Identities for Sequenced Web Services

Extensible Markup Language (XML) Web services deployments present unique challenges that emerge when creating an application system based on independently developed, reusable segments of business logic. Although initial adoption of Web services often begins with simple point-to-point integration of different applications, successful deployment rapidly moves enterprises to deploy reusable business logic where transaction processing involves multiple Web services.

One of the most significant challenges presented by these multiple-hop Web services sequences is that of dealing with identity and trust: how to verifiably establish confidence in both the identity of a transaction initiator and the identity of the application code that processes the business data. In addition, federated user identities need to be meaningfully integrated into Web services to tie business transactions to the users who initiate them through a browser or portal interface.

Enterprises experienced in deploying Web services commonly identify the following needs:

- The need to increase confidence in the handling of business transactions within an application system deployed with Web services
- The need for more comprehensive audit trails for processing transactions through multiple tiers of an IT infrastructure
- The need to correlate identities across many applications to detect and remedy instances of identity theft, particularly as applied to phishing attacks

The entity that initiates a transaction in a Web service may be a user at a browser or an automated application such as an order-entry process triggered when a stock level drops below a threshold value. To account for both human and nonhuman initiators of transactions, this document uses the term principal to describe the identity of the entity that initiates a transaction.

Cisco®, in concert with enterprises experienced in large-scale deployment of Web services, has developed a reference architecture, described in this document, to address the problems of trust, identity, and auditing central to these needs.

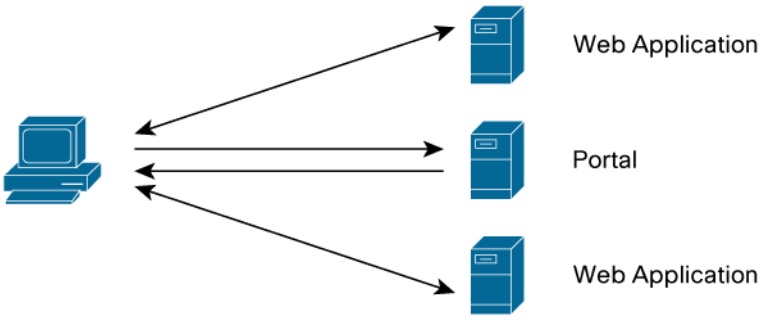
The Changing World of Web Deployments

Over the past 10 years, the model for user access to enterprise systems has been based on browsers and Web portals. Complex interactions relying on access to multiple systems used redirection to additional Web servers (Figure 1). Web single-sign-on solutions were implemented to reduce the need to reauthenticate to multiple Web servers.

Security has generally been provided using server-side Secure Sockets Layer (SSL) Protocol, with user authentication based on usernames and passwords. The applications that provided access to business resources were fairly monolithic and were protected using network security products and access control mechanisms or (in larger organizations) entitlement systems.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 1. Browser Redirection



LIBERTY ALLIANCE, OASIS SAML VERSION 2 AND FEDERATED IDENTITIES

Liberty Alliance has produced specifications dealing with federated identities and Web services. Federated identity access has been primarily motivated by the need for cross-domain Web single sign-on, federation of identities across multiple trust domains, and user session management.

Profiles for the use of SAML in support of federation have been successfully deployed by many vendors of Liberty Alliance–compliant products and customers. The concepts from the Liberty Alliance Federation Framework have been integrated into the latest set of standards from the Security Services Technical Committee in the Organization for the Advancement of Structured Information Standards (OASIS) in SAML Version 2 (SAMLv2).

Liberty Alliance and SAMLv2 call out concepts supporting federated identities including the following:

- Identity provider (IdP): Responsible for identity information about principals on behalf of service providers
- Service provider (SP): Responsible for hosting Web services; they rely on IdPs
- Authentication authority: An authoritative source of SAML authentication assertions

The relatively simple browser security model had to work within the constraints dictated by unsophisticated browsers and HTTP. Initiatives such as Security Assertion Markup Language (SAML) and Liberty Alliance addressed issues such as transparent cross-domain single sign-on and session control. However, other aspects of the user experience, such as interfaces to shopping carts and checkout and payment systems and navigation among products provided by financial institutions, remain inconsistent and unique to each service provider.

