TOWARDS INTEROPERABLE STANDARDIZATION FOR END-TO-END SECURITY IN A GRID SERVICES CONTEXT

Gaolathe Seelo[a] and Maree Pather[b]

[a, b] Nelson Mandela Metropolitan University

[a, b] Faculty of Engineering, Department of Computer Studies, PO Box 77000,
Nelson Mandela Metropolitan University, Port Elizabeth, 6013
[a] gseelo@yahoo.com
[b] maree.pather@nmmu.ac.za

ABSTRACT

The advent of Grid Computing promises users the power to have access to a vast amount of heterogeneous, distributed resources. The envisaged goal is to enable users and applications to seamlessly access these resources to solve complex large-scale problems whether in science, engineering, or commerce. To realize this goal the numerous barriers that normally separate different computing systems within and across organizations must be addressed. This can be achieved through effective standardization. Standardization plays a crucial role in achieving interoperability, portability and reusability of components and systems. The Open Grid Services Infrastructure (OGSI) Specification defines a set of conventions and extensions that contribute to the standardization of Grid Services. Since Grid Services are typically implemented as Web Services, they rely heavily on XML technologies. Thus, the focus of this research is to propose a multilaterally-interoperable Grid Service Framework that is robust and secure, using common XML standards relating to SOAP and Web Services. (After only four months into the research, only an analysis of the problem context is provided).

KEY WORDS

Grid Service, SAML, SOAP, XML Encryption, XML Signatures, WS-Choreography, WS-Addressing, WS-Architecture, WS-Security

TOWARDS INTEROPERABLE STANDARDIZATION FOR END-TO-END SECURITY IN A GRID SERVICES CONTEXT (RESEARCH IN PROGRESS)

1 INTRODUCTION

The advent of Grid Computing promises users the power to have access to a vast amount of heterogeneous, distributed resources (Foster, Kesselman, & Tuecke, 2001; Foster, Kesselman, Nick, & Tuecke, 2002). The envisaged goal is to enable users and applications to seamlessly access these resources to solve complex large-scale problems whether in science, engineering, or commerce (Foster et al., 2001, 2002; Czajkowski, Fitzgerald, Foster, & Kesselman, 2001). To realize this goal, the numerous barriers that normally separate different computing systems within and across organizations must be addressed. This can be achieved through standardization.

Standardization plays a crucial role in the achievement of interoperability, portability and reusability of components and systems. It allows for computers, application services, data, and other resources to be discovered, accessed, allocated and accounted for as and when required, regardless of the location of the resource (Foster et al., 2004). The use of Open Standards can also go a long way in the development of secure, robust, and scalable Grid systems by facilitating the use of platform-independent best practices.

The Open Grid Services Infrastructure (OGSI) specification defines a set of conventions and extensions on the use of Web Service Definition Language (WSDL) and XML Schema to enable stateful Web services. The OGSI specification, released in July 2003 by the OGSI Working Group of the Global Grid Forum, is primarily concerned with creating, addressing, inspecting and managing the lifetime of stateful Grid Services. According to Czajkowski, Ferguson, Foster, et al (2004), Grid Services provide for the controlled management of the distributed and often long-lived state that is commonly required in distributed applications. Grid Services are implemented as Web Services which, in turn, rely on SOAP over HTTP.

The Web Services world has evolved considerably as developments continue to be made on the OGSI specification. The need for new use-patterns and specifications that simplify and clarify the OGSI specification have motivated the proposal for WS-Resource Framework. This was done as a way of refactoring and evolving the OGSI specification. Based on previous implementation and application experiences, the WS-Resource Framework utilizes a set of new Web service standards, while retaining all of the essential functional capabilities present in the OGSI specification (Czajkowski et al., 2004).

The main objective of this research is to propose a framework for multilaterally-interoperable Grid Services that is robust and secure using common standards, such as those for WS-Security, WS-Architecture and WS-Choreography. The focus of this paper is to propose a set of security standards to promote the goal of interoperability, explaining with justification the security architecture that should be used within a proposed Grid Services framework.

To contribute to interoperability objectives, certain standards already exist (Box et al., 2000; Booth et al., 2004; Foster et al., 2002). These standards will be described in the next section.

2 STANDARDS FOR INTEROPERABILITY AND SECURITY

In this section, standards, technologies and paradigms, which help to ensure interoperability and security in Grid Services, are discussed.

