OASIS SECURITY SERVICES TECHNICAL COMMITTEE

SECURITY ASSERTIONS MARKUP LANGUAGE

ISSUES LIST

VERSION 4

JUNE 21, 2001

Hal Lockhart, Editor

Purpose

This document catalogs issues for the Security Assertions Markup Language (SAML) developed the Oasis Security Services Technical Committee.

Introduction

The issues list presented here documents issues brought up in response to draft documents as well as other issues mentioned on the security-use and security mailing lists, in conference calls, and in other venues.

Each issue is formatted according to the proposal of David Orchard to the general committee:

ISSUE:[Document/Section Abbreviation-Issue Number: Short name] Issue long description. Possible resolutions, with optional editor resolution Decision

The issues are informally grouped according to general areas of concern. For this document, the "Issue Number" is given as "#-##", where the first number is the number of the issue group.

Issues on this list were initially captured from meetings of the Use Cases subcommittee or from the security-use mailing list. They were refined to a voteable form by issue champions within the subcommittee, reviewed for clarity, and then voted on by the subcommittee. To achieve a higher level of consensus, each issue required a 75% super-majority of votes to be resolved. Here, the 75% number is of votes counted; abstentions or failure to vote by a subcommittee member did not affect the percentage.

At the second face-to-face meeting it was agreed to close all open issues relating to Use Cases and requirements accepting the findings of the sub committee, with the exception of issues that were specifically selected to remain open. This has been interpreted to mean that:

- Issues that received a consensus vote by the committee were settled as indicated.
- Issues that did not achieve consensus were settled by selecting the “do not add” option.

To make reading this document easier, the following convention has been adopted for shading sections in various colors.

Gray is used to indicate issues that were previously closed.

Blue is used to indicate issues that have just been closed in the most recent revision

Yellow is used to indicated issues which have recently been created or modified or are actively being debated.

Other open issues are not marked, i.e. left white.

Use Case Issues

Group 0: Document Format & Strategy

CLOSED ISSUE:[UC-0-01:MergeUseCases]

There are several use case scenarios in the Straw Man 1 that overlap in purpose. For example, there are several single sign-on scenarios. Should these be merged into a single use case, or should the multiplicity of scenarios be preserved?

Possible Resolutions:

1. Merge similar use case scenarios into a few high-level use cases, illustrated with UML use case diagrams. Preserve the detailed use case scenarios, illustrated with UML interaction diagrams. This allows casual readers to grasp quickly the scope of SAML, while keeping details of expected use of SAML in the document for other subcommittees to use.
2. Merge similar use case scenarios, leave out detailed scenarios.

Status: Closed, resolution 2 carries.

CLOSED ISSUE:[UC-0-02:Terminology]

Several subcommittee members have found the current document, and particularly the use case scenario diagrams, confusing in that they use either domain-specific terminology (e.g., "Web User", "Buyer") or vague, undefined terms (e.g., "Security Service.").

One proposal is to replace all such terms with a standard actor naming scheme, suggested by Hal Lockhart and adapted by Bob Morgan, as follows:

1. User
2. Authn Authority
3. Authz Authority
4. Policy Decision Point (PDP)
5. Policy Enforcement Point (PEP)

A counter-argument is that abstraction at this level is the point of design and not of requirements analysis. In particular, the real-world naming of actors in use cases makes for a more concrete goal for other subcommittees to measure against.

Another proposal is, for each use case scenario, to add a section that maps the players in the scenario to one or more of the actors called out above.

Possible Resolutions:

1. Replace domain-specific or vague terms with standard vocabulary above.
2. Map domain-specific or vague terms to standard vocabulary above for each use-case and scenario.
3. Don't make global changes based on this issue.

Status: Closed, resolution 3 carries

CLOSED ISSUE:[UC-0-03:Arrows]

Another problem brought up is that the use case scenarios have messages (arrow) between actors, but not much detail about the actual payload of the arrows. Although this document is intended for a high level of analysis, it has been suggested that more definite data flow in the interaction diagrams would make them clearer.

UC-1-08:AuthZAttrs, UC-1-09:AuthZDecisions, and UC-1-11:AuthNEvents all address this question to some degree, but this issue is added to state for a general editorial principle for the document.

Possible Resolutions:

1. Edit interaction diagrams to give more fine-grained detail and exact payloads of each message between players.
2. Don't make global changes based on this issue.

Status: Closed, resolution 2 carries.

Group 1: Single Sign-on Push and Pull Variations

CLOSED ISSUE:[UC-1-01:Shibboleth]

The Shibboleth security system for Internet 2 (http://middleware.internet2.edu/shibboleth/index.shtml) is closely related to the SAML effort. An attempt has been made to address the requirements and design of Shibboleth in the SAML requirements document to allow implementation of SAML to be part of, or at least interoperable with, Shibboleth implementations.

In particular, the following issues have been introduced to address Shibboleth requirements:

- UC-1-04:ARundgrenPush
- UC-1-06:Anonymity
- UC-1-07:Pseudonymity
- UC-1-10:UntrustedPartners
- UC-4-04:SecurityDiscovery
- UC-9-03:PrivacyStatement
- UC-9-04:RuntimePrivacy

If these issues, along with the straw man 2 document, have addressed the requirements of Shibboleth, then the subcommittee can address each issue on its own, rather than Shibboleth as a monolithic problem.

Possible Resolutions:

1. The above list of issues, combined with the straw man 2 document, address the requirements of Shibboleth, and no further investigation of Shibboleth is necessary.
2. Additional investigation of Shibboleth requirements are needed.

Status: Closed per F2F #2, Resolution 1 Carries

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18

Resolution 1	6
Resolution 2	0
Abstain	3

CLOSED ISSUE:[UC-1-02:ThirdParty]

Use case scenario 3 (single sign-on, third party) describes a scenario in which a Web user logs in to a particular 3rd-party security provider which returns an authentication reference that can be used to access multiple destination Web sites. Is this different than Use case scenario 1 (single sign-on, pull model)? If not, should it be removed from the use case and requirements document?

As written, the use case is not truly different from use case scenario 1. However, if the use case scenario is expanded to include multiple destination sites, the importance of this use case becomes more apparent.

The following edition to the single sign-on, third party use case scenario would be added:

In this single sign-on scenario, a third-party security service provides authentication assertions for the user. Multiple destination sites can use the same authentication assertions to authenticate the Web user. Note that the first interaction, between the security service and the first destination site, uses the pull model as described above. The second interaction uses the push model. Either of the interactions could use a different single sign-on model.

{PRIVATE "TYPE=PICT;ALT=Single Sign-on, Third-Party Security
Service"}

Fig. X. Single Sign-on, Third-Party Security Service

Steps:

1. Web user authenticates with security service.
2. Security service returns SAML authentication reference to Web user.
3. Web user requests resource from first destination Web site, providing authentication reference.
4. First destination Web site requests authentication document from security service, passing the Web user's authentication reference.
5. Security service provides authentication document to first destination Web site.
6. First destination Web site provides resource to Web user.
7. Web user requests link to second destination Web site from first destination Web site.
8. First destination Web site requests access authorization from second destination Web site,

providing third-party security service authentication document for user.

9. Second destination Web site provides access authorization. 10. First destination Web site provides authorization reference to Web user.
10. Web user requests resource from second destination Web site, providing authorization reference.
11. Second destination Web site provides resource.

Possible Resolutions:

1. Edit the current third-party use case scenario to feature passing a third-party authentication assertion from one destination site to another.
2. Remove the third-party use case scenario entirely.

Status: Closed per F2F #2, Resolution 1 Carries

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	7
Resolution 2	2
Abstain	0

CLOSED ISSUE:[UC-1-03:ThirdPartyDoable]

Questions have arisen whether use case scenario 3 is doable with current Web browser technology. An alternative is using a Microsoft Passport-like architecture or scenario.

It seems that at least one possible solution for the third-party security system exists -- that each destination site pass the authentication assertion from the third party security service to the next destination site, just as in peer source and destination scenarios such as use case scenarios 1 and 2.

Therefore, it seems that the scenario is at least theoretically implementable. It will be up to the other subcommittees and implementors of the standard to decide on how to define that implementation.

Possible Resolutions:

1. The use case scenario should be removed because it is unimplementable.
2. The use case scenario is implementable, and whether it should stay in the document or not should be decided based on other factors.

Status: Closed per F2F #2, Resolution 2 Carries

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	2
Resolution 2	8
Abstain	0

Bob Blakley noted, "I think the proposed implementation only works if you follow direct links, and not if you pick destinations from a history list, use bookmarks, etc..."

CLOSED ISSUE:[UC-1-04:ARundgrenPush]

Anders Rundgren has proposed on security-use an alternative to use case scenario 2 (single sign-on, push model). The particular variation is that the source Web site requests an authorization profile for a resource (e.g., the credentials necessary to access the resource) before requesting access.

{PRIVATE "TYPE=PICT;ALT=Single Sign-on, Alternative Push
Model"}

Fig X. Single Sign-on, Alternative Push Model.

Possible Resolutions:

1. Use this variation to replace scenario 2 in the use case document.
2. Add this variation as an additional scenario in the use case document.
3. Do not add this use case scenario to the use case document.

Status: Closed per F2F #2 3 carries

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18

Resolution 1	0
Resolution 2	3
Resolution 3	6
Abstain	0

Bob Blakley noted, "I can't really see how to do this without significant changes to the current link resolution architecture of web sites -- specifically without making sure both source and destination are expecting to have to handle this flow."

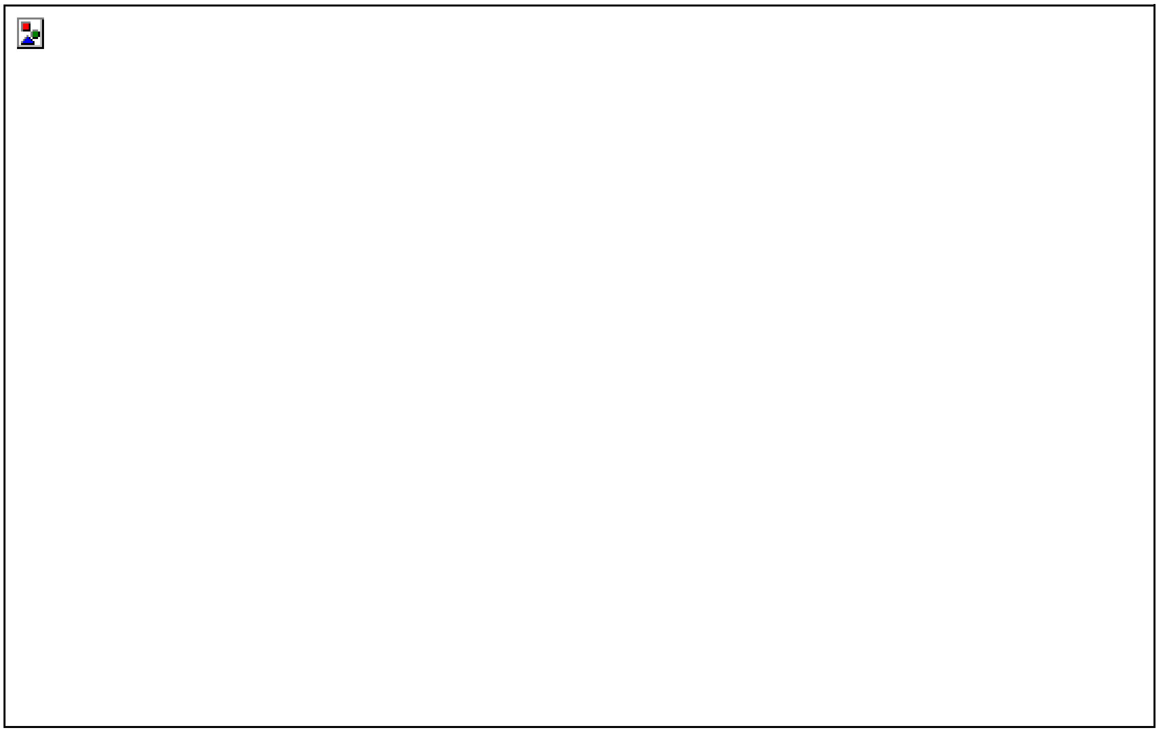
ISSUE:[UC-1-05:FirstContact]

A variation on the single sign on use case that has been proposed is one where the Web user goes directly to the destination Web site without authenticating with a definitive authority first.

A single sign-on use case scenario would be added as follows:

In this single sign-on scenario, the user does not first authenticate with their home security domain. Instead, they go directly to the destination Web site, first. The destination site must then redirect the user to a site they can authenticate at. The situation then continues as if in a single sign-on, push model scenario.

{PRIVATE "TYPE=PICT;ALT=Single Sign-on, Alternative Push
Model"}



Single Sign-on, Alternative Push Model

Steps:

1. Web user requests resource from destination Web site.
2. Destination Web site determines that the Web user is unauthenticated. It chooses the appropriate home domain for that user (deployment dependent), and redirects the Web user to that source Web site.
3. Web user authenticates with source Web site.
4. Source Web site provides user with authentication reference (AKA "name assertion reference"), and redirects user to destination Web site.
5. Web user requests destination Web site resource, providing authentication reference.
6. Destination Web site requests authentication document ("name assertion") from source Web site, passing authentication reference.
7. Source Web site returns authentication document.
8. Destination Web site provides resource to Web user.

Possible Resolutions:

1. Add this use case scenario to the use case document.

2. Do not add this use case scenario to the use case document.

Status: Voted, No conclusion

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	6
Resolution 2	3
Abstain	0

Bob Blakley said, " I agree that servers will have to do this, but it can easily be done by writing HTML with no requirement for us to provide anything in our specification."

CLOSED ISSUE:[UC-1-06:Anonymity]

What part does anonymity play in SAML conversations? Can assertions be for anonymous parties? Here, "anonymous" means that an assertion about a principal does not include an attribute uniquely identifying the principal (ex: user name, distinguished name, etc.).