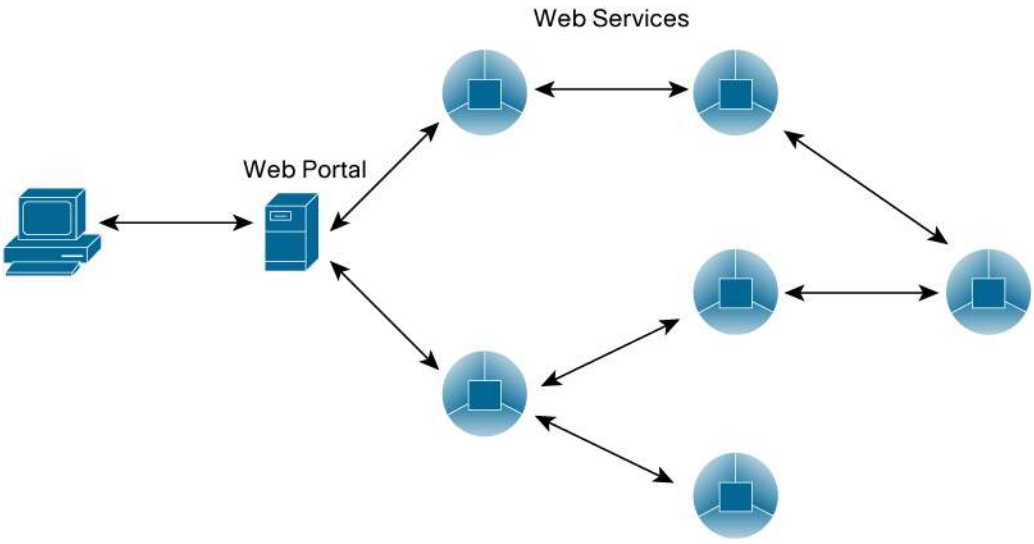
In this browser or portal model, the security equation is straightforward. The identities of the two end points are required (user and service provider), and security rules are applied to those identities to determine access control.

Enterprise IT architectures are moving toward a service-oriented architecture (SOA) based on Web services. Typically, adoption of this approach begins by addressing integration of existing monolithic applications by retrofitting Web service interfaces and interconnections on a point-to-point basis. Applications are then progressively disaggregated into reusable segments of business logic. Applications are constructed by forwarding transactions through multiple hops associated with the Web services that expose this business logic. User interfaces providing authentication, navigation, and presentation will continue to be based on browser interfaces and interactions with portals.

The challenge is how to integrate a Web services infrastructure and the federated identity solutions already deployed at Web portals and service providers (Figure 2).

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 2. Browsers, Portals, and Web Services



SECURING SOAP MESSAGES WITH THE WEB SERVICES SECURITY STANDARD

The Web Services Security (WS-Security) standard is provided by the Web Security Services Technical Committee (WSTC) of OASIS. It builds on other core specifications including the XML Signature and XML Encryption specifications from the World Wide Web Consortium (W3C).

It has three major functions:

- Provide SOAP message integrity, including multiple and overlapping signatures
- Provide SOAP message privacy, including encryption of messages that support Web service intermediaries
- Define how identity information in the form of WS-Security tokens is carried and used to secure a SOAP message

A series of profiles describe how identity information including X.509 certificates and SAML assertions are used in a SOAP message protected using WS-Security.

Web services deployments raise identification issues that need to be addressed with different techniques. For simple point-to-point connections between Web service peers, server-side SSL and a username and password are usually sufficient authentication mechanisms. In more complex environments, where multiple services are involved, service reuse is expected, or multiple Simple Object Access Protocol (SOAP) intermediaries may participate in processing a transaction, simple mechanisms such as SSL are not sufficient.

The Web Services Security Standard

The WS-Security standard was designed to support security in progressively more complex Web service deployments. It defines standard mechanisms for describing security information, including identities carried in a SOAP message. All the information necessary to identify and secure a message is carried with the message.

When dealing with Web services, unlike with the browser and portal model, knowing the identities of the communicating peers is a necessary but not sufficient condition for establishing a secure and trusted environment.