2.1 SOAP

SOAP (Medjahed, Benatallah, Bouguettaya, Ngu, Elmagarmid, 2003; Encyclopedia, 2005b; Box, Ehnebuske, Kakivaya, Layman, Mendelsohn, Nielsen, 2000) is a lightweight messaging framework for exchanging XML-formatted data among Web services in a decentralized, distributed environment. The adoption of SOAP as a XML-based messaging protocol facilitates the interaction between heterogeneous systems. A major design goal for SOAP, as indicated in the SOAP Specification (Box et al., 2000), is simplicity and extensibility. SOAP will be used uniformly for interaction between the different users and resources in the proposed Grid Service.

2.2 Web Services

An XML Web service is essentially a programmable entity providing specific functionality, by way of application logic, and is potentially accessible to any number of distributed client-systems. Client-systems can interact with the Web service as prescribed by its (published) interface, using SOAP messages, usually conveyed using HTTP (Booth, Haas, Newcomer, Champion, Ferris, & Orchard, 2004). The fundamental idea behind Web services is to develop software applications as services. This concept is based on technologies which are supported by open industry standards. These standards facilitate interoperability among heterogeneous systems: Since Web services are based on open-standard interfaces, they can communicate even if they are running on different operating systems and are written in different languages. Thus, Web services provide an excellent approach for building distributed applications that must harness resources on diverse systems over a network (Pullen, Brunton, Brutzman, Drake, Hieb, Morse, & Tolk, 2004), such as intended by Grid computing.

Web services utilize the Universal Description Discovery and Integration (UDDI) specification; it provides a platform-independent way of describing services, discovering businesses, and integrating business services (Erl, 2004c; Colgrave, Januszewski, Curbera, Ehnebuske, & Rogers, 2002). The Web Services Description Language (WSDL) is a general purpose XML language for describing the interface, protocol bindings and the deployment details of Web services (Christensen, Curbera, Meredith, & Weerawarana, 2001; Colgrave et al., 2002; Erl, 2004b). Thus, Web services, UDDI, and WSDL are obvious choices for an interoperability framework. Before attempting to relate Web services to Grid Services from the perspective of interoperable security, Web Services Architecture and related Web services standards will be considered briefly.

2.2.1 Web Services Architecture (WSA)

The Web Services Architecture (WSA) provides a conceptual framework and a context for understanding Web services and the Web services relationships. WSA is, therefore, equivalent to “interoperability architecture”; encompassing global elements required to ensure interoperability between Web services components (Booth et al., 2004).

The Web services architecture is based upon the interactions between three primary roles: service provider, service registry, and service requestor. These roles interact using publish, find, and bind operations. The service provider is the business that provides access to the Web service and publishes the service description in a service registry. The service requestor finds the service description in a service registry and uses the information in the description to bind to a service (Brittenham, 2002). This functionality is provided by SOAP, UDDI and WSDL. The following standards (World-Wide Web Consortium specifications) are used to extend the functionality of SOAP within WSA.

2.2.1.1 Web Services Addressing (WS-Addressing)

One of the core parts of WSA is Web Service Addressing (WS-Addressing). WS-Addressing provides transport-neutral mechanisms to address Web services and messages. Specifically, this specification defines XML elements to identify Web services endpoints and to secure end-to-end multiple endpoint identification in messages (BEA, IBM, Microsoft, SAP, & Sun, 2004). This mechanism is essential in a Grid Service context where there many resources comprising many end-points. WS-Addressing defines two constructs: message addressing properties and endpoint references. They standardize the information typically provided by transport protocols and messaging systems in a way that is independent of any particular transport or messaging system (Gudgin & Hadley, 2005; Box et al., 2004). According to Box et al. (2004), both these constructs are designed to be extensible and re-usable so that other specifications can build on and leverage endpoint references and message information headers.

2.2.1.2 WS-Security

WS-Security (Web Services Security also known as the Web Services Security Language) Specification (Atkinson, Della-Libera, Hada, et al, 2002) proposes a standard set of SOAP extensions that can be used when building secure Web services to implement message integrity, message confidentiality, and single message authentication. WS-Security can be used to bridge gaps between disparate security frameworks. It also goes beyond traditional transport-level security to provide a standard end-to-end security framework for SOAP messages (Erl, 2004). WS-Security is flexible and is designed to be used as the basis for the construction of a wide variety of security frameworks. The specification provides three main mechanisms, namely security token propagation, message integrity, and message confidentiality (Atkinson et al., 2002).