A requirement for anonymity would state:

> [CR-1-06-Anonymity] SAML will allow assertions to be made about anonymous principals, where "anonymous" means that an assertion about a principal does not include an attribute uniquely identifying the principal (ex: user name, distinguished name, etc.).

Possible Resolutions:

1. Add this requirement to the use case and requirement document.

2. Do not add this requirement.

Status: Closed per F2F #2, Resolution 1 Carries

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18

Resolution 1	9
Resolution 2	0
Abstain	0

CLOSED ISSUE:[UC-1-07:Pseudonymity]

What part do pseudonyms play in SAML conversations? Can assertions be made about principals using pseudonyms? Here, a pseudonym is an attribute in an assertion that identifies the principal, but is not the identifier used in the principal's home domain.

A requirement for pseudonymity would state:

> [CR-1-07-Pseudonymity] SAML will allow assertions to be made about principals using pseudonyms for identifiers.

Possible Resolutions:

1. Add this requirement to the use case and requirement document.
2. Do not add this requirement.

Status: Closed per F2F #2, Resolution 1 Carries

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	7
Resolution 2	2
Abstain	0

In support of Resolution 1, while voting, Bob Blakley said, "I'm really ambivalent about this. At an implementation level AND at a specification level, I can't see how a pseudonym should differ from a 'real' name. If it shouldn't, then we have no work to do. However, we should at least discuss the issue."

CLOSED ISSUE:[UC-1-08:AuthZAttrs]

It's been pointed out that the concept of an "authentication document" used in the use case and requirements document does not clearly specify the inclusion of authz attributes. Here, authz attributes are attributes of a principal that are used to make authz decisions, e.g. an identifier, or group or role membership.

Since authz attributes are important and are required by [R-AuthZ], it has been suggested that the single sign-on use case scenarios specify when authz assertions are passed between actors.

Possible Resolutions:

1. Edit the use case scenarios to specify passing authz attributes with authentication documents.
2. Do not specify the passing of authz attributes in the use case scenarios.

Status: Closed per F2F #2, Resolution 1 Carries

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	9
Resolution 2	0
Abstain	0

CLOSED ISSUE:[UC-1-09:AuthZDecisions]

The current use case and requirements document mentions "Access Authorization" and "Access Authorization References." In particular, this data is a record of a authorization decision made about a particular principal performing a particular action on a particular resource.

It would be more clear to label this data as "AuthZ Decision Documents" to differentiate from other AuthZ data, such as AuthZ attributes or AuthZ policy. To this point, the mentions of "access authorization" would be changed, and a new requirement would be added as follows:

> [CR-1-09-AuthZDecision] SAML should define a data format for recording authorization decisions.

Possible Resolutions:

1. Edit the use case scenarios to use the term "authz decision" and add the [CR-1-09-AuthZDecision] requirement.

2. Do not make these changes.

Status: Closed per F2F #2, Resolution 1 Carries

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	8
Resolution 2	0
Abstain	1

CLOSED ISSUE:[UC-1-10:UnknownParty]

The current straw man 2 document does not have a use case scenario for exchanging data between security services that are previously unknown to each other. For example, a relying party may choose to trust assertions made by an asserting party based on the signatures on the AP's digital certificate, or through other means.

The following use case scenario would illustrate using assertions from an unknown party.

In this scenario, an application service provider has a policy to allow access to resources for all full-time students at accredited 4-year universities and colleges. It would be difficult for the application service provider to maintain agreements with hundreds of such organizations in order to verify assertions made by those parties. Instead, it chooses to check the key of the asserting party to ensure that the asserting party is a 4-year university.

{PRIVATE "TYPE=PICT;ALT=Unknown
Partner"}

Fig X. Unknown Partner

Steps:

1. Student authenticates to university security system.
2. University provides authentication document to student application, including authentication event data and authorization attributes.
3. Student application requests resource from application service provider. Request includes authentication document.
4. Application service provider makes a trust decision about the authn and authz data, based on the key used to sign the assertion. It determines that the signing party is an accredited 4-year university, based on a signature on the key made by an accrediting organization.
5. Application service provider makes an authorization decision based on the authz attributes of the student.
6. Application service provider returns resource to the student.

Possible Resolutions:

1. Add this use case scenario to the use case document.
2. Do not add this use case scenario to the use case document.

Status: Closed per F2F #2, Resolution 2 Carries

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	2
Resolution 2	7
Abstain	0

In voting for resolution 2, Bob Blakley said, " I think this overspecifies behavior... both the 'interesting' flows in the diagram here are from the Application Service Provider to *itself*. Why should we tell the A.S.P. how to make trust decisions about assertions?"

CLOSED ISSUE:[UC-1-11:AuthNEvents]

It is not specified in straw man 2 what authentication information is passed between parties. In particular, specific information about authn events, such as time of authn and authn protocol are alluded to but not specifically called out.

The use case scenarios would be edited to show when information about authn events would be transferred, and the requirement for authn data would be edited to say:

> [CR-1-11-AuthN] SAML should define a data format for authentication assertions, including descriptions of authentication events.

Possible Resolutions:

1. Edit the use case scenarios to specifically define when authn event descriptions are transferred, and edit the R-AuthN requirement.
2. Do not change the use case scenarios or R-AuthN requirement.

Status: Closed per F2F #2, Resolution 1 Carries

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18

Resolution 1	9
Resolution 2	0
Abstain	0

CLOSED ISSUE:[UC-1-12:SignOnService]

Bob Morgan suggests changing the title of use case 1, "Single Sign-on," to "Sign-on Service."

Possible Resolutions:

1. Make this change to the document.
2. Don't make this change.

Status: Closed per F2F #2, 2 carries

CLOSED ISSUE:[UC-1-13:ProxyModel]

Irving Reid suggests an additional use case scenario for single sign-on, based on proxies.

A scenario would be added to the document as follows:

Scenario X: Single Sign-on, Proxy Model

In this model, the user authenticates to a proxy and then sends a request, including credentials, to the proxy. The proxy generates SAML assertions, attaches them to the request, and forwards the request to the destination web site. The destination web site replies to the proxy, and the proxy forwards the reply back to the client.

In this model, the user authenticates to a proxy and then sends a request, including credentials, to the proxy. The proxy generates SAML assertions, attaches them to the request, and forwards the request to the destination web site. The destination web site replies to the proxy, and the proxy forwards the reply back to the client.

Alternatively, the initial message from the client to the proxy could include both the authentication credentials and the request rather than having a separate round-trip for authentication.

{PRIVATE "TYPE=PICT;ALT=Single Sign-on, Proxy Model"}

Fig X. Single Sign-on, Proxy Model

Steps:

1. Web user authenticates to proxy.
2. Web user requests destination resource through proxy.
3. Proxy provides authentication document to destination Web site.
4. Proxy requests destination resource from destination Web site.
5. Destination Web site provides destination resource to proxy.
6. Proxy provides destination resource to Web user.

There are two sub-variants to this use case: In some cases the proxy will return SAML tokens of some sort to the client, and the client will use those tokens (most likely in the form of HTTP cookies) to make subsequent requests within the single-sign-on session. In the other variant, the proxy has an existing session mechanism with the client. In that case, the proxy can store the SAML tokens and transparently attach them to subsequent requests within that session.

Possible Resolutions:

1. Add this use case scenario to the document.
2. Don't make this change.

Status: Closed by explicit vote at F2F #2, 2 carries, however see UC-1-14

CLOSED ISSUE:[UC-1-14: NoPassThruAuthnImpactsPEP2PDP]

Stephen Farrell has argued that dropping PassThruAuthN prevents standardization of important functionality in a commonly used configuration.

The counter argument is the technical difficulty of implementing this capability, especially when both username/password and PKI AuthN must be supported.

Possible Resolutions:

1. Add this requirement to SAML 1.0
2. authorize a subgroup/task force to evaluate a suitable pass-through authN solution for eventual inclusion in V.next of SAML. If the TC likes the design once it is presented, it may choose to open up its scope to once again include pass-through authN in V1.0. Stephen is willing to champion this."
3. Do not add this requirement.

Status: Closed on May 15 telcon, 2 carries

Group 2: B2B Scenario Variations

CLOSED ISSUE:[UC-2-01:AddPolicyAssertions]

Some use cases proposed on the security-use list (but not in the straw man 1 document) use a concept of a "policy document." In concept a policy document is a statement of policy about a particular resource, such as that user "evanp" is granted "execute" privileges on file "/usr/bin/emacs." Another example may be that all users in domain "Acme.com" with role "backup administrator" may perform the "shutdown" method on resource "mail server," during non-business hours.

Use cases where policy documents are exchanged, and especially activities like security discovery as in UC-4-04:SecurityDiscovery, would require this type of assertion. If these use cases and/or services were adapted, the term "policy document" should be used. In addition, the following requirement would be added:

> [CR-2-01-Policy] SAML should define a data format for security policy about resources.

In addition, the explicit non-goal for authorization policy would be removed.

Another thing to consider is that the intended XACML group within Oasis is planning on working on defining a policy markup language in XML, and any work we do here could very well be redundant.

Possible Resolutions:

1. Remove the non-goal, add this requirement, and refer to data in this format as "policy documents."
2. Maintain the non-goal, leave out the requirement.

Status: Closed per F2F #2, Resolution 1 Carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	11
Resolution 2	0

CLOSED ISSUE:[UC-2-02:OutsourcedManagement]

A use case scenario provided by Hewlett Packard illustrates using SAML enveloped in a CIM/XML request. Should this scenario be included in the use case document?

The use case would be inserted as follows (some editing for clarity):

This scenario shows an enterprise A that has outsourced the management of its network devices to a management service provider B. Management messages are exchanged using CIM/XML over HTTP. (CIM or Common Information Model, is a management standard being developed by the Distributed Management Task Force - http://www.dmtf.org/, an XML DTD for CIM has been defined.)

Suppose the operator, Joe, wants to invoke the StopService method. This will be executed by the XML/CIM agent on the managed device, if authorized.

{PRIVATE "TYPE=PICT;ALT=Outsourced Management"}

Fig X. Outsourced Management.

Fig X. Outsourced Management.

Steps:

1. This SAML assertion has been generated by B's attribute authority (or Policy Decision Point) and confers the role "System Manager for A" to Joe.

2. The CIM management console generates the XML content and attaches an SAML assertion. The CIM management console signs the request and sends it as an HTTP request.
3. The request now has to traverse A's firewall or the boundary into A's network. The gateway at this boundary uses its SAML evaluation engine (or Policy Enforcement Point) to verify that this incoming message is allowed. It does this, by verifying the signature and discovering the request is from Joe. Next it uses two assertions to authorize the incoming message: the assertion issued by B's attribute authority that is attached to the message (conferring the role "System Manager for A" on Joe); an assertion issued by A's attribute authority granting "Gateway Access" to any entity that has a valid "System Manager for A" assertion issued by B's attribute authority. Note that the second assertion can be pushed to the gateway (part of its configuration), or retrieved dynamically from a repository (or indeed the issuer) (the last case is shown here).
4. The request is forwarded by the gateway to the managed device.
5. The SAML evaluation engine on the managed device needs to determine if a "StopService" request from Joe is allowed. It does this by using two assertions: the "System Manager for A" assertion issued by B's attribute authority; an assertion issued by A's attribute authority granting "Full Management Rights" to any entity with a valid "System Manager for A" assertion issued by B's attribute authority.
6. The managed device executes the "StopService" method.

Potential Resolutions:

1. Add this use-case scenario to the document.
2. Do not add this use-case scenario.

Status: Closed per F2F #2, 2 carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	5
Resolution 2	6

CLOSED ISSUE:[UC-2-03:ASP]

A use case scenario provided by Hewlett Packard illustrates using SAML for a secure interaction between an application service provider (ASP) and a client. Should this scenario be included in the use case document?

The use case would be inserted as follows (some editing for clarity):

In this scenario an ASP, A, is providing an application (possible examples could be a word processor or an ERP application) to users in another enterprise, B. A VPN (for example IPSEC) is used to provide a secure end-to-end tunnel between the client and server.

A major difference between this scenario and the outsource management service scenario is that all assertions are "pulled" in this scenario. This means the assertions are not attached to application messages; instead they must be retrieved either directly from the attribute authority, or a repository. For example, once the client has been authenticated, the SAML evaluation engine in the server needs to retrieve the SAML assertions issued by A and B. This will involve making a request to a repository inside B, traversing both A and B's firewall as shown in the diagram. Similarly the SAML engines in the gateway and client will have to retrieve assertions issued by both authorities.

