VeriSign®

White Paper

Security Service Markup Language (S2ML)

XML Trust Services

Contents

Executive Summary

XML (Extensible Markup Language), the flexible data framework that allows applications to communicate on the Internet, has become the preferred infrastructure for e-commerce applications. All of those transactions require trust and security, making it mission-critical to devise common XML mechanisms for authenticating merchants, buyers, and suppliers to each other, and for digitally signing and encrypting XML documents like contracts and payment transactions.

XML Trust Services—a four-component suite of open specifications for application developers developed in partnership with industry leaders including Microsoft, Ariba, webMethods, and Netegrity—makes it easier than ever to integrate a broad range of trust services into B2B and B2C applications. XML complements Public Key Infrastructure (PKI) and digital certificates, the standard method for securing Internet transactions.

B2C and B2B transactions that take place between enterprises across the Internet have had no standard language for communicating authorization data that specifies what transactions or information a buyer, seller, or enterprise is permitted to access. The **S2ML** (Security Services Markup Language) specification developed by VeriSign with Netegrity and other vendors, solves this problem. It offers a vendor-neutral, open XML standard for enabling secure e-commerce transactions by describing authentication, authorization, and profile information, allowing businesses to exchange this data between customers, partners, or suppliers, regardless of the security systems or e-commerce platforms they have in place.

Using standard XML toolkits instead of proprietary third-party software, developers can use S2ML to make trust information completely portable, travelling with XML documents for business transactions across multiple Web sites. In B2C applications, for example, users can sign on to a service and present digital certificates only once, and then travel across linked or affiliated Web sites without having to log on and re-authenticate.

I. Securing E-Commerce Transactions

A. The Challenge of Access Control—Authentication & Authorization

The purpose of establishing controls for online trust and security is to determine who should have access to sensitive, business-critical information. Access control is traditionally broken down into two separate components:

- **Authentication** Who are you?
- **Authorization** What are you allowed to do?

As complex business transactions and e-commerce increasingly take place among different enterprises across different Web sites, exchanges, or portals, the process of

determining which individuals and business entities may access secured information has become more complicated.

In B2C environments, the primary goals of online authentication and authorization are enabling single sign-on and remote authorization, so that users can visit a Web site, authenticate themselves once (ideally, with digital certificates), and then hyperlink to other, related or partner Web sites without having to reauthenticate. Authorization privileges should follow the user from site to site.

In B2B environments, enterprises need to exchange documents required for complex transactions, such as credit reports, requests for proposals, contracts, or financial documents, across multiple Web sites. Authentication and authorization data should travel with the documents regardless of the security systems or transport protocols in place.

Accomplishing these goals has been elusive due to the lack of a single, common language for sharing authorization and authentication information between companies.

Separating access-control into two components allows authentication credentials to be standardized across an entire application domain. However, authorization credentials do not lend themselves to re-use in the same degree. For example, large number of enterprises can agree to authenticate Alice using the same credentials. However, what the enterprise allows Alice to do using the credential will vary from enterprise to enterprise. Her own employer might allow her to view company secrets while other enterprises might allow her to only place orders, subject to an authorization limit that varied from enterprise to enterprise.

The Authorization problem may also be broken down into two separate problems:

- **Policy**—Analyzing data from multiple sources to make an authorization decision
- **Distribution**—Making authorization decisions available to applications

Standardization of Authorization policy is very difficult. There is considerable variation in the policy needs of different applications using the same data. A solution that is comprehensive enough to meet the needs of one application is likely to be far too complex to be implemented in another. Fortunately it is not necessary to standardize policy—as long as authorization decisions are made by centralized services rather than individual application.

B. S2ML: The XML Infrastructure Solution

Security Services Markup Language (S2ML) is a vendor-neutral, open standard for enabling interoperable, secure e-commerce transactions through XML. It provides a common language for the sharing of security services in B2B and B2C e-commerce transactions, allowing companies to securely exchange authentication, authorization, and user profile information among their customers, partners, and suppliers—regardless of the systems or platforms each use. Its supporters include Bowstreet, JamCracker, Netegrity, Sun, VeriSign, and webMethods.

S2ML uses the eXtensible Markup Language (XML), which is firmly established as the *lingua franca* of e-business. Using XML provides S2ML with the foundation for vendor-neutral interoperability. Applications can quickly take advantage of S2ML using standard XML toolkits. The ubiquitous use of XML means that in many cases XML services are available as common operating system facilities. This is particularly the case in restricted devices such as mobile and wireless devices where memory is at a premium.