2.2.1.3 Web Services Choreography

Web Services Choreography deals with the observable interactions between the Web services and the clients (Austin, Barbir, Peters, & Ross-Talbot, 2004). According to Austin et al., (2004) the main use of a choreography description is to precisely define the sequence of interactions between a set of cooperating Web services in order to facilitate a common means to:

1. promote a common understanding between WS participants;
2. automatically validate conformance;
3. ensure interoperability;
4. increase robustness; and to
5. generate code skeletons.

Global definitions of WS-Choreography facilitate choreography reuse (Burdett & Kavantzas, 2004). A uniform choreography will be required to define how resources will interact within a Grid Service context.

2.2.1.4 XML Encryption

XML Encryption provides end-to-end security for applications that require secure exchange of structured data. As stated by Siddiqui (2002), both encrypted and non-encrypted data can be exchanged within the same document. Another benefit of XML Encryption is that it can handle both XML and non-XML (e.g. binary) data. This is essential as different kinds of data are exchanged in Grid Services, not only XML.

2.2.1.5 XML Digital Signatures

The need exists for message authentication, integrity and non-repudiation in the proposed Grid Service. Digital certificates are a globally-recognized method, which can be used to enable the encryption and digital signing of the exchanged data. XML digital signatures are digital signatures designed for use in XML transactions (Simon, Madsen, & Adams, 2001).

2.2.1.6 SAML

According Hughes & Maler (2004), the Security Assertions Markup Language (SAML) is an XML-based framework that enables Web services to readily exchange information in a single-sign-on (SSO) authentication context. This information takes the form of trusted statements, called security assertions, about end users, Web services, or any other entity that can be assigned a digital identity.

There are three major types of SAML assertions.

- Authentication assertions, such as contained in digital certificates or Kerberos tickets, declare that the identity of a user or a Web service has been authenticated to access protected resources, for example, an intranet or extranet.
- Attribute assertions, generated by an attribute service, verify that a user or Web service possesses certain static attributes (e.g., a user role) or dynamic attributes (such as an account balance). Attribute information can be vital to authorization.
- An authorization service that brings together authentication assertions, attribute assertions and authorization policies, and generates authorization assertions that define which resources a user/service is entitled to access.

SAML shields applications from the complexity of the underlying authentication and authorization systems. SSO is important within the Grid service context as a user is likely to access may resources either directly or indirectly; persisting his/her credentials transparently would be most useful. SAML Requests and Responses are embedded in the body of a SOAP message.

2.3 Grid Computing

Grid computing is described in terms of: parallel distributed systems composed of heterogeneous resources, belonging to different administrative domains over a network using open standards and protocols. Grid computing offers a framework for solving massive computational problems by making use of the unused resources of large numbers of disparate computers. The computers are treated as a virtual cluster embedded in a distributed telecommunications infrastructure (Encyclopedia, 2005a). Because Grid computing solutions use open standards and protocols, they have gained the one thing that is necessary for their success: ubiquity of peer resources (Pullen et al., 2004). The Semantic Grid (http://www.semanticgrid.org/) extends Grid Computing aiming at standardisation of meanings in information and services, thereby promoting interoperability. Another related computing paradigm is the peer-to-peer (P2P) network. Again, a very large number of autonomous computing nodes (the peers) pool together their resources and rely on each other for data and services in a symbiotic-mutualism fashion. Typical examples are the Napster application (Napster.com) in which, instead of storing the songs on a central computer, the songs are stored on users' machines; a central index server was used. Berkley University (http://boinc.berkeley.edu/intro.php) has developed a software platform for distributed computing using volunteered computer resources called Berkley Open Infrastructure for Network Computing (BOINC), which uses a scheduling mechanism. It is hoped that these paradigms will contribute to a versatile hybrid system, underpinned by Grid Services objectives.

2.4 Grid Services

A Grid Service comprises at least one Web service that provides a set of well-defined Open Standards-based interfaces that follow specific conventions. The interfaces are concerned with the discovery, dynamic service creation, lifetime management, inspection, notification, and manageability of the distributed and often long-lived state that is commonly required in distributed applications. (Foster, Kesselman, Nick, & Tuecke, 2002; Czajkowski et al., 2004). Grid services can utilise all the afore-mentioned technologies, standards and paradigms in providing a distributed collaboration platform, harnessing distributed resources in a co-ordinated and interoperable fashion.