{PRIVATE "TYPE=PICT;ALT=Application Service
Provider"}

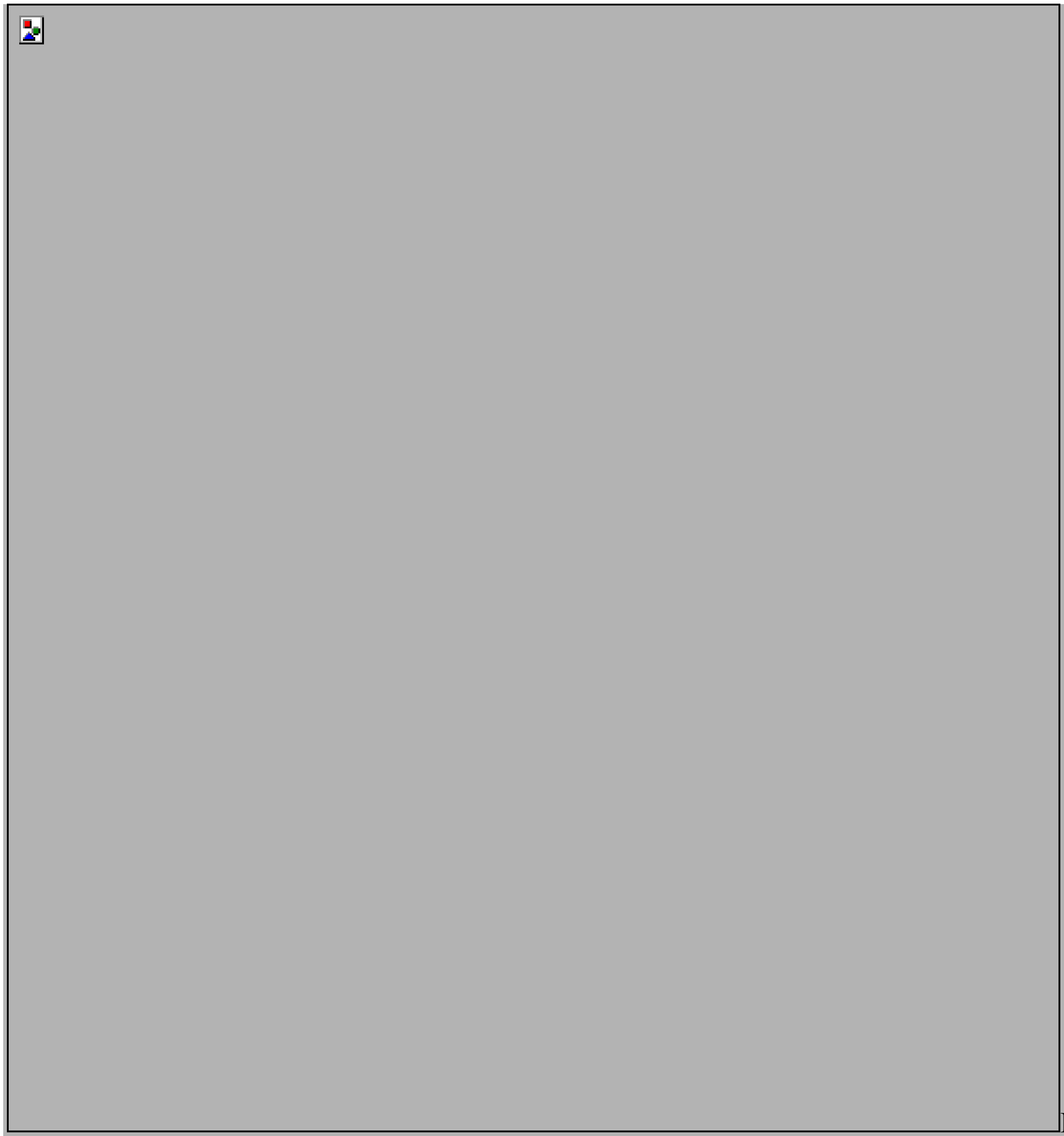


Fig X. Application Service Provider.

Fig X. Application Service Provider.

Steps:

1. The client authenticates with B's attribute authority.
2. B's attribute authority provides an authentication assertion that the client is a "valid user."
3. The client requests an application through A's gateway, providing a reference to the

authentication assertion.

4. The gateway needs to know that incoming packets from a client in B are allowed. It needs an assertion from B's attribute authority that the client is a valid user, and an assertion from A's attribute authority that entities issued "valid user" assertions from B are allowed access. The gateway requests the assertion from B's attribute authority.
5. B's attribute authority provides the assertion.
6. The gateway requests an authorization assertion from A's attribute authority.
7. A's attribute authority provides the authorization assertion.
8. The gateway forwards the request to the Server.
9. The server requests the assertion from B's attribute authority.
10. B's attribute authority provides the assertion.
11. The server requests an authorization assertion from A's attribute authority.
12. A's attribute authority provides the authorization assertion.
13. The server authenticates with A's attribute authority.
14. A's attribute authority provides a reference to an authentication assertion that the server is an "Approved Application".
15. The server returns the application to the client.
16. It is also important that the client check that the application is valid. This avoids problems such as an attacker spoofing the service provider and providing a word processor service that silently emails copies of all documents generated by the client to the attacker. This might be done by the client SAML evaluation engine checking two assertions: one from A granting "Approved Application" status to the server; one from B granting the attribute "execute" to any entity with "Approved Application" status issued by A. The Client requests the authentication assertion from A's attribute authority.
17. A's attribute authority provides the assertion.
18. The client requests an authorization assertion from B's attribute authority.
19. B's attribute authority provides the authorization assertion.

Potential Resolutions:

1. Add this use-case scenario to the document.

2. Do not add this use-case scenario.

Status: Closed per F2F #2, 2 carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	5
Resolution 2	6

ISSUE:[UC-2-05:EMarketplace]

Zahid Ahmed proposes the following additional use case scenario for inclusion in the use case and requirements document.

Scenario X: E-Marketplace

{PRIVATE
"TYPE=PICT;ALT=EMarketplace"}

Fig X. EMarketplace.

Figure X: E-Marketplace Transaction.

A B2B Transaction involving buyers and suppliers that conduct trade via an e-marketplace that provides trading party authentication and authorization services, and other business services, in support of secure transaction and routing of business document exchanges between trading parties.

Steps:

1. A trading party (TP, e.g., buyer) creates a business document for subsequent transaction with another trading party (e.g., supplier) accessible via its e-marketplace.

2. The sending, i.e., transaction-initiating trading party (TP) application creates credential data to be authenticated by the authentication and security service operated by an e-

marketplace.

3. The trading party application transaction client packages the XML-based credential data along with the other XML-based business document over a specific transport, messaging, and application protocol. Note: Credential data for login is not in SAML scope at the present time.

   Some examples of such (layered) protocols are following (but not limited to):

   - Secure transports: SSL and/or HTTPS
   - Messaging protocol: S/MIME and JMS.
   - Message Enveloping Formats: SOAP, etc.
   - B2B Application Protocol: ebXML, BizTalk, etc.

4. E-marketplace Authentication Service validates the TP Credential and creates a SAML authn assertion along with attribute assertions for the transaction-initiating TP.

   NOTE: The authentication protocol and service and message processing service that process SAML document instances are beyond the scope of the OASIS SAML Specification. However, it is included here mainly to highlight the transaction flow and is not defined as part of any SAML spec.

5. The E-marketplace Messaging Service then packages the AuthN Assertion and attribute assertions along with the original message payload into a tamper-proof envelope (i.e., S/MIME multi-part signed)

6. The resulting message envelope is transmitted to the target trading party (service provider).

7. The receiving trading party application extracts and processes the TP identity and authorization information available in the received envelope.

8. Receiving TP application then processes the business document of the sending TP.

9. Receiving TP sends back a response to sending TP via its e-marketplace by repeating Steps 1 through 5.

Possible Resolutions:

1. The above scenario should be added to the use cases document.

2. The above scenario should not be added to the document.

Status: Voted, No conclusion

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	7
Resolution 2	4

CLOSED ISSUE:[UC-2-06:EMarketplaceDifferentProtocol]

Zahid Ahmed has proposed that the following use case scenario be added to the use case and requirements document.

Scenario X: E-Marketplace, Different Protocol

{PRIVATE "TYPE=PICT;ALT=EMarketplace Different Protocol"}

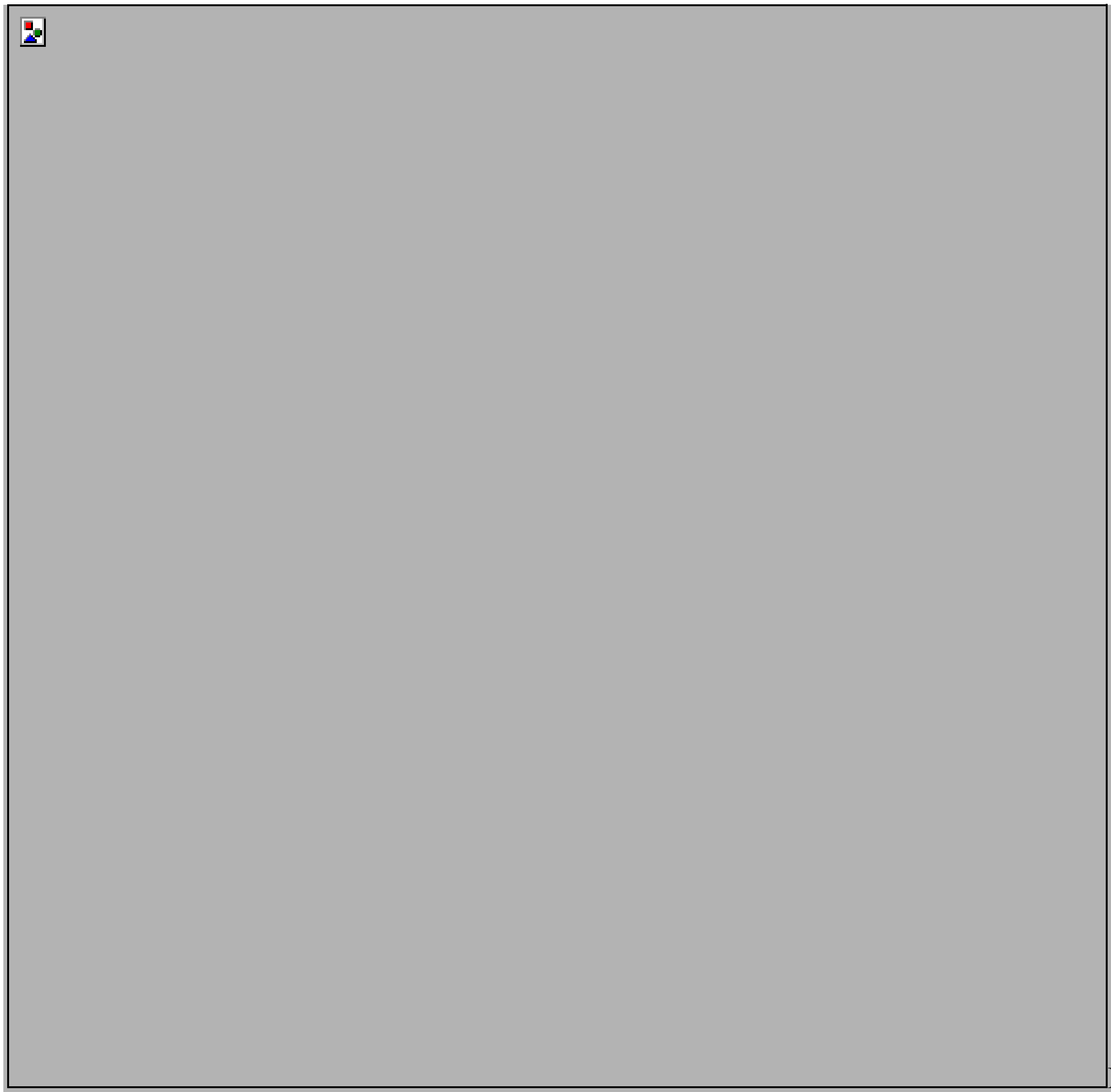


Fig X. EMarketplace, Different Protocol.

A B2B Document Exchange Transaction that involves two trading parties such that sending trading party (e.g., Buyer) uses one messaging and transport protocol (e.g., OBI) and receiving party (e.g., Supplier) uses a another messaging/transport protocol (e.g., ebXML). A B2B transaction service must provide relevant security interoperability services as part of its general messaging and application interoperability mechanism.

Steps:

1. The sending trading party employs a specific messaging and application protocol.
2. The sending TP application then transacts with the receiving TP via its e-marketplace

following Steps# 1 through 3 in Issue# UC-2-05 described above.

3. The e-marketplace authentication and security service provider authenticated and validates the sending TP and produce relevant SAML security assertions as described in Step# 4in Issue# UC-2-05 described above.

4. The e-marketplace interoperability service transforms the incoming message to target trading party messaging and application protocol such that SAML AuthN and any attribute assertion document instances are included into the newly transformed message for subsequent transmission to the receiving TP.

5. The receiving TP extracts, processes the security assertions about the sending TP as described in Step# 7 in Issue# UC-2-05 above.

6. Receiving TP sends back a response to sending TP via its e-marketplace by repeating Steps 1 through 5.

Possible Resolutions:

1. Add this scenario to the document.

2. This use case scenario should not be added to the document.

Status: Closed per F2F #2, 2 carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	3
Resolution 2	8

CLOSED ISSUE:[UC-2-07:MultipleEMarketplace]

Zahid Ahmed proposes the following use case scenario for inclusion in the document. This use case/issue is a variant of ISSUE# [UC-2-05].

In this scenario the transacting trading parties are members of different e-marketplaces or trading communities. To support B2B transactions between trading parties of different e-markletplaces, the e-marketplaces will provide secure interconnectivity between the set of trading hubs involved in the transaction between the transaction parties. In this manner e-marketplaces will act as trusted intermediaries between transacting trading parties.

Steps:

1. Repeat Steps# 1-5 in Issue# [UC-2-07].
2. Receiving e-marketplace, e.g., e-marketplace A, message service transmits the message to target e-marketplace, e-marketplace B.
3. E-marketplace B Authentication Service validates the Signed Envelope that contains the E-marketplace signature used to package the SAML security assertions about the sending TP.
4. E-marketplace B Authentication Service may additionally validate And/or insert new SAML AuthN assertion and attribute assertions, depending on its inter-portal connectivity security policies.
5. E-marketplace B transmits the authenticated message received from E-marketplace A to the target TP.

Possible Resolutions:

1. Add this scenario to the document.
2. The above scenario should not be added to the document.

Status: Closed per F2F #2, 2 carries

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	3
Resolution 2	8

CLOSED ISSUE:[UC-2-08:ebXML]

Maryann Hondo proposed this use case scenario for inclusion in the use case document. (Note that an interaction diagram illustrating this use case still must be developed, to replace the current diagram. Also, the steps involved should be brought in line with other use case scenarios in the use case and requirements document.)