For B2C environments, S2ML provides standard security tags that identify individual users across multiple Web sites, allowing single sign-on and remote authorization. For B2B environments, enterprises can agree, for example, on a single XML-based invoice payment message format, allowing all documents that conform to the format to be automatically exchanged between the enterprises' systems, complete with authentication and authorization data, regardless of transport protocols. And for enterprises that want to rely on authentication and authorization decisions made remotely by trusted third parties, S2ML can be used as the common security language for hosted services.

1. URIs Express Authorizations

S2ML expresses authorizations using URIs. In the most direct implementation the URI might be a Uniform Resource Locator (URL) the address of a resource to which access was requested:

- Alice attempts to connect to a secure Web page.
- The Web server queries the trust server to find out if Alice is allowed read access.
- The Trust server responds that Alice is permitted access.

URIs may also be used indirectly to represent roles. For example Alice may need access to a large number of servers in the enterprise that contain financial data. Configuring the Trust service with the location of every finance-related Web page in the company would be both tedious and as sites were reorganized would create an administrative nightmare.

In a role-based authorization scheme a group of sites agree on a common name to be used to stand for the right to access pages with financial data with a particular degree of sensitivity. These are the pages Alice needs in her *role* as Finance director.

S2ML allows roles to be encoded using any URI scheme. Uniform Resource Names are particularly suitable however since URNs are explicitly intended to be used to identify abstract resources of this type.

Using role-based authorization allows a Trust Service to serve an entire community. The community might consist of a part of an Enterprise, the Enterprise as a whole or span multiple enterprises.

2. Authorization Webs

E-business applications typically involve multiple levels of authorization in a single transaction. For example when Alice puts in a purchase order for office supplies costing $100, the following authorization services are required:

- The merchant is concerned that payment for the services will be made by the bank, that is that the payment is authorized
- The bank is concerned that the payment order is properly authorized by its customer (the company)
- The company is concerned that Alice is authorized to sign purchase orders and that she has not exceeded either her signing authority or her budget.

S2ML provides a single, coherent message syntax that allows each of the parties to receive the authorization information they require.

3. Assertion-Based Infrastructure

The S2ML architecture is built upon the use of *Trust Assertions*. At its simplest, a trust assertion is a standard format for expressing a statement that is intended to convey trust. Trust assertions extend and generalize the architecture set out in the XML Key Management Specification (XKMS). While traditional Public Key Infrastructures (PKIs) are designed to allow trusted statements to be made about the use of public keys, Trust Assertions allow trusted statements to be made on any subject, including financial transactions and authenticated data in addition to public keys.

Trust Assertions are designed to compliment rather than replace digital certificates. While Trust Assertions may be used to replace an established X.509-based PKI, it is much more interesting to use them to support new applications that X.509 certificates were not designed to address.

4. Service-Based Architecture

S2ML is designed for deployment as a *Trust Service*. A trust service is a particular form of client-server implementation in which communication between the client and server is authenticated in a manner that is designed to allow services to be provided across enterprises as well as internally within an enterprise.

As with the traditional client-server model, complex operations requiring management of significant volumes of data are concentrated. Client implementations are independent of the server complexity. An important benefit of this architecture is that revisions may be made to the service alone. It is not necessary to upgrade every client to provide new functionality.

A critical weakness of the traditional architecture in which each resource makes independent authorization decisions is the lack of global oversight and control. An attacker may evade detection by spreading the attack across many resources, carefully avoiding exceeding the likely detection threshold for any single resource. Concentrating the authorization function in a service enables site wide auditing. Suspicious patterns of behavior may be detected across independent resources and effective remedial action taken.

II. Premium Authorization Services

An exciting example of the use of S2ML is to allow B2B applications a standard and uniform means of access to premium authorization services. Following are several examples

A. Credit Rating

A large number of premium authorization services already exist, providing necessary and useful business related information such as credit ratings, transaction approvals, etc. Connecting to and making use of this data has to date required proprietary interfaces. The international span of Internet commerce further exacerbates this problem. A company in Texas, for example, might require a report on a company based in France.

S2ML meets the needs of both direct providers of authorization services and of aggregators, providing access to data from multiple sources, and possibly providing additional value-added services.

B. Business Exchange Credentials

Diverse forms of Internet business exchanges are changing the way companies do business. Common to all these exchanges is the need for authentication and authorization of many representatives from multiple organizations.