3 SECURITY REQUIREMENTS

The most common concern for organizations implementing Web services solutions like the Grid Service, is Security. There is need for an end-to-end security architecture that is straightforward to implement across organizations (Microsoft, 2001). Currently the security standards that are available, like SSL/TLS (Dierks & Allen, 1999), Kerberos (Neuman & Ts'o, 1994) and IPSec (Atkinson & Kent, 1998), provide only point-to-point integrity and confidentiality for a message.

The major challenge facing security on a Grid services platform is overcoming specific differences in security configurations between participants; precisely how will security-interoperability in the Grid be addressed? Simply reconciling differences between two partners in a mutual agreement is obviously inadequate. A comprehensive mechanism – obviating continuous dynamic re-configuration – is essential.

As in standard Web services contexts, SOAP messages may travel through multiple intermediaries before reaching their destination. Current security standards provide protection of the data is only in transit between browser and Web server. Often, data is left unprotected on the server. Encrypting the data itself would help reduce the incidents of unencrypted data left vulnerable on public servers (Simon et al., 2001).

Grid Services represent a convenient and powerful way for organizations to deploy new business services and integrate existing business applications. However, the open and flexible nature of the SOAP framework potentially exposes organizations to security risks. SOAP applications generally rely on HTTPS as the underlying transport security protocol. However, SOAP/HTTP messages are typically allowed to cross domain boundaries (Brose, 2003). Hence, SOAP messages with malicious content can traverse corporate firewalls and evade packet-filtering technologies. Further, SOAP messages, in their basic format, are prone to eavesdropping, being forged, being intercepted, and so forth. Such security risks are not unique to Grid Services; but protecting Grid Services from data exposure and application misuse requires a comprehensive solution that ensures a high-degree of reliability and trust (Xtradyne, 2004).

4 TOWARDS A PROPOSED GRID SERVICE FRAMEWORK

The main objective of this research is to design a multilaterally-interoperable Grid Service that is robust and secure using common Web Service standards. What follows is an exposition of the fundamental ideas for the framework; the actual infrastructural composition and mode of operation is a work-in-progress.

The SOAP message framework operates on logical endpoints that abstract the physical network and application infrastructure. Therefore it frequently incorporates a multi-hop topology with intermediate actors. When data is received and forwarded on by an intermediary beyond the transport layer, any corresponding security information may be lost. This forces any subsequent message processors to rely on the security evaluations made by previous intermediaries and to completely trust their handling of the content of messages (IBM & Microsoft, 2002). A mechanism that therefore provides end-to-end security is needed, especially in a comprehensive Grid Service Security Architecture. The proposed framework will attempt to leverage application layer security mechanisms to provide comprehensive security capabilities. The objectives of the framework are based on those established for the Globus Toolkit (www.globus.org):

Providing authenticated and confidential communication between users and resources in a Grid; providing security across organizational boundaries, thus avoiding a system of centrally-managed security; and providing a "single sign-on" mechanism for users of the Grid, allowing for persistence across elements in the Grid.

The proposed framework will work at the message level to establish an identity for the users and resources of a Grid. It will share security information among numerous intermediaries in the Grid. This is done by attaching security credentials – standard mechanism will be chosen from:

usernames, passwords, public-key certificates, and security tokens - to SOAP messages through the use of SAML. By using this approach, an intermediary can authenticate a message according to the enclosed credentials as well as add new security information to the message. This assists end-to-end security and provides a means to monitor and track the exchange of messages. Since each message contains and disseminates the necessary security information and credentials, the proposed framework can ensure authorized use and message integrity.

XML Digital Signature and XML Encryption will be used to digitally sign and encrypt a message or its component parts, respectively. This prevents eavesdropping and tampering, thus ensuring message confidentiality and integrity. This will also ensure security on a per-message basis (Xtradyne, 2004). XML Encryption can be use to encrypt parts of the data that is being exchanged. The encryption of certain parts of a message is important when confidential information must not be revealed to certain intermediaries when the message is processed. The encryption is done with symmetric encryption after a secret key is generated using asymmetric encryption (Siddiqui, 2002). XML-signatures have a useful feature that enables one to sign selective parts of a message. Thus, different sections of an XML document can be signed by different signatures. This will provide high-level security for the data in the proposed Grid Service Security Framework (Simon et al., 2001).

The proposed Grid Service Security Framework provides end-to-end message security through the WS-Security specification. WS-Security explicitly addresses the requirement of end-to-end message security even in application environments where a message crosses organizational and trust boundaries as is the case with Grid Services. As stated by Brose, (2003) this is technically achieved through the definition of a security header format so that each message can contain all the security about itself that is required for making security decisions. WS Security also provides support for multiple security tokens authentication or authorization, multiple trust domains, multiple signature formats, and multiple encryption technologies.