Use Case Scenario X: ebXML

This scenario shows the use of SAML for providing security services to an ebXML conversation. In addition, it gives an example of ebXML providing the necessary negotations to enable a SAML conversation.

{PRIVATE
"TYPE=PICT;ALT=EMarketplace"}

Fig X. ebXML.

Steps:

1. Party A wishes to engage with Party B in a business transaction. To do this, Party A accesses information [stored in an ebXML Collaboration Party Profile (CPP)] about Party B's requirements for doing business.
2. Party A and Party B negotiate at ebXML Collaboration Party Agreement (CPA). Some of the information in a CPP or CPA might include:
    - Party B requires authorization attributes from AttributeAuthorityFoo
    - Party B requires that Party A be authorized by Foo in the BuyerQ role.

   Party A then must be able to determine:

    - How to get these authorization attributes.
    - where/how to insert these assertions in an ebXML message
3. Party A enrolls with AttributeAuthorityFoo. Party A engages in ebXML business transactions and wants to restrict what entities are able to retrieve its attributes.

4. Party B's Message Service Handler (MSH) has received a digitally-signed ebXML message from Party A and wishes to obtain authorization attributes about Party A. Authorization attributes must be retrievable based on the DN in the certificate used to sign the ebXML message.
5. AttributeAuthorityFoo checks authentication of Party B to ensure B can read A's authorization attributes. It then returns the data to B.

Steps 1-3 are specified by ebXML, and step 4 is what is relevent to SAML. Step 4 would add a requirement to the SAML specification to allow the query of authorization data from an attribute authority, using a DN as the UID passed to locate the record.

Potential Resolutions:

1. Add this use case scenario to the use case and requirements document.
2. Do not add this scenario.

Status: Closed per F2F #2, 2 carries

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	3
Resolution 2	8

Group 3: Sessions

[At F2F #2, it was agreed to charter a sub group to "do the prep work to ensure that logout, timein, and timeout will not be precluded from working with SAML later; commit to doing these other pieces "next" after 1.0." Therefore all the items in this section have been closed with the notation "referred to sub group."]

The purpose of the issues/resolutions in this group is to provide guidance to the rest of the TC as to the functionality required related to sessions. Some of the scenarios contain some detail about the messages which are transferred between parties, but the intention is not to require a particular protocol. Instead, these details are offered as a way of describing the functionality required. It would be perfectly acceptable if the resulting specification used different messages to accomplish the same functionality.

CLOSED ISSUE:[UC-3-01:UserSession]

Should the use cases of log-off and timeout be supported? These result in the notion of session management. Advantage: Allows complete web user experience across multiple web sites. If not done as part of this specification, then some other body or work will have to standardize this functionality. Disadvantage: More complex than just passing authentication references between source and destination. Will slow down Technical committees work on specification of authentication/authorization only queries.

Candidate Requirement:

> [CR-3-1-UserSession] SAML shall support web user session(s).

The following use case scenario would be added to the use case and requirements document.

A Single Sign-on and hand-off

Note that this is a duplicate of Oasis security Services Scenario #1

{PRIVATE "TYPE=PICT;ALT=Single Sign-on, User

Session"}

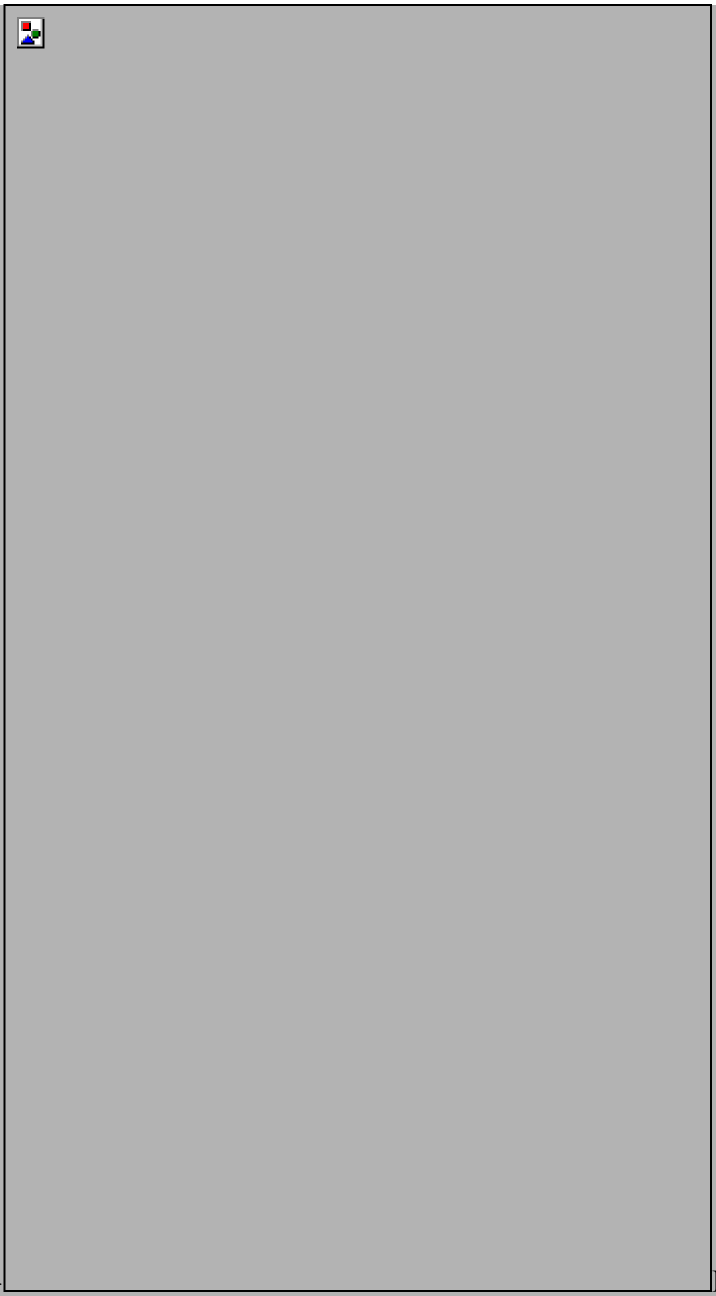


Fig X. Single Sign-on, User Session.

Steps:

1. A user logs onto the source Web site. This results in the creation of a session on the source web site.
2. User requests a link to a destination web site. This link contains an authentication reference/token/ticket.

3. User requests resource represented by link on destination web site, including reference
4. Destination web site requests validation of authentication reference from source web site.
5. Source web site returns success or failure, optionally additional session information.
6. Destination web site returns web site to user

Timeout

1. Assume that the user has gone beyond the timeout limit on the source web site.
2. The source web site will query each participating web site to determine if the user has been active on their web site.
3. If the user has not been active on any of the destination web sites within the timeout period, the destination web sites are instructed to delete the session.

Logout

1. User logs out of the source web site.
2. Each of the destination web sites are instructed to delete the session.

Possible Resolutions:

1. Add this requirement and/or use cases to SAML.
2. Do not add this requirement and/or use cases.

Status: Closed, referred to sub group

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	8
Resolution 2	2
Abstain	0

In voting for resolution 1, Jeff Hodges added, "rationale: if there's these "assertions" floating about between various entities that serve to assert the identity of some particular entity, there's notions of "validity time period" (however implemented), and there's notions of "state" relative to the asserted identity, then I feel what we have here meets the definition of a "session", and we ought to use that term (and really figure out what all the implications are)." He also attached the following URLs:

```
http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?query=session&action=Search
      http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?query=state
```

CLOSED ISSUE:[UC-3-02:ConversationSession]

Is the concept of a session between security authorities separate from the concept of a user session? If so, should use case scenarios or requirements supporting security system sessions be supported? [DavidO: I don't understand this issue, but I have left in for backwards compatibility]. [DarrenP: I think this issue arose out of a misunderstanding/miscommunication on the mailing list and has been resolved. This is more of a formality to vote this one to a closed status.]

Possible Resolutions:

1. Do not pursue this requirement as it is not in scope.
2. Do further analysis on this requirement to determine what it is specifically.

Status: Closed, referred to sub group

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	5
Resolution 2	5
Abstain	0

CLOSED ISSUE:[UC-3-03:Logout]

Should SAML support transfer of information about application-level logouts (e.g., a principal intentionally ending a session) from the application to the Session Authority ?

Candidate Requirement:

[CR-3-3-Logout] SAML shall support a message format to indicate the end of an application-level session due to logout by the principal.

Note that this requirement is implied by Scenario 1-3 (the second scenario 1-3 in straw man 3 - oops). This issue seeks to clarify the document by making the requirement explicit.

Possible Resolutions:

1. Add this requirement to SAML.
2. Do not add this requirement to SAML.

Status: Closed, referred to sub group

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	5
Resolution 2	5
Abstain	0

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	9
Resolution 2	1
Abstain	1

CLOSED ISSUE:[UC-3-05:SessionTermination]

For managing a SAML User Sessions, it may be useful to have a way to indicate that the SAML-level session is no longer valid. The logout requirement would invalidate a session based on user input. This requirement, for termination, would invalidate the SAML-level session based on other factors, such as when the user has not used any of the SAML-level sessions constituent application- level sessions for more than a set amount of time. Timeout would be an example of a session termination.

Candidate requirement:

> [CR-3-5-SessionTermination] SAML shall support a message format for timeout of a SAML-level session. Here, "termination" is defined as the ending of a SAML-level session by a security system not based on user input. For example, if the user has not used any of the application-level sub-sessions for a set amount of time, the session may be considered "timed out."

Note that this requirement is implied by Scenario 1-3, figure 6, specifically the last message labeled 'optionally delete/revoke session'. This issue seeks to clarify the document by making the requirement explicit.

Possible Resolutions:

1. Add this requirement to SAML.
2. Do not add this requirement and/or use cases.

Status: Closed, referred to sub group

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	6
Resolution 2	4
Abstain	0

In voting for resolution 2, Jeff Hodges added, "rationale: I believe this is subsumed within the topic of [UC-3-1:UserSession] and we should deal with it explicitly in that context."

Bob Blakley said, "However I believe that the phrasing of the requirement is wrong. I think what we should support is expiration of assertions. Timeout is an action a receiving system implements based on observing that an assertion has timed out."

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	9

Resolution 2	2
Abstain	1

CLOSED ISSUE:[UC-3-06:DestinationLogout]

Should logging out of an individual application-level session be supported? Advantage: allows application Web sites control over their local domain consistent with the model most widely implemented on the web. Disadvantage: potentially more interactions between the application and the Session Authority.

In this scenario a Session Authority is managing a SAML-level session that includes an application-level session maintained by the destination Web site. The user invokes a logout event on the destination Web site, which invalidates the application-level session. The destination Web site passes this information back to the Session Authority.

{PRIVATE "TYPE=PICT;ALT=Destination Logout"}

Fig. X. Destination Logout.

Steps:

1. User initiates a logout event on the destination Web site.
2. Destination Web site invalidates the application-level session and notifies the Session Authority.

Candidate Requirement:

> [CR-3-6-DestinationLogout] The SAML model for session management shall support logout initiated by the user at a destination site, that is, a site other than the one where the session was initiated.

Possible Resolutions:

1. Add this scenario and requirement to SAML.
2. Do not add this scenario or requirement.

Status: Closed, referred to sub group

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	4
Resolution 2	5
Abstain	1

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	8
Resolution 2	3
Abstain	1

CLOSED ISSUE:[UC-3-07:Logout Extent]

What is the impact of logging out at a destination web site?

Possible Resolution:

1. Logout from destination web site is local to destination [DavidO recommendation]
2. Logout from destination web site is global, that is destination + source web sites.

Status: Closed, referred to sub group

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	7
Resolution 2	0
Resolution 3	1
Abstain	2

Jeff Hodges, abstaining, said, "rationale: needs clarification. E.g. BobB's point in Group3VoteBlakley.html should be considered."

CLOSED ISSUE:[UC-3-08:DestinationSessionTermination]

Having the Session Authority determine the timeout of a session is covered under [UC-3-5]. This issue covers the manner and extent to which systems participating in that session can initiate and control the timeout of their own sessions.

In this scenario a Session Authority is managing a SAML-level session that includes an application-level session maintained by the destination Web site. The user's application-level session times out (or is terminated for any reason) on the destination Web site, and the destination consults with the Session Authority to determine if the application-level session should be terminated.

{PRIVATE "TYPE=PICT;ALT=Destination Timeout"}

Fig. X. Destination Timeout.

Steps:

1. Based on an internal timer, the destination Web site determines that the user's application-level session has expired.
2. The destination Web site requests information on the session from the Session Authority to determine if the SAML-level session has other, active application-level sessions elsewhere.
3. Based on domain-specific policy the destination Web site either:
    1. leaves the application-level session untouched (thus deferring all control to the Session Authority)
    2. terminates the application-level session (thus rejecting any control by the Session Authority) and sends a message to the Session Authority informing the Session Authority that this application-level session is no longer active
    3. extends the application-level session by some pre-determined "grace period" (compromise between 'a' and 'b')

Candidate requirement:

> [CR-3-8-DestinationSessionTermination] SAML shall support destination system session termination.

Possible Resolutions:

1. Add this scenario and requirement to SAML.
2. Do not add this scenario or requirement.

Status: Closed, referred to sub group

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	4
Resolution 2	6
Abstain	0

In voting for resolution 2, Jeff Hodges added, "rationale: I believe this is subsumed within the topic of [UC-3-1:UserSession] and we should deal with it explicitly in that context."

Bob Blakley said, "I don't feel that I understand well enough what we'd consider doing here to express an opinion yet."

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	7
Resolution 2	4
Abstain	1

CLOSED ISSUE:[UC-3-09:Destination-Time-In]

In this scenario, a user has traveled from the source site (site of initial login) to some destination site. The source site has set a maximum idle-time limit for the user session, based on user activity at the source or destination site. The user stays at the destination site for a period longer than the source site idle-time limit; and at that point the user returns to the source site. We do not wish to have the user time-out at the source site and be re-challenged for authentication; instead, the user should continue to enjoy the original session which would somehow be cognizant of user activity at the destination site.