Well-structured and partitioned Web services should be reusable by many peers. Over time, this reuse leads to conditions where a transaction passed between two Web services may have originated several processing hops away. You cannot tell from the identity of the peer that passes you a message whether the message itself is trustworthy. The message may have been generated as part of a transaction that now originates outside of your enterprise by a user belonging to a different trust domain. Similarly, the final destination of a response cannot be determined from the identity of the peer that passed you the original request.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

The identity and context of the principal that originated the request must be maintained and is at least as important as the identity of the communicating peers. Confidence in both sets of identities must be established where a transaction has high value, privacy, or regulatory requirements. Passing a message with a valid identity to a Web service that is not trusted is just as problematic as passing an untrusted message between trusted peers.

AUTHENTICATION CONTEXT

To evaluate the trust that should be placed in an identity, a relying party such as a service provider or Web service may need information about the context of an identity. Identity context information required for trust evaluation purposes can take many forms. Some of the multiple dimensions include the following:

- Initial user identification or registration mechanisms (for example, face-to-face or online registration)
- Lifecycle management handling of credentials (for example, key generation and renewal)
- Credential storage mechanisms (for example, smart cards and software stores)
- Authentication methods (for example, two-factor authentication)

Liberty Alliance and OASIS Security Services Technical Committee (SSTC) have described a set of standard elements describing an authentication context.

The Web Services Identity Model

The goals of this reference architecture include the following:

- Providing a verifiable identity that describes both the originator of a transaction and the Web services peers that forward a SOAP message
- Integration of identities generated with the user- or browser-oriented identity systems based on Liberty Alliance and SAMLv2
- Deployment of a system that allows performance and scaling to large numbers of Web services and high volumes of transactions

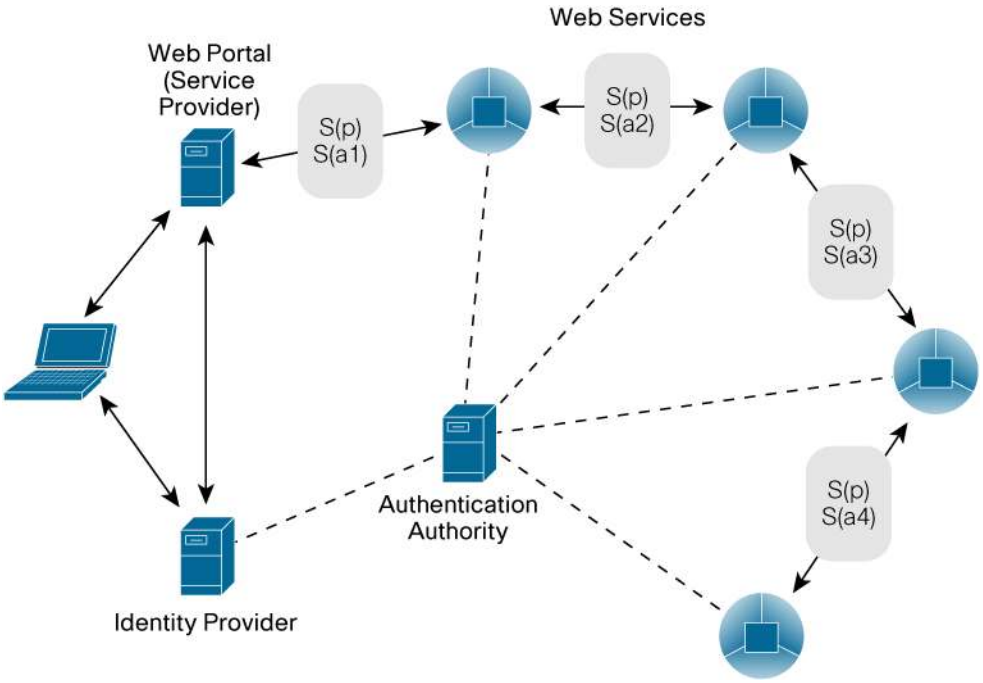
SAML Assertions

In this identity model (Figure 3), a user or nonhuman principal (p) originating a transaction is identified using a SAML assertion S(p) composed of authentication and attribute statements describing the identity and context of the principal. In addition, each application component or Web service (a) is identified using a specific SAML assertion S(a).