The WS-Security specification will define processing rules for the proposed framework. These rules will define how XML Digital Signature, XML Encryption, and the Security Assertion Markup Language (SAML) should be used protect parts or all of the SOAP message, and to insert security tokens into the security header (Brose, 2003). WS-Security also provides single-sign on authentication in a Grid Service (Foster, 1998).

The Web Services Choreography facilitates the standardized description of choreographies. According to (Austin et al., 2004) the benefits of the Web Services Choreography are that it:

- will enable more robust Grid Services to be constructed on the framework;
- will enable more effective interoperability of Grid Services through behavioral multi-party contracts, which are choreography descriptions;
- will reduce the cost of implementing Grid Services by ensuring conformance to expected behavior, and;
- will increase the utility of Grid Services as they will be able to be shown to meet contractual behavior.

The proposed framework will thus provide interoperability of Grid Services through existing standards, such as: WS-Addressing, Web Services Choreography and Web Service Architecture.

5 CONCLUSION

This paper focuses on the preliminary work towards the design of a multilaterally-interoperable Grid Service security framework. The focus is on end-to-end message security.

Much research still needs to be conducted in order to formulate a suitable design infrastructure and modus operandi. To date, the available technologies and the pros and cons of available paradigms have been investigated.

REFERENCES

Atkinson, B., Della-Libera, G., Hada, S., Hondo, M., Hallam-Baker, P., Kaler, C., Klein, J., LaMacchia, B., Leach, P., Manferdelli, J., Maruyama, H., Nadalin, A., Nagaratnam, N., Prafullchandra, H., Shewchuk, J., & Simon, D. (2002, April). *Web Services Security (WS-Security)*. (http://www.verisign.com/wss/wss.pdf)

Atkinson, R., & Kent, S. (1998, November). *Security Architecture for the Internet Protocol.* Web. (http://www.ietf.org/rfc/rfc2401.txt)

Austin, D., Barbir, A., Peters, E., & Ross-Talbot, S. (2004, March). *Web Services Choreography Requirements*. Web. (http://www.w3.org/TR/2004/WD-ws-chor-reqs-20040311/)

BEA, IBM, Microsoft, SAP, & Sun. (2004, March). *Web Services Addressing*. Web. (http://www-128.ibm.com/developerworks/library/ws-add/index.html)

Bellwood, T., Clement, L., Ehnebuske, D., Hately, A., Hondo, M., Husband, Y. L., Januszewski, K., Lee, S., McKee, B., & Riegen, J. M. C. von. (2002, July*). UDDI Version 3.0*. Web. (UDDI Spec Technical Committee Specification)

Booth, D., Haas, H., Newcomer, F. M. E., Champion, M., Ferris, C., & Orchard, D. (2004, February). *Web Services Architecture*. Web. (http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/)

Box, D., Christensen, E., Curbera, F., Ferguson, D., Frey, J., Kaler, C., Langworthy, D., Leymann, F., Lovering, B., Lucco, S., Millet, S., Mukhi, N., Nottingham, M., Orchard, D., Shewchuk, J., Storey, T., & Weerawarana, S. (2004, August). *Web Services Addressing (WS-Addressing)*. Web. (http://www.w3.org/Submission/2004/SUBM-ws-addressing-20040810/)

Box, D., Ehnebuske, D., Kakivaya, G., Layman, A., Mendelsohn, N., Nielsen, H. F., Thatte, S., & Winer, D. (2000, May). *Simple Object Access Protocol (SOAP) 1.1*. Web. (http://www.w3.org/TR/2000/NOTE-SOAP-20000508)

Brittenham, P. (2002, June). *An overview of the Web Services Inspection Language.* Web. (http://www-106.ibm.com/developerworks/library/ws-wsilover/index.html)

Brose, G. (2003, May). *Securing Web Services with SOAP Security Proxies.* White Paper. (www.xtradyne.com/documents/whitepapers)

Burdett, D., & Kavantzas, N. (2004, March). *WS Choreography Framework Overview*. Web. (http://www.w3.org/TR/2004/WD-ws-chor-framework-20040324/)

Christensen, E., Curbera, F., Meredith, G., & Weerawarana, S. (2001, March). *Web Services Description Language (WSDL) 1.1*. Web. (http://www.w3.org/TR/2001/NOTE-wsdl-20010315)