Candidate Requirement:

> [CR-3-9:Destination-TimeIn] SAML shall support destination system time-in.

Possible Resolutions:

1. Add this scenario and requirement to SAML.
2. Do not add this scenario or requirement to SAML.

Status: Closed, referred to sub group

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	7
Resolution 2	4

Abstain	1

Group 4: Security Services

CLOSED ISSUE:[UC-4-01:SecurityService]

Should part of the use case document be a definition of a security service? What is a security service and how is it defined?

Potential Resolutions:

1. This issue is now obsolete and can be closed as several securityservices (shared sessioning, PDP--PEP relationship) have been identified within SAML.
2. This issue should be kept open.

Status: Closed per F2F #2, 1 carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	8
Resolution 2	3

CLOSED ISSUE:[UC-4-02:AttributeAuthority]

Should a concept of an attribute authority be introduced into the [SAML] use case document? What part does it play? Should it be added in to an existing use case scenario, or be developed into its own scenario?

The "attribute authority" terminology has already been introduced in the Hal/David diagrams and discussed by the use-case group. So this issue can be viewed as requiring more detail concerning the flows derived from the diagram to be introduced into the use-case document.

The following use-case scenario is offered as an instance:

(a) User authenticates and obtains an AuthN assertion. (b) User or server submits the AuthN assertion to an attribute authority and in response obtains an AuthZ assertion containing authorization attributes.

Potential Resolutions:

1. A use-case or use-case scenario similar to that described above should be added to

SAML.

2. This issue is adequately addressed by existing use cases and does not require further elaboration within SAML.

Status: Closed per F2F #2, Resolution 2 Carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	2
Resolution 2	7

CLOSED ISSUE:[UC-4-03:PrivateKeyHost]

A concept taken from S2ML. A user may allow a server to host a private key. A credentials field within an AuthN assertion identifies the server that holds the key. Should this concept be introduced into the [SAML] use case document? As a requirement? As part of an existing use case scenario, or as its own scenario?

The S2ML use-case scenario had the following steps:

1. User Jane (without public/private key pair) authenticates utilizing a trusted server X and receives an AuthN assertion. The trusted server holds a private/public key pair.The AuthN assertion received by Jane includes a field for the server X's public key.

2. User submits a business payload and said AuthN assertion to trusted server X. The trusted server "binds" the assertion to the payload using some form of digital signing and sends the composite package onto the next stage in the business flow.

Potential Resolutions:

1. A use-case or use-case scenario comprising steps 1 and 2 above should be added to the use-case document.

2. A requirement for supporting "binding" between AuthN assertions and business payloads thru digital signature be added to the use-case document.

3. This issue has been adequately addressed elsewhere; there is no need for any additions to the use-case document.

Status: Closed per F2F #2, Resolution 2 Carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	3
Resolution 2	9

CLOSED ISSUE:[UC-4-04:SecurityDiscover]

UC-1-04:ARundgrenPush describes a single sign-on scenario that would require transfer of authorization data about a resource between security zones.Should a service for security discovery be part of the [SAML] standard?

Possible Resolutions:

1. Yes, a service could be provided to send authorization dataabout a service between security zones. This would require some sort of policy assertions (UC-2-01:AddPolicyAssertions).

2. No, this extends the scope of [SAML] too far. AuthZ in [SAML]should be concerned with AuthZ attributes of a principal, not of resources.

Status: Closed per F2F #2, Resolution 2 Carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	12
Resolution 1	0
Resolution 2	11

Group 5: AuthN Protocols

CLOSED ISSUE:[UC-5-01:AuthNProtocol]

Straw Man 1 explicitly makes challenge-response authentication a non-goal. Is specifying which types of authn are allowed and what protocols they can use necessary for this document? If so, what types and which protocols?

As written, this issue covers a lot of ground. [UC-5-03:AuthNthrough] covers the core issue of the removal of all considerations of modeling authentication methods within SAML, which need not be discussed further in 5-01.

There is an aspect of these requirements that has been discussed and noted as important on the list. There is a need for describing different forms of credentials (name-password, public key, X509 certificates etc) within SAML. In this sense there is a connection to the different "permitted forms of authn" [2] and SAML.

REFERENCES: I believe these requirements are consistent with or can be derived from Nigel's suggestion [1] but is perhaps closer to the current style of specification in Strawman 2. It also reflects the discussion in [2] and [3].

```
      [1] http://lists.oasis-open.org/archives/security-
use/200102/msg00029.html
      [2] http://lists.oasis-open.org/archives/security-
use/200102/msg00038.html
      [3] http://lists.oasis-open.org/archives/security-
use/200102/msg00064.html
```

Possible Resolutions (not mutually exclusive):

1. The Non-Goal

   > "Challenge-response authentication protocols are outside the scope of the SAML"

   should be removed from the Strawman 3 document.

2. The following requirements should be added to the Strawman 3 document:

   > [CR-5-01-1-StandardCreds] SAML should provide a data format for credentials including those based on name-password, X509v3 certificates, public keys, X509 Distinguished name, and empty credentials.
   >
   > [CR-5-01-2-ExtensibleCreds] SAML The credentials data format must support extensibility in a structured fashion.

Status: Closed per F2F #2, 1 is not removed, 2 is not added, but see UC-1-14

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1 For	8
Resolution 1 Against	3
Resolution 2 For	8
Resolution 2 Against	3
Abstain	0

In voting for resolution 2, Bob Blakley said, "My thinking here is that we need to provide a way to assert what mechanism was used to authenticate the user (e.g. certificate-based authentication) and what the user's authenticated credential resulting from that authentication (e.g. X.509 cert) was. I'm still nervous about allowing the VALUE of the password to be used as credential information as in S2ML, but I do understand why this was done and that it's useful."

CLOSED ISSUE:[UC-5-02:SASL]

Is there a need to develop materials within SAML that explore its relationship to SASL [SASL]?

Possible Resolutions:

1. Yes
2. No

Status: Closed per F2F #2, 2 carries

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1	3
Resolution 2	5

Abstain	2

CLOSED ISSUE:[UC-5-03:AuthNThrough]

All the scenarios in Straw Man 1 presume that the user provides authentication credentials (password, certificate, biometric, etc) to the authentication system out-of-band.

Possible Resolutions (not mutually exclusive):

1. Should SAML be used directly for authentication? In other words should the SAML model or express one or more authentication methods or a framework for authentication?
2. Should this be explicitly stated as a non-goal?
3. Should the following statement be added to the non-goals section?

> [NO-Authn] Authentication methods or frameworks are outside the scope of SAML.

Status: Closed per F2F #2, Resolution 1 Fails, Resolution 2 Passes, Resolution 3 Fails

Voting Results

{PRIVATE}Date	23 Feb 2001
Eligible	18
Resolution 1 For	1
Resolution 1 Against	10
Resolution 2 For	10
Resolution 2 Against	1
Resolution 3 For	7
Resolution 3 Against	4
Abstain	0

NOTE: resolutions for this issue were voted on separately.

Group 6: Protocol Bindings

CLOSED ISSUE:[UC-6-01:XMLProtocol]

Should mention of a SOAP binding in the use case and requirements document be changed to a say "an XML protocol" (lower case, implying generic XML-based protocols)? Or "XML Protocol", the specific W3 RPC-like protocol using XML (http://www.w3.org/2000/xp/)?

Although SOAP is being reworked in favor of XP, the current state of XML Protocol is unknown. Requiring a binding to that protocol by June may not be feasible.

Per David Orchard, "There is no such deliverable as XML Protocol specification. We don't know when an XMLP 1.0 spec will ship. We can NEVER have forward references in specifications. When XMLP ships, we can easily change the requirements. [...] I definitely think we should mandate a SOAP 1.1 binding."

Possible Resolutions:

1. Change requirement for binding to SOAP to binding to XML Protocol.
2. Leave current binding to SOAP.
3. Remove mention of binding to either of these protocols.

Status: Closed per F2F #2, Resolution 2 Carries

Voting Results

{PRIVATE}Date	27 Mar 2001
Eligible	15
Resolution 1	0
Resolution 2	12
Abstain	2

Group 7: Enveloping vs. Enveloped

ISSUE:[UC-7-01:Enveloping]

SAML data will be transferred with other types of XML data not specific to authn and authz, such as financial transaction data. What should the relationship of the documents be?

One possibility is requiring that SAML allow for enveloping business-specific data within SAML. Such a requirement might state:

> [CR-7-01:Enveloping] SAML messages and assertions should be able to envelop conversation-specific XML data.

Note that this requirement is not in conflict with [CR-7-02:Enveloped]. They are mutually compatible.

Possible Resolutions:

1. Add this proposed requirement.
2. Do not add this proposed requirement.

Status: Voted, No Conclusion

Voting Results

{PRIVATE}Date	27 Mar 2001
Eligible	15
Resolution 1	9
Resolution 2	4
Abstain	1

ISSUE:[UC-7-02:Enveloped]

SAML data will be transferred with other types of XML data not specific to authn and authz, such as financial transaction data. What should the relationship of the documents be?

One possibility is requiring that SAML should be fit for being enveloped in other XML documents.

> [CR-7-02:Enveloped] SAML messages and assertions should be fit to be enveloped in

conversation-specific XML documents.

Note that this requirement is not in conflict with [CR-7-01:Enveloping]. They are mutually compatible.

Possible Resolutions:

1. Add this proposed requirement.
2. Do not add this proposed requirement.

Status: Voted, Resolution 1 Carries

Voting Results

{PRIVATE}Date	27 Mar 2001
Eligible	15
Resolution 1	12
Resolution 2	2

Group 8: Intermediaries

CLOSED ISSUE:[UC-8-01:Intermediaries]

The use case scenarios in the S2ML 0.8a specification include one where an intermediary passes an S2ML message from a source party to a destination party. What is the part of intermediaries in an SAML conversation?

A requirement to enable passing SAML data through intermediaries could be phrased as follows:

> [CR-8-01:Intermediaries] SAML data structures (assertions and messages) will be structured in a way that they can be passed from an asserting party through one or more intermediaries to a relying party. The validity of a message or assertion can be established without requiring a direct connection between asserting and relying party.

Possible Resolutions:

1. Add this requirement to the document.
2. Do not add this requirement to the document.

Status: Closed per F2F #2, Resolution 1 Carries

Voting Results

{PRIVATE}Date	27 Mar 2001
Eligible	15
Resolution 1	12
Resolution 2	2

ISSUE:[UC-8-02:IntermediaryAdd]

One question that has been raised is whether intermediaries can make additions to SAML documents. It is possible that intermediaries could add data to assertions, or add new assertions that are bound to the original assertions.

If we wanted to support allowing intermediaries to add data to SAML documents, the following use-case scenario could be added to the use case and requirements document:

In this use case scenario, two parties -- a buyer and a seller -- perform a transaction using a B2B exchange as an intermediary. The intermediary adds AuthN and AuthZ data to orders as they go through the system, giving additional points for decisions made by the parties.

{PRIVATE "TYPE=PICT;ALT=Intermediary Add"}

Fig. X. Intermediary Add

Steps:

1. Buyer authenticates to Buyer Security System.

2. Buyer Security System provides a SAML AuthN assertion to Buyer, containing data about the authentication event and authorization attributes about the Buyer.

3. Seller authenticates to Seller Security System.

4. Seller Security System provides a SAML AuthN assertion to Seller, containing data about the authentication event and authorization attributes about the Seller.

5. Buyer requests authorization from Buyer Security System to submit a given order.

6. Buyer Security System provides a SAML AuthZ Decision assertion to Buyer, stating that Buyer is allowed to submit the order.

7. Buyer submits order to B2B Exchange, providing AuthN assertion and AuthZ decision assertion.

8. B2B exchange adds AuthN assertion data, specifying that the exchange authenticated the buyer (using the assertion).

9. B2B exchange adds AuthZ decision assertion data, stating that the Buyer is permitted to use the exchange to make this order.

10. B2B exchange submits order to Seller.

11. Seller validates the order, using the assertions.

12. Seller requests authorization from Seller Security System to fulfill a given order.

13. Seller Security System provides a SAML AuthZ Decision assertion to Seller, stating that Seller is allowed to fulfill the order.

14. Seller submits intention to fulfill the order to the B2B exchange, including AuthN assertions and AuthZ decision assertions.

15. B2B exchange adds AuthN data, specifying that it used the original SAML AuthN assertion to authenticate the Seller.

16. B2B exchange add AuthZ decision data, specifying that the seller is authorized to fulfill this order through the exchange.

17. B2B exchange sends the order fulfillment to the Buyer.

18. Buyer validates the order fulfillment based on AuthN assertion(s) and AuthZ decision assertion(s).

Possible Resolutions:

1. Add this use-case scenario to the document.

2. Don't add this use-case scenario.

Status: Voted, Resolution 1 Carries

Voting Results

{PRIVATE}Date	27 Mar 2001
Eligible	15
Resolution 1	11
Resolution 2	3

ISSUE:[UC-8-03:IntermediaryDelete]

Another issue with intermediaries is whether SAML must support allowing intermediaries to delete data from SAML documents.

If so, the following use-case scenario could be added to the use case document to illustrate.

Use Case Scenario X: Intermediary Delete

In this scenario, a buyer and a seller are using a B2B exchange to perform a transaction. The B2B exchange acts as an intermediary between the two parties. The exchange has an interest in not being disintermediated by the parties, so it modifies submitted SAML data to anonymize the buyer. This would prevent the seller from directly contacting the buyer without using the exchange.