Any conformant SOAP message will contain a WS-Security header with at least two SAML assertions S(p) and S(a1). In the case of requests, S(p) identifies the originator of the transaction, and S(a) identifies the peer Web service (possibly an intermediate processing node) that is forwarding the request. Responses will provide an S(a) assertion describing the peer Web service forwarding the response, and S(p) will identify the original transaction requestor for whom the response is ultimately intended.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 3. The Basic Identity Model



User sign-on is performed by portals in conjunction with directories and other identity and access management servers.

Identity federation and single-sign-on functions are performed according to the Liberty Alliance or OASIS SAMLv2 specifications. In Figure 3, an identity provider creates a SAML assertion for the browser user. When the user accesses a Web portal, the SAML assertion is obtained from the user's client or Web browser (directly or by reference). This assertion is used to create the SAML token S(p) used in the WS-Security header of SOAP messages originating at the service provider or portal. S(p) identifies the principal originating the message.

Service providers and other Web service elements need to be explicitly identified and request SAML tokens from an authentication authority. The interface and protocol providing the most flexibility and security here is WS-Trust, which provides a consistent WS-Security token issuance service across multiple authentication and credential issuance infrastructures. Because WS-Trust is still being specified and adopted, the SAML assertion may be obtained from a SAML authentication authority using the SAML request and response protocol; however, some work may be required to transform the SAML assertion to a WS-Security–compliant SAML token. The token S(a) identifies the Web service application component sending a SOAP message.

Identity Trail

In many systems that require a detailed audit trail, it is often difficult to be sure that the identity of a user originating a transaction is maintained throughout all processing steps and logged in a consistent fashion at all points throughout the system. This identity model provides a consistent approach to maintaining the identity of the requesting principal.

In cases where an audit trail is required, a sequence of SAML assertions S(a1) to S(an) can be maintained to identify the processing nodes through which a transaction has passed.

In addition, an audit trail describing the sequence of processing nodes through which a message has passed is required to validate the operations and transformations that were applied to a

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

transaction. This audit trail could be maintained as a stack within the message, provided that mechanisms are applied to help ensure that this record is not altered. A more useful option is to use a trusted authority that logs the interactions within the set of Web services that comprise a distributed application.

Information Privacy

Where information privacy is a requirement of a transaction, additional mechanisms such as public key–based encryption can be used. If more sophisticated control over the final disposition of information is required (to control operations such as copying or printing), additional attributes supporting rights management can be required.

Practical Implementation Issues

Implementing trusted identities requires significant expertise in the use of underlying technologies such as SAML and knowledge of how to integrate with the various supporting identity and access management (IAM) infrastructures.

The creation and validation of SAML tokens requires considerable overhead in several areas. The cryptographic processing needed to generate and validate signatures generally relies on public key technologies, a fairly costly set of operations, particularly when combined with the canonicalization processing associated with XML Signature generation. Potentially more expensive are the latencies associated with the request and response protocols used to obtain SAML tokens or assertions and the processing overhead of the IAM systems that support their generation.

The large numbers of SAML assertions used to deploy this model raise potential concerns about the overhead of the cryptographic operations to make this scheme operate at acceptable performance levels. A number of optimizations are available when deploying this model, including control over validity periods, offloading of high-overhead operations such as cryptographic processing, and caching of results for reuse.

Validity Periods

Actual values for the validity periods established for the SAML assertions are determined by enterprise security policy. However, the authentication assertion for a principal such as a user will usually have a fairly short validity period, and reissuance of the token based on reauthentication that is in turn based on the principal user credential is often desirable. Stable components such as Web services operated in a secure network support tokens with longer validity periods and may be able to reuse tokens when forwarding many requests. In general, the validity of S(p) will be on the order of several minutes, whereas for S(a) it will be on the order of hours.

Provided that there is a way to monitor the effects of changes on the operation of the Web services application, the validity period of the SAML tokens may be tuned based on the safety and sensitivity of the principals and service components used.

System Optimizations

A variety of implementation choices are available to address the application challenges that a loosely coupled Web services infrastructure raises, including platforms, toolkits, agents, and gateways.