S2ML allows authorization services to be provided across organizational boundaries to meet these needs. The S2ML/XML Trust Services architecture is particularly advantageous in situations where an exchange is sponsored by a trade organization or other mutual interest group that is recognized as an honest broker by all the parties but that may not have the technical expertise to support the service. In such a circumstance, day-to-day maintenance and administration of the service may be outsourced to a specialist provider under the direction of the honest broker.

C. Health Services Data

One of the most significant challenges facing the health care sector is the management of highly confidential patient data. A significant number of health care professionals may need access to patient records to provide care. In certain circumstances, immediate access may be necessary to provide treatment to a patient who is unable to provide consent.

Patient confidentiality is a genuine concern however, both for patients and practitioners. In response to these concerns, many governments (including the U.S.) are instituting stringent requirements for the protection of confidential patient data.

S2ML provides a platform for providing authorization services that meet the demanding needs of handling health services data. Diverse networks of practitioners and other professionals may be supported. Modern medicine frequently requires exchanges of confidential data across organizational and institutional boundaries. A patient may be referred to a hospital for tests, which may in turn outsource analysis to an independent

pathology lab. S2ML allows authorization services to be provided that track data, allowing access to be controlled as it is passed from one provider to another.

III. Enterprise Infrastructure

In addition to meeting the authorization needs of applications that span enterprises, S2ML is equally applicable as an Intranet solution.

S2ML provides a single point of configuration, integrating ERP solutions from multiple vendors in single sign on solution

S2ML also supports sophisticated requirements. Traditionally authorization schemes have followed a hierarchical scheme in which each user is granted specific static access rights according to their position within the organization. These schemes fail to meet the needs of organizations whose authorization needs are dynamic.

Businesses that manage confidential client information frequently need to restrict access according to dynamic criteria. Access to confidential data belonging to one company may automatically deny access to data belonging to a competitor.

Concentrating authorization policy management through a Trust Service allows dynamic authorization models to be implemented cleanly and reliably.

IV. Outsource or Insource?

Enterprises considering the question of whether or not to outsource authorization services to VeriSign should consider the following points:

- VeriSign has pioneered the deployment of outsourced trust services.
- Outsourcing reduces costs allowing infrastructure development and administration costs to be amortized over many deployments.
- Outsourcing allows enterprises to rapidly take advantage of new technology, while avoiding lock-in.
- Outsourcing meets the needs of trade associations, etc. where the joint entity typically has minimal staff and limited IT support.
- S2ML technology is neutral, supporting both service models or a mixture of the two.

V. References

[SOAP] D. Box, D Ehnebuske, G. Kakivaya, A. Layman, N. Mendelsohn, H. Frystyk Nielsen, S Thatte, D. Winer. *Simple Object Access Protocol (SOAP) 1.1*, W3C Note 08 May 2000, http://www.w3.org/TR/SOAP

[WDSL] E. Christensen, F. Curbera, G. Meredith, S. Weerawarana, *Web Services Description Language (WSDL) 1.0* September 25, 2000, http://msdn.microsoft.com/xml/general/wsdl.asp

[XML] T. Bray, J. Paoli, C. M. Sperberg-McQueen, E Maler, *Extensible Markup Language (XML) 1.0 (Second Edition)*, W3C Recommendation 6 October 2000, http://www.w3.org/TR/REC-xml

[XML-DIGSIG] D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. *XML-Signature Syntax and Processing*, World Wide Web Consortium. http://www.w3.org/TR/xmldsig-core/

[XML-Schema1] H. S. Thompson, D. Beech, M. Maloney, N. Mendelsohn. *XML Schema Part 1: Structures*, W3C Working Draft 22 September 2000, http://www.w3.org/TR/xmlschema-1/

[XML-Schema2] P. V. Biron, A. Malhotra, *XML Schema Part 2: Datatypes*; W3C Working Draft 22 September 2000, http://www.w3.org/TR/xmlschema-2/

[X-TASS] P. Hallam-Baker, *XML Trust Assertion Service Specification*, To be published.

VI. For More Information

For more information about S2ML, go to http://www.s2ml.org.

To learn more about VeriSign's XML Trust Services, see http://www.verisign.com/developer/xml/index.html

VERISIGN, INC.
1350 CHARLESTON ROAD
MOUNTAIN VIEW, CALIFORNIA 9404
WWW.VERISIGN.COM