Colgrave, J., Januszewski, K., Curbera, F., Ehnebuske, D., & Rogers, D. (2002, November). *Using WSDL in a UDDI Registry, Version 1.08*. Web. (http://www.oasis-open.org/committees/uddi-

spec/doc/bp/uddi-spec-tc-bp-using-wsdl-v108-20021110.htm)

Czajkowski, K., Ferguson, D., Foster, I., Frey, J., Graham, S., Maguire, T., Snelling, D., & Tuecke, S. (2004, January). *From Open Grid Services Infrastructure to WSResource Framework: Refactoring & Evolution*. Whitepaper.

Czajkowski, K., Fitzgerald, S., Foster, I., & Kesselman, C. (2001). *Grid Information Services for Distributed Resource Sharing*. Web.

Dierks, T., & Allen, C. (1999, January). *The Transport Layer Security(TLS Protocol Version 1.0.* Web. (http://www.ietf.org/rfc/rfc2246.txt)

Encyclopedia, W. T. F. (2005a, April). *Grid Computing*. Web.

Encyclopedia, W. T. F. (2005b, April). *SOAP*. Web.

Erl, T. (2004a). An *Overview of the WS-Security Framework*. In (1 ed., Vol. 1, chap. 4).

Erl, T. (2004b). *Defining the Web Service with WSDL*. In (1 ed., Vol. 1, chap. 4).

Erl, T. (2004c). *UDDI In and Out of the Enterprise*. In (1 ed., Vol. 1, chap. 4).

Foster, I., Berry, D., Djaoui, A., Grimshaw, A., Horn, B., Kishimoto, H., Maciel, F., Savva, A., Siebenlist, F., Subramaniam, R., Treadwell, J., & Reich, J. V. (2004, July). *The Open Grid Services Architecture, Version 1.0.*

Foster, I., Kesselman, C., Nick, J., & Tuecke, S. (2002). *The Physiology of The Grid: An Open Grid Services Architecture for Distributed Systems Integration.*

Foster, I., Kesselman, C., & Tuecke, S. (2001). *The Anatomy of the Grid: Enabling Scalable Virtual Organizations*. Lecture Notes in Computer Science, 2150, 1{25.

Foster, I. T., Kesselman, C., Tsudik, G., & Tuecke, S. (1998*). A Security Architecture for Computational Grids*. In ACM conference on computer and communications security (p. 83-92).

Gudgin, M., & Hadley, M. (2005, February). *Web Services Addressing 1.0 - Core*. Web. (http://www.w3.org/TR/2005/WD-ws-addr-core-20050215)

Hughes, J., & Maler, E. (2004, May). *Technical Overview of the OASIS Security Assertion Markup Language (SAML) V1.1*. Web. (http://www.oasis-open.org)

IBM, & Microsoft. (2002, April). Security in a Web Services World: A Proposed Architecture and Roadmap. White Paper. (http://www-106.ibm.com/developerworks/library/ws-secmap/)

Medjahed, B., Benatallah, B., Bouguettaya, A., Ngu, A. H. H., & Elma-garmid, A. K. (2003). *Business-to-Business Interactions: Issues and Enabling Technologies*. The VLDB Journal, 12 (1), 59{85.

Microsoft. (2001, October). *Global XML Web Services Architecture*. White Paper. (http://www.gotdotnet.com/team/XMLwebservices/GlobalServices)

Neuman, B. C., & Ts'o, T. (1994, September). *Kerberos: An Authentication Service for Computer Networks.* IEEE Communications Magazine, 32 (9), 33{38. (http://www.isi.edu/gost/publications/kerberos-neuman-tso.html)

Pullen, J. M., Brunton, R., Brutzman, D., Drake, D., Hieb, M., Morse, K. L., & Tolk, A. (2004). *Using Web Services to Integrate Heterogeneous Simulations in a Grid Environment*. Conference.

Siddiqui, B. (2002, March). *Exploring XML Encryption, Part 1*. Web. (http://www-106.ibm.com/developerworks/xml/library/x-encrypt/)

Simon, E., Madsen, P., & Adams, C. (2001, August). *An Introduction to XML Digital Signatures*. Web. (http://www.xml.com/pub/a/2001/08/08/xmldsig.html)

Xtradyne. (2004, June). *Protecting Web Services with the XML/SOAP Security Gateway*. Whitepaper. (http://www.xtradyne.com/documents/whitepapers)