Platform-based implementations using toolkits or agents have significant disadvantages for organizations trying to visualize and manage an application system developed with Web services. In particular, it is difficult to provide a view into the operation of the system as a whole or to provide

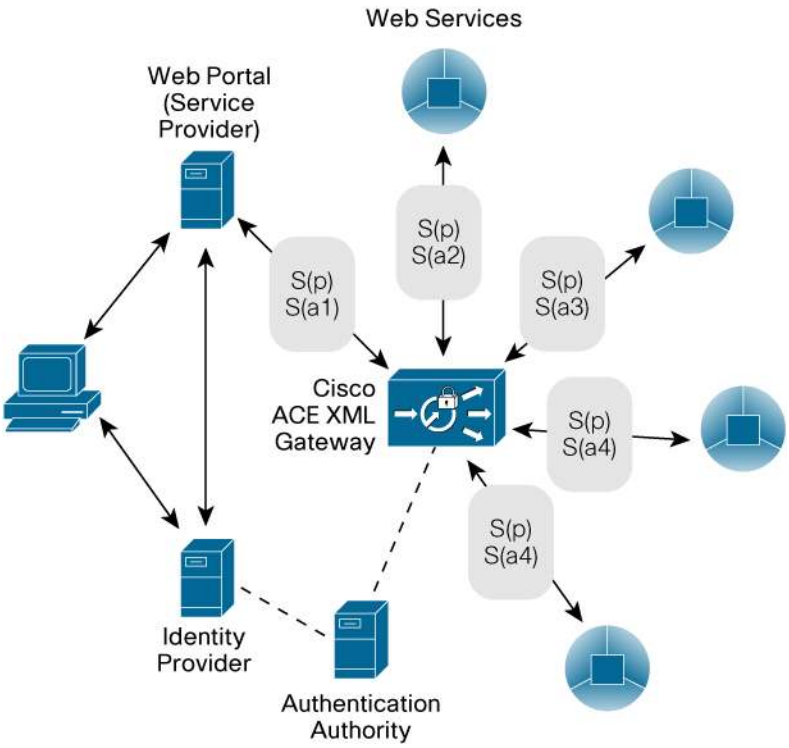
All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

information caches optimized for the system. As a result, systemwide performance optimizations are extremely difficult to achieve.

Cisco ACE Application Control Engine XML Gateways can be used to filter, monitor, transform, and audit transaction streams as they pass between Web service elements (Figure 4). The gateway is an effective location for integration with the existing IAM infrastructures that support single sign-on and federated identities. Capabilities including identity validation, privacy, and integrity enforcement and data transformation and mediation can be optimized by applying appropriate techniques at the gateway. The results of these expensive operations can often be cached and reused, resulting in major systemwide performance enhancements.

For example, the results of a validation operation performed on a given SAML token can be cached and reused. This capability allows quick comparisons and validation against previously seen SAML tokens without the need to rerun cryptographic validation techniques for each token.

Figure 4. Placement of XML Infrastructure Gateways



A systemwide cache where all results of validation operations are stored in a Cisco ACE XML Gateway enables significant use and reuse of SAML tokens across many different Web services and transactions. Fast compare operations are possible based on this cached data, dramatically reducing the number of cryptographic operations required.

Conclusion

Sequenced or multiple-hop Web services require special techniques to address problems that arise from their flexibility, reuse, and distributed control properties. The identity model architecture describes how to implement suitable identity information to secure progressively sophisticated Web service deployments in an optimal fashion, helping ensure confidence in the processing of business transactions and delivering detailed audit trails. In addition, the architecture integrates user identities implemented in a federated identity system to link the browser and Web services.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Identification mechanisms that provide suitable levels of trust for both the messages, and processing nodes within this framework require expanded use of existing infrastructures. Multiple identities are required to establish sufficient levels of trust and to provide an audit trail of operations and transformations.

SAML authentication assertions support these requirements and provide a suitable crossover between the user and browser and Web services. However, to practically support such a solution, the systemwide caching and optimization of signatures and cryptographic processing described here required.

References

Liberty Alliance Project: https://www.projectliberty.org/

- Federated identity framework specifications

OASIS: http://www.oasis-open.org/

- Security Services Technical Committee (SSTC) SAML specification
- Web Services Security Technical Committee (WSTC) WS-Security specification

W3C: http://w3c.org/

- XML Signature and Encryption specifications

WS-Trust: ftp://www6.software.ibm.com/software/developer/library/ws-trust.pdf

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IPTV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Printed in USA

C11-410329-00 5/07

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.