{PRIVATE "TYPE=PICT;ALT=Intermediary
Delete"}

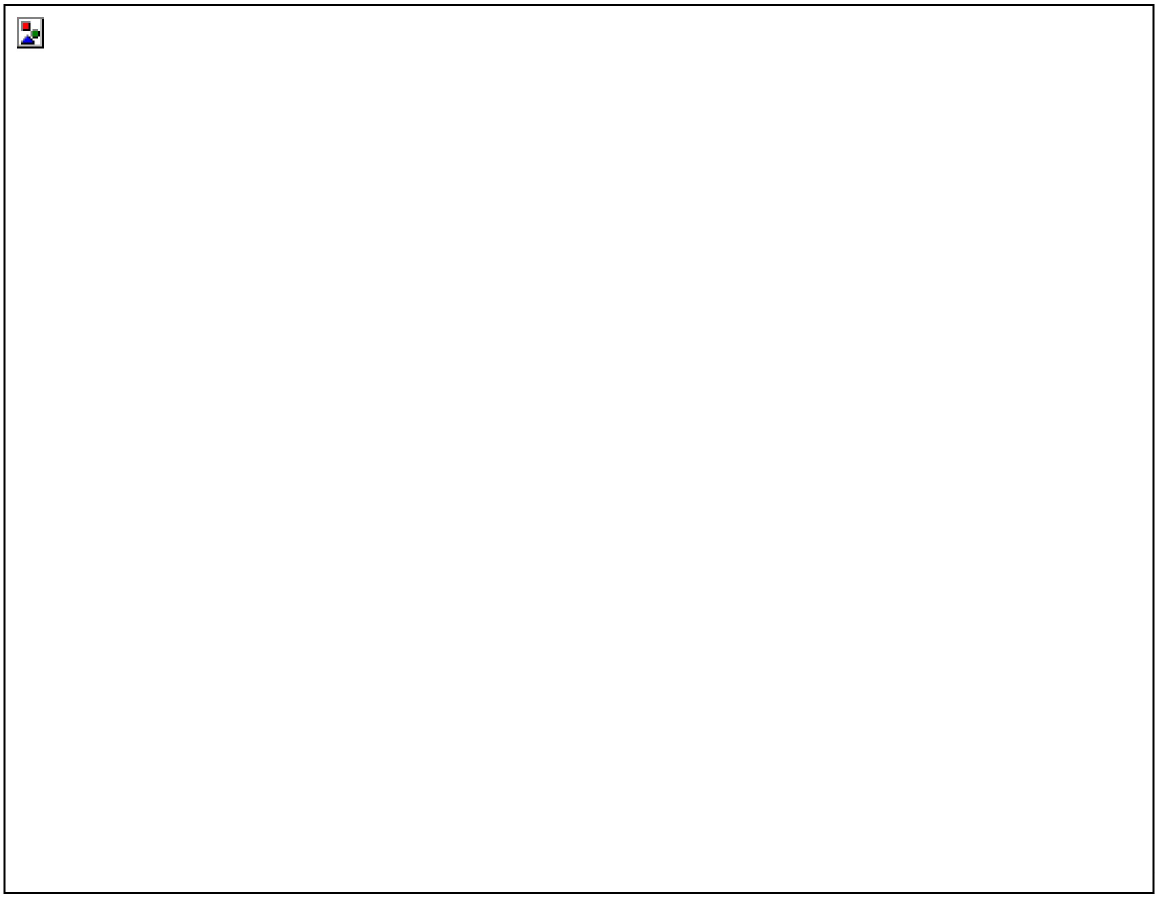


Fig. X. Intermediary Delete

Steps:

1. Buyer authenticates to Buyer Security System.
2. Buyer Security System provides a SAML AuthN assertion to Buyer, containing data about the authentication event and authorization attributes about the Buyer.
3. Buyer requests authorization from Buyer Security System to submit a given order.
4. Buyer Security System provides a SAML AuthZ Decision assertion to Buyer, stating that Buyer is allowed to submit the order.
5. Buyer submits order to B2B Exchange, providing AuthN assertion and AuthZ decision assertion.
6. B2B exchange anonymizes the order by removing identifying attributes from the SAML submitted by Buyer.
7. B2B exchange submits order to Seller.

Possible Resolutions:

1. Add this use-case scenario to the document.
2. Don't add this use-case scenario.

Status: Voted, No Conclusion

Voting Results

{PRIVATE}Date	27 Mar 2001
Eligible	15
Resolution 1	6
Resolution 2	8

ISSUE:[UC-8-04:IntermediaryEdit]

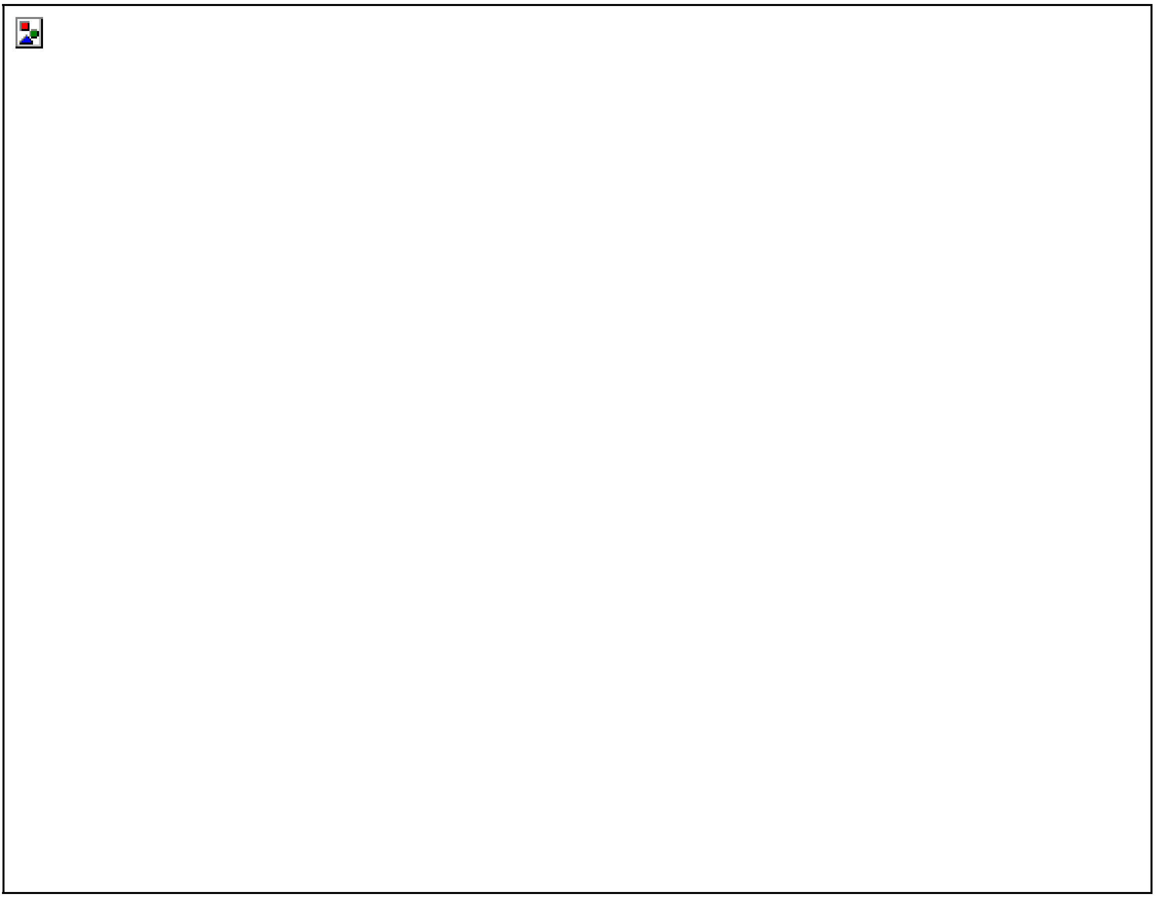
Similar to [UC-8-03:IntermediaryDelete] is the issue of whether SAML must support allowing intermediaries to edit or change SAML data as they pass it between parties.

If so, the following use-case scenario could be added to the use case document to illustrate.

Use Case Scenario X: Intermediary Edit

In this scenario, a buyer and a seller are using a B2B exchange to perform a transaction. The B2B exchange acts as an intermediary between the two parties. In this case, the buyer and seller use different vocabularies for expressing security concepts and also different vocabularies for domain concepts. The B2B exchange provides a translation before passing on SAML documents.

{PRIVATE "TYPE=PICT;ALT=Intermediary



Edit"}

Fig. X. Intermediary Edit

Steps:

1. Buyer authenticates to Buyer Security System.
2. Buyer Security System provides a SAML AuthN assertion to Buyer, containing data about the authentication event and authorization attributes about the Buyer. One AuthZ attribute is that the Buyer has a "role" of "purchase agent".
3. Buyer requests authorization from Buyer Security System to submit a given order.
4. Buyer Security System provides a SAML AuthZ Decision assertion to Buyer, stating that Buyer is allowed to submit the order. Specifically, it states that Buyer has the "purchase" privilege for the given order.
5. Buyer submits order to B2B Exchange, providing AuthN assertion and AuthZ decision assertion.
6. Based on registered settings of the Seller, the B2B exchange knows that Seller uses a different vocabulary than Buyer. For example, Seller has only group-based AuthZ, not

role-based. So it changes the "role" attribute to "group". Additionally, it knows that the Seller uses the term "buy" and not "purchase" for the privilege of making an order, so it translates that AuthZ information, too.

7. B2B exchange submits order to Seller.

Possible Resolutions:

1. Add this use-case scenario to the document.
2. Don't add this use-case scenario.

Status: Voted, No Conclusion

Voting Results

{PRIVATE}Date	27 Mar 2001
Eligible	15
Resolution 1	4
Resolution 2	10

ISSUE:[UC-8-05:AtomicAssertion]

One implicit assumption about SAML is that assertions will be represented as XML elements with associated digital signatures. Any additions, deletions or changes would make the signature on the assertion invalid. This would make it difficult for relying parties to determine the validity of the assertion itself, especially if it is received through an intermediary.

Thus, the implementation of assertions as element + signature would make [UC-8-02:IntermediaryAdd], [UC-8-03:IntermediaryDelete], and [UC-8-04:IntermediaryEdit] difficult to specify, if the idea is to actually modify the original assertions themselves. One possible solution is that some kind of diff or change structure could be added. Another possibility is that signatures on each individual sub-element of the assertion could be required, so that if the intermediary changes one sub-element the others remain valid. Neither of these is a clean solution.

However, if there's no goal of changing the sub-elements of the assertion, then it's possible to implement modifications. For example, [UC-8-02:IntermediaryAdd] can be implemented without breaking apart assertions. The B2B exchange could simply add its own assertions to the order, as well as the assertions provided by the buyer.

Deletion and edition could be implemented by simply replacing the assertions made by the buyer -- passing new AuthZ and AuthC assertions made and signed by the B2B exchange. These would incorporate elements from the assertions made by the Buyer Security System, but be signed by the B2B exchange.

There is semantic value to who makes an assertion, though. If the B2B exchange makes the assertion rather than the Buyer Security System, there is a different level of validity for the Seller.

Since assertion as element + signature is a very natural implementation, it may be good to express the indivisibility of the assertion as part of a non-goal. One such non-goal could be:

> [CR-8-05:AtomicAssertion] SAML does not need to specify a mechanism for additions, deletions or modifications to be made to assertions.

In addition, the use case scenarios should be edited to specifically point out that additions, deletions or modifications make changes to whole assertions, and not to parts of assertions.

Possible Resolutions:

1. Add this non-goal to the document, and change use case scenarios to specify that intermediaries must treat assertions as atomic.
2. Don't add this non-goal.

Status: Voted, Resolution 1 Carries

Voting Results

{PRIVATE}Date	27 Mar 2001
Eligible	15
Resolution 1	12
Resolution 2	2

Group 9: Privacy

ISSUE:[UC-9-01:RuntimePrivacy]

Should protecting the privacy of the user be part of the SAML conversation? In other words, should user consent to exchange of data be given at run time, or at the time the user establishes a relationship with a security system?

An example of runtime privacy configuration would be use case scenario described in [UC-1-04:ARundgrenPush]. Because this scenario has been rejected by the use cases and requirement group, it makes sense to phrase this as a non-goal of SAML, rather than as a requirement.

> [CR-9-01:RuntimePrivacy] SAML does not provide for subject control of data flow (privacy) at run-time. The determination of privacy policy is between the subject and security authorities and should be determined out-of-band, for example, in a privacy agreement.

Possible Resolutions

1. Add this proposed non-goal.

2. Do not add this proposed non-goal.

Status: Voted, No Conclusion

Voting Results

{PRIVATE}Date	27 Mar 2001
Eligible	15
Resolution 1	9
Resolution 2	4

ISSUE:[UC-9-02:PrivacyStatement]

Important private data of end users should be shared as needed between peers in an SAML conversation. In addition, the user should have control over what data is exchanged. How should the requirement be expressed in the use case and requirements document?

One difficulty is that, if run-time privacy is out of scope per UC-9-01:RuntimePrivacy, it's difficult to impose a privacy requirement on eventual implementers. Especially considering that our requirements doc is for the specification itself, and not for implementers. In addition, specifications rarely proscribe guiding principles that cannot be expressed in the specified technology itself.

One statement suggested by Bob Morgan is as follows:

> [CR-9-02-3-DisclosureMorgan] SAML should support policy-based disclosure of subject security attributes, based on the identities of parties involved in an authentication or authorization exchange.

Another, by Bob Blakley:

> [CR-9-02-2-DisclosureBlakley] SAM should support *restriction of* disclosure of subject security attributes, *based on a policy stated by the subject*. *This policy might be* based on the identities of parties involved in an authentication or authorization exchange.

A final one, by Prateek Mishra:

> [CR-9-02-4-DisclosureMishra] An AP should only release credentials for a subject to an RP if the subject has been informed about this possibility and has assented. The exact mechanism and format for interaction between an AP and a subject concerning such privacy issues is outside the scope of the specification.

