference on Information Technology and Applications ITCITA 2007*, Harbin, China, 2007, pp. 100-105.

[2] D. Nebert, *Developing Spatial Data Infrastructures: The SDI Cookbook*: GSDI, 2004.

[3] T. R. Peltier, J. Peltier, and J. A. Blackley, *Information security fundamentals*: Auerbach, 2003.

[4] Devargas, *The total quality management approach to IT security*. Oxford, UK: NCC Blackwell, 1995.

[5] McCumber, *Assessing and managing security risk in IT systems: A structured methodology*. USA: CRC Press LLC, 2005.

[6] D. B. Parker and M. E. Kabay, "Fighting computer crime : a new framework for protecting information," in *Computer Security Handbook*, 4th ed, S. Bosworth, Ed. USA: John Wiley & Sons, INC., 2002, pp. 5.1 - 5.21.

[7] Campbell, Calvert, and Boswell, *Security+ Guide to Network Security Fundamentals*. Boston, USA: Thomson, Course Technology, 2003.

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

[9] P. White, I. Altas, J. Howarth, and J. Weckert, "An Internal Enterprise Framework for Identity based Management," in *Australian Partnership for Advanced Computing 07*, Perth, WA, 2007.

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

[11] J. Rouault and J. Pato, "Identity Management: the drive to freedom," Hewlett-Packard Development Company, 2003.

[12] K. Cameron, "The Laws of Identity," Redmond, WA, USA: Microsoft Corp, 2005.

[13] T. Daemen and I. Rubinstein, "The Identity Metasystem: Towards a Privacy-Compliant Solution to the Challenges of Digital Identity," Redmond, WA: Microsoft Corp, 2006.

[14] A. Josang and S. Pope, "User Centric Identity Management," *AusCERT Conference 2005*, 2005.

[15] S. Cantor, J. Hodges, J. Kemp, and P. Thompson, "Liberty ID-FF Architecture Overview," T. Wason, Ed. Piscataway. NJ: Liberty Alliance Project, 2003.

[16] S. Woodhouse and P. White, "Identity based Management: Extending the ISMS for Federation," in *ISACA Oceania Computer Audit Control and Security Conference 2007*, Auckland NZ, 2007.

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

[18] P. White, "Identity Management Architecture in the Australian Public Sector," in *5th International Conference on Information Technology and Applications ICITA 2008*, Cairns, QLD. , 2008.

[19] Novell Inc, "Novell Enhanced Provisioning Module for Novell NSure Identity Manager," Provo, UT, USA: Novell Inc, 2006.

[20] Microsoft Corp, "Microsoft Identity and Access Management Series: Fundamental Concepts," Redmond, WA, USA: Microsoft Corp, 2006.

[21] R. Sandhu and P. Samarati, "Access Control: Principles and practice," *IEEE Communications*, vol. 32, pp. 40-48, 1994.