Comment by David Orchard:

"My concerns about all of the disclosure requirements, is that I cannot see how any piece of software could be tested for conformance. In the case of Blakely style, "SAM should support *restriction of* disclosure of subject security attributes, *based on a policy stated by the subject*", how do I write a conformance test that verifes:

- what are allowable and non-allowable restrictions?
- How do I test that an non-allowable restriction hasn't been made?
- How do I verify that a subject has stated a policy?
- How can a subject state a policy?"

Possible Resolutions

1. Add [CR-9-02-3-DisclosureMorgan] as a requirement.
2. Add [CR-9-02-2-DisclosureBlakley] as a requirement.
3. Add [CR-9-02-4-DisclosureMishra] as a requirement.
4. Add none of these as requirements.

Status: Voted, No Conclusion

Colors: Gray Blue Yellow

Voting Results

{PRIVATE}Date	27 Mar 2001
Eligible	15
Resolution 1	4
Resolution 2	0
Resolution 3	4
Resolution 4	7

Group 10: Framework

CLOSED ISSUE:[UC-10-01:Framework]

Should SAML provide a framework that allows delivery of security content negotiated out-of-band? A typical use case is authorization extensions to the core SAML constructs. The contra-position is to rigidly define the constructs without allowing extension.

A requirement already exists in the SAML document for extensibility: [R-Extensible] SAML should be easily extensible. Therefore, the change that voting on this issue would make would be to remove rather than add a requirement.

Possible Resolutions:

1. Remove the extensibility requirement.
2. Leave the extensibility requirement.

Status: Closed per F2F #2, Resolution 2 Carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	1
Resolution 2	10

ISSUE:[UC-10-02:ExtendAssertionData]

Assertions are the "nouns" of SAML. One way to extend SAML is to allow additional elements in an assertion besides the ones specified by SAML. This could be used to add additional attributes about a subject, or data structured under another namespace.

A requirement that captures this functionality would be:

> [CR-10-02:ExtendAssertionData] The format of SAML assertions should allow the addition of arbitrary XML data as extensions.

Possible Resolutions:

1. Add requirement [CR-10-02:ExtendAssertionData].
2. Do not add this requirement.

Status: Closed per F2F #2, 2 carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	7
Resolution 2	4

CLOSED ISSUE:[UC-10-03:ExtendMessageData]

Similarly to [UC-10-02], it would be useful to allow additional data to SAML messages. Either defined SAML assertions, or arbitrary XML, could be attached.

A potential requirement to add this functionality would be:

> [CR-10-03:ExtendMessageData] The format of SAML messages should allow the addition of arbitrary XML data, or SAML assertions not specified for that message type, as extensions.

Possible Resolutions:

1. Add requirement [CR-10-03:ExtendMessageData].
2. Do not add this requirement.

Status: Closed per F2F #2, 2 carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	7
Resolution 2	4

CLOSED ISSUE:[UC-10-04:ExtendMessageTypes]

It's common in protocol definitions that real-world implementations require additional message types. For example, a system handling a request for authorization that is taking a long time might send a <KeepWaiting> or <AskAgainLater> message to the requester.

Many protocols explicitly allow for a mechanism for adding extended message types in their specification. We may want to require that SAML also allow for extended message types in the specification. One requirement may be:

> [CR-10-04:ExtendMessageTypes] The SAML protocol will explicitly allow for additional message types to be defined by implementers.

Note that this is different from [UC-10-03:ExtendMessageData]. That issue is about adding extended data to existing message types in the protocol. This issue is about adding new message types entirely.

Also note that adding this requirement would strongly favor [CR-10-07-1], to allow interoperability.

Possible Resolutions:

1. Add requirement [CR-10-04:ExtendMessageTypes].

2. Do not add this requirement.

Status: Closed per F2F #2, 2 carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	4
Resolution 2	7

CLOSED ISSUE:[UC-10-05:ExtendAssertionTypes]

As with [UC-10-04], it may be useful to add extended assertions to a SAML conversation. As an admittedly stretched example, an implementer may choose to add auditing to the SAML specification, and therefore define one or more <AuditAssertion> types.

Note that this is different from [UC-10-02:ExtendAssertionData]. That issue is about adding arbitrary XML to an existing assertion type. This issue is about creating new assertion types altogether.

Note that this is also different from [UC-10-03:ExtendMessageData]. In that issue, arbitrary XML data could be added to a message. In this issue, the XML would have some format or attributes to identify it specifically as a SAML assertion.

One requirement that would make this functionality clear would be:

> [CR-10-05:ExtendAssertionTypes] SAML will explicitly allow for additional assertion types to be defined by implementers.

Also note that adding this requirement would strongly favor [CR-10-07-1], to allow interoperability. Also, extended assertion types would probably require extended messages, so this requirement would favor adding [CR-10-04:ExtendMessageTypes].

Possible Resolutions:

1. Add requirement [CR-10-05:ExtendAssertionTypes].
2. Do not add this requirement.

Status: Closed per F2F #2, 2 carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	4
Resolution 2	7

CLOSED ISSUE:[UC-10-06:BackwardCompatibleExtensions]

Because SAML is an interoperability standard, it's important that custom extensions for SAML messages and/or assertions be compatible with standard SAML implementations. For this reasons, extensions should be clearly recognizable as such, marked with flags to indicate whether processing should continue if the receiving party does not support the extension.

One possible requirement for this functionality is the following:

> [CR-10-06-BackwardCompatibleExtensions] Extension data in SAML will be clearly identified for all SAML processors, and will indicate whether the processor should continue if it does not support the extension.

Possible Resolutions:

1. Add requirement [CR-10-06-BackwardCompatibleExtensions].
2. Do not add this requirement.

Status: Closed per F2F #2, Resolution 1 Carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	11
Resolution 2	0

CLOSED ISSUE:[UC-10-07:ExtensionNegotiation]

Many protocols allow a negotiation phase between parties in a message exchange to determine which extensions and options the other party supports. For example, HTTP 1.1 has the OPTIONS method, and ESMTP has the EHLO command.

Since this is a fairly common design model, it may be useful to add such a feature to SAML. One option is to add a requirement for extension negotiation:

> [CR-10-07-1:ExtensionNegotiation] SAML protocol will define a message format for negotiation of supported extensions.

However, this may unnecessarily complicate the SAML protocol. Because negotiation is a common design, it may be a good idea to have a clarifying non-goal in the requirements document:

> [CR-10-07-2:NoExtensionNegotiation] SAML protocol does not define a message format for negotiation of supported extensions.

Possible Resolutions:

1. Add requirement [CR-10-07-1:ExtensionNegotiation].
2. Add non-goal [CR-10-07-2:NoExtensionNegotiation].
3. Add neither the requirement nor the non-goal.

Status: Closed per F2F #2, 3 carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	4

Resolution 2	2
Resolution 3	5

Group 11: AuthZ Use Case

CLOSED ISSUE:[UC-11-01:AuthzUseCase]

Use Case 2 in Strawman 3 (http://www.oasis-open.org/committees/security/docs/draft-sstc-use-strawman- 03.html) describes the use of SAML for the conversation between a Policy Enforcement Point (PEP) and a Policy Decision Point (PDP), in which the PEP sends a request describing a particular action (such as 'A client presenting the attached SAML data wishes to read http://foo.bar/index.html'), and the PDP replies with an Authorization Decision Assertion instructing the PEP to allow or deny that request.

Possible Resolutions:

1. Continue to include this use case.
2. Remove this use case.

Status: Closed per F2F #2, Resolution 1 Carries

Voting Results

{PRIVATE}Date	27 Mar 2001
Eligible	15
Resolution 1	9
Resolution 2	2

Group 12: Encryption

UC-9-02:PrivacyStatement addresses the importance of sharing data only as needed between security zones (from asserting party to relying party). However, it is also important that data not be available to third parties, such as snoopers or untrusted intermediaries.

One possible solution for protocol bindings to define secure channels between relying party and asserting party. Another is specifically encrypt the SAML data, so that it is protected whether or not the channel is secure, and can also be stored securely outside of the protocol binding (for example, in a cache or as a cookie).

If confidentiality protection is specified both within the SAML message format and within protocol bindings, deployments can choose the appropriate solution. For example, SAML messages within encrypted S/MIME documents may not need message-level protection, while SAML messages passed as HTTP cookies do.

The issues addressed here also relate to [R-Signature], [UC-13-02:EfficientMessages], [UC-13-03:OptionalAuthentication], and [UC-13-04:OptionalSignatures]. In particular, we would be contradicting ourselves if we voted that confidentiality protection is required without exception, and at the same time voted for option 1 on any of the UC-13 issues listed above. The point raised in the UC-13 issues is that within a protected security domain where confidentiality protection is not a concern, requiring encryption could introduce key management and performance issues that could otherwise be avoided.

This issue breaks down into several decisions:

Should confidentiality protection of SAML assertions be required, optional, or unsupported?

Should confidentiality protection be provided by the protocol binding or within the SAML message format?

What (if any) encryption method should be used now?

What (if any) encryption method should be used once XML Encryption is a published standard?

One thing to note is that there is currently an explicit non-goal that SAML will not protect messages from interception by third parties; this is left up to the transport mechanism. The issue group 12 decisions may force removal of this non-goal (specifically, if we choose encryption of individual SAML messages or assertions).

CLOSED ISSUE:[UC-12-01:Confidentiality]

Add the following requirement:

> [R-Confidentiality] SAML data should be protected from observation by third parties or

untrusted intermediaries.

Possible Resolutions:

1. Add [R-Confidentiality]
2. Do not add [R-Confidentiality]

Status: Closed per F2F #2, Resolution 1 Carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	8
Resolution 2	2

CLOSED ISSUE:[UC-12-02:AssertionConfidentiality]

1. Add the requirement: [R-AssertionConfidentiality] SAML should define a format so that individual SAML assertions may be encrypted, independent of protocol bindings.
2. Add the requirement: [R-AssertionConfidentiality] SAML assertions must be encrypted, independent of protocol bindings.
3. Add a non-goal: SAML will not define a format for protecting confidentiality of individual assertions; confidentiality protection will be left to the protocol bindings.
4. Do not add either requirement or the non-goal.

Status: Closed per F2F #2, No Conclusion

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	3
Resolution 2	0
Resolution 3	4

Resolution 4	4

CLOSED ISSUE:[UC-12-03:BindingConfidentiality]

The first option is intended to make the protection optional (both in the binding definition, and by the user at runtime).

1. [R-BindingConfidentiality] Bindings SHOULD (in the RFC sense) provide a means to protect SAML data from observation by third parties. Each protocol binding must include a description of how applications can make use of this protection. Examples: S/MIME for MIME, HTTP/S for HTTP.
2. [R-BindingConfidentiality] Each protocol binding must always protect SAML data from observation by third parties.
3. Do not add either requirement.

Status: Closed per F2F #2, Resolution 1 Carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	11
Resolution 2	0
Resolution 3	0

CLOSED ISSUE:[UC-12-04:EncryptionMethod]

If confidentiality protection is included in the SAML assertion format (that is, you chose option 1 or 2 for [UC-12-02:AssertionConfidentiality]), how should the protection be provided?

Note that if option 2 (assertion confidentiality is required) was chosen for UC-12-02, resolution 1 of this issue implies that SAML will not be published until after XML Encryption is published.

Proposed resolutions; choose one of:

1. Add the requirement: [R-EncryptionMethod] SAML should use XML Encryption.
2. Add the requirement: [R-EncryptionMethod] Because there is no currently published standard for encrypting XML, SAML should define its own encryption format. Edit the

existing non-goal of not creating new cryptographic techniques to allow this.

3. Add no requirement now, but include a note that this issue must be revisited in a future version of the SAML spec after XML Encryption is published.

4. Do not add any of these requirements or notes.

Status: Closed per F2F #2, Resolution 3 Carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	0
Resolution 2	0
Resolution 3	9
Resolution 4	2

Group 13: Business Requirements

CLOSED ISSUE:[UC-13-01:Scalability]

Bob Morgan brought up several "business requirements" on security-use. One was scalability. This issue is a placeholder for further elaboration on the subject.

A candidate requirement might be:

> [CR-13-01-Scalability] SAML should be appropriate for high volume of messages, and for messages between parties made up of several physical machines.

Potential Resolutions:

1. Add requirement [CR-13-01-Scalability].
2. Do not add this requirement.

Status: Closed per F2F #2, 2 carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	4
Resolution 2	5
Abstain	1

CLOSED ISSUE:[UC-13-02:EfficientMessages]

Philip Hallam-Baker's core assertions requirement document included several requirements that were efficiency-oriented. When that requirement document was merged into Straw Man 2, the efficiency requirements were excluded.

One such requirement was:

> [CR-13-02-EfficientMessages] SAML should support efficient message exchange.

Potential Resolutions:

1. Add this requirement to the use case and requirements document.

2. Leave this requirement out of use case and requirements document.

Status: Closed per F2F #2, 2 carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	3
Resolution 2	7

CLOSED ISSUE:[UC-13-03:OptionalAuthentication]

Philip Hallam-Baker's core assertions requirement document included several requirements that were efficiency-oriented. When that requirement document was merged into Straw Man 2, the efficiency requirements were excluded.

One such requirement was:

> [CR-13-03-OptionalAuthentication] Authentication between asserting party and relying party should be optional. Messages may omit authentication altogether.

In this case, "authentication" means authentication between the parties in the conversation (for example, by means of a digital signature) and not authentication by the subject.

Potential Resolutions:

1. Add this requirement to the use case and requirements document.
2. Leave this requirement out of use case and requirements document.

Status: Closed per F2F #2, 2 carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	6
Resolution 2	4

CLOSED ISSUE:[UC-13-04:OptionalSignatures]

Philip Hallam-Baker's core assertions requirement document included several requirements that were efficiency-oriented. When that requirement document was merged into Straw Man 2, the efficiency requirements were excluded.

One such requirement was:

> [CR-13-04-OptionalSignatures] Signatures should be optional.

Potential Resolutions:

1. Add this requirement to the use case and requirements document.
2. Leave this requirement out of use case and requirements document.

Status: Closed, Voted on May 15 telcon for resolution 1

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	6
Resolution 2	4

CLOSED ISSUE:[UC-13-05:SecurityPolicy]

Bob Morgan proposed a business-level requirement as follows:

> [CR-13-05-SecurityPolicy] Security measures in SAML should support common institutional security policies regarding assurance of identity, confidentiality, and integrity.

Potential Resolutions:

1. Add this requirement to the use case and requirements document.
2. Leave this requirement out of use case and requirements document.

Status: Closed per F2F #2, Resolution 2 Carries

Voting Results

{PRIVATE}Date	6 Apr 2001

Eligible	11
Resolution 1	2
Resolution 2	8

CLOSED ISSUE:[UC-13-06:ReferenceReqt]

Bob Morgan has questioned requirement [R-Reference] in that it is not specific enough. In particular, he said: "Goal [R-Reference] either needs more elaboration or (likely) needs to be dropped. What is a 'reference'? It doesn't have a standard well-understood security meaning nor is it defined in the glossary. This Goal seems to me to be making an assumption about a low-level mechanism for optimizing some of the transfers."

One possible, more specific elaboration might be:

> [CR-13-06-1-Reference] SAML should define a data format for providing references to authentication and authorization assertions. Here, a "reference" means a token that may not be a full assertion, but can be presented to an asserting party to request a particular assertion.
>
> [CR-13-06-2-Reference-Message] SAML should define a message format for requesting authentication and authorization assertions using references.
>
> [CR-13-06-2-Reference-Size] SAML references should be small. In particular, they should be small enough to be transferred by Web browsers, either as cookies or as CGI parameters.

Potential Resolutions:

1. Replace [R-Reference] with these requirements.
2. Leave [R-Reference] as it is.
3. Remove mention of references entirely.

Status: Closed per F2F #2, Resolution 2 Carries

Voting Results

{PRIVATE}Date	6 Apr 2001
Eligible	11
Resolution 1	6

Resolution 2	0
Resolution 3	5

ISSUE [UC-13-07: Hailstorm Interoperability]

Should SAML provide interoperability with the Microsoft Hailstorm architecture, including the Passport login system?

Status: Open

Design Issues

Group 1: Naming Subjects

ISSUE:[DS-1-01: Referring to Subject]

By what means should Assertions identify the subject they refer to?

Bob Blakely points out that references can be:

1. Nominative (by name, i.e. some identifier)
2. Descriptive (by attributes)
3. Indexical (by "pointing")

SAML may need to use all types, but Indexical ones in particular can be dangerous from a security perspective.

Potential Resolutions:

??

Status: Open

ISSUE:[DS-1-02: Anonymity Technique]

How should the requirement of Anonymity of SAML assertions be met?

Potential Resolutions:

1. Generate a new, random identified to refer to an individual for the lifetime of a session.

2. ???

Status: Open

Group 2: Naming Objects

CLOSED ISSUE:[DS-2-01: Wildcard Resources]

Nigel Edwards has proposed that Authorization Decision Assertions be allowed to refer to multiple resources by means of some kind of wildcards.

Potential Resolutions:

1. Allow resources to be specified with fully general regular expressions.
2. Allow resources to be specified with simple * wildcard in the final path element: e.g. /foo/*, but not /foo/*/x or /foo/y*
3. Don’t allow wildcarded resources

Status: Closed by vote during May 29 telecon

ISSUE:[DS-2-02: Permissions]

Should the qualifiers of objects be called permissions, actions or operations? Authorization decision assertions contain an object that identifies the target of the request. This is qualified with a field called permissions, containing values like “Read” and “Write”. Normal English language usage suggests that this field represents an Action or Operation on the object.

Possible Resolutions:

1. Retain Permissions
2. Change to Actions
3. Change to Operations

Status: Open

Group 3: Assertion Validity

ISSUE:[DS-3-01: DoNotCache]

It has been suggested that there should be a way in SAML to specify that an assertion is currently valid, but should not be cached for later use. This should not depend on the particular amount of variation between clocks in the network.

For example, a PDP may wish to indicate to a PEP that it should make a new request for every authorization decision. For example, its policy may be subject to change at frequent and unpredictable intervals. It would be desirable to have a SAML specified convention for doing this. This may interact with the position taken on clock skew. For example, if SAML takes no position on clock skew the PDP may have to set the NotAfter value to some time in the future to insure that it is not considered expired by the PEP.

Potential Resolutions:

1. SAML will specify some combination of settings of the IssueInstant and ValidityInterval to mean that the assertion should not be cached. For example, setting all three datetime fields to the same value could be deemed indicate this.

2. SAML will add an additional element to either Assertions or Responses to indicate the assertion should not be cached.

3. SAML will provide no way to indicate that an Assertion should not be cached.

Status: Open

ISSUE:[DS-3-02: ClockSkew]

SAML should consider the potential effects of clock skew in environments it is used.

It is impossible for local system clocks in a distributed system to be exactly the same, the only question is: how much do they differ by? This becomes an issue in security systems when information is marked with a validity period. Different systems will interpret the validity period according to their local time. This implies:

1. Relying parties may not make the same interpretation as asserting parties.

2. Distinct relying parties may make different interpretations.

Generally what matters is not the absolute difference, but the difference as compared to the total validity interval of the information. For example, the PKI world has tended to (rightly) ignore this issue because CA and EE certificates tend to have validity intervals of years. Even Attribute Certificates and SAML Attribute Assertions are likely to have validity intervals of days or hours.

However, it seems likely that Authorization Decision Assertions may sometimes have validity intervals of minutes or seconds. Therefore, the issue must be raised.

One common problem is what to set the NotBefore element to. If it is set to the AP's current time, it may not yet be valid for the RP. If set in the past, (a common practice) the questions arise 1) how far in the past? and 2) should the NotAfter time also be adjusted? If NotBefore is omitted, this may not be satisfactory for nonrepudiation purposes.

The NotAfter value can also be an issue if the assumed clock skew is large compared to the Validity Interval.

[These paragraphs contain personal observations by Hal Lockhart, others may disagree.

In the early 1990's some popular computer systems had highly erratic system clocks which could drift from the correct time by as much as five minutes per day. Kerberos's requirement for rough time synchronization (usually 5 minutes) was criticized at that time because of this reality.

Today most popular computer systems have clocks which keep time accurately to seconds per month. Therefore the most common current source of time differences is the manual process of setting time. Therefore, most systems tend to be accurate within a few minutes, generally less than 10.

By means of NTP or other time synchronization system, it is not hard to keep systems synchronized to less than a minute, typically within 10 seconds. It is common for production server systems to be maintained this way. The price of GPS hardware has fallen to the point where it is not unreasonably expensive to keep systems synchronized to the true time with sub-second accuracy. However, few organizations bother to do this.]

Potential Resolutions:

1. SAML will leave it up to every deployment how to deal with clock skew.

2. SAML will explicitly state that deployments must insure that clocks differ by no more that X amount of time (X to be specified in the specification)

3. SAML will provide a parameter to be set during deployment that defines the maximum clock skew in that environment. This will be used by AP's to adjust datetime fields according to some algorithm.

4. SAML will provide a parameter in assertions that indicates the maximum skew in the environment. RPs should use this value in interpreting all datetime fields.

Status: Open

ISSUE:[DS-3-03: ValidityDependsUpon]

In a previous version of the draft spec, assertions contained a `ValidityDependsUpon` element, which allowed the asserting party to indicate that this assertion was valid only if another, specified assertion was valid. This was dropped because it was felt that the lack of a SAML mechanism to revoke previously issued assertions made it moot.

A number of people feel that this element is useful nevertheless and should be restored.

It is worth noting that even in the absence of this element (from the a particular assertion or SAML as a whole) a particular relying party can still have a policy that requires multiple assertions to be valid.

Status: Open

Group 4: Assertion Style

ISSUE:[DS-4-01: Top or Bottom Typing]

Should assertions be identified as Authentication, Attribute and Authorization Decision, each containing specified elements? (Top Typing) Or should only the elements be defined allowing them to be freely mixed? (Bottom Typing)

Two comprehensive proposals to address this issue have been made in draft-orchard-maler-assertion-00 and draft-sstc-core-08.

Status: Open

ISSUE:[DS-4-02: XML Terminology]

Which XML terms should we be using in SAML? Possibilities include: message, document, package.

Status: Open

ISSUE:[DS-4-03: Assertion Request Template]

What is the best way to provide a template of values in an assertion request?

Two comprehensive proposals to address this issue have been made in draft-orchard-maler-assertion-00 and draft-sstc-core-08.

Potential Resolutions:

1. The requestor sends an assertion with the required field types, but missing values
2. The requestor sends fields and values, in the form of a list, not an assertion
3. XPATH expressions
4. XML query statements

Status: Open

ISSUE:[DS-4-04: URIs for Assertion IDs]

Should URIs be used as identifiers in assertions?

Background...

From the focus group minutes [1]:

> >- URIsForAssertionIDs: What are the pros and cons? What other
>
> > methods are there?
>
>
> DS-4-04: URIs for Assertion IDs: (still open after today)
>
>
> Eve, with help from Dave, gave a short tutorial on the problems with
>
> URI identity in XML namespace names.

There followed a brief discussion in which we touched upon various aspects of this problem space. We terminated the discussion upon issuing the above "new action". (the discussion as-documented in the aforementioned minutes is attached below for reference [1])

Further background, in the form of the specs for AssertionID and Issuer from draft-sstc-core-07 are excerpted at [2].

Relevant, recent discussion on security-services@lists.oasis-open.org...

Hal said in

http://lists.oasis-open.org/archives/security-services/200105/msg00146.html

> 5. In 1.3.1 I don't understand the intended purpose of AssertionID.

PHB replied in

http://lists.oasis-open.org/archives/security-services/200105/msg00159.html

> The AssertionID provides a unique reference for the assertion. ...
>
> Within SAML 1.0 the principle use of an AssertionID would be to allow
>
> one assertion to reference another (see previous Tim discussion) thus
>
> allowing statements of the form `this assertion was constructed from
>
> that assertion'.

> The principle use of the AssertionID however would be in systems built
>
> around SAML, they provide the basis for audit and accountability for

> example. If a system is built that allows for second order logic
>
> (assertions may be true or false and other assertions may make
>
> statements about validity (c.f. TASS meta-assertions)), then an
>
> assertionID is essential.

Analysis...

The stated purpose of the AssertionID element is as an "assertion unique identifier" [2]. The stated syntax of this identifier is a URI [3]. Implicit in this line of thinking is a notion that URIs may be created (aka "minted") in a globally decentralized, non-colliding fashion due to the properties of the URI "space" [4].

The following is stated in [2] about AssertionID..

> The URI is used as a name for the assertion and not as a locator. It
>
> is only necessary to ensure that no two assertions share the same
>
> identifier. Provision of a service to resolve an identifier into an
>
> assertion is not a requirement.

Also, as far as I can tell, [2] postulates (in section 1.3) that a requester need supply only an assertionID in a SAMLQuery in order to obtain an assertion. It does not make clear any distinction between newly minting an assertion and retrieving an already-existing one.

Thus it seems that there is a tacit assumption in [2] that an assertion may be uniquely identified and minted/retrieved using only an assertionID, regardless of the quote above.

So it seems that an assertionID is being asked to both..

A. identify, globally and uniquely, assertions;

B. provide at least a hint about where to direct requests for minting

or retrieving assertions.

..but again, this is to a fair degree inferred from a rough, incomplete, draft spec ([2]).

Additionally, there are many subtleties to using URIs as identifiers rather than straight-ahead resoure locators. See the minutes of the "Future of URIs" Birds of the Feather session held at the 50th IETF meeting [11],

Thoughts...

It is an arguably good design principle to separate functions between various data items such that their roles in life are unambiguous.

[2] already has an "Issuer" assertion element. If identifying assertions is predicated on using the tuple "assertionID, Issuer", and some method for guaranteeing non-colliding Issuer names is used (e.g. DNS domain names, and things built upon them), then the assertionID can be quite simple, e.g. an integer (as is done in PKIX [10]).

In using the "assertionID, Issuer" tuple to identify assertions, and also provide guidance about where to go to make requests about or for them, the role of the Issuer element may arguably be (too) overloaded. E.g. if the overall SAML design calls for assertions to (perhaps optionally) specify within their structure where a receiver of an assertion may go to make queries about the assertion, then the requirements for persistence and location-independence for that particular identifier may conflict with the requirements of simply globally and uniquely (and perhaps persistently) identifying the Issuer security domain.

So it may be the case that to..

case 1) globally uniquely identify an assertion one needs the combination of "assertionID, Issuer",

case 2) uniquely identify assertions in the context of a given security domain, one needs only "assertionID" (it doesn't need to be disambiguated from assertions from other security domains; in this case the assertionID starts to look a lot like a serial number),

case 3) one needs to cover either of the prior cases, and also needs to specify where to go (and "how" to "go") to make requests to the security domain in question. I.e...

```
  <assertionID>123123123123</assertionID>

  <Issuer>some-issuer-identifier</Issuer>  -- perhaps optional

  <Source>saml://example.org/send-yer-SAML-based-requests-here   -- optional

  </Source>
```

Tho there are good arguments for not making Issuer optional (case 2), thus the overall set of identifying information might be structured something like this..

```
  <assertionID>

    <serialNumber>123123123123</serialNumber>

    <Issuer>some-issuer-identifier</Issuer>

  </assertionID>

  <Source>saml://example.org/send-yer-SAML-based-requests-here   -- optional
```

</Source>

Further thoughts...

There's tons of subtle-but-important details in all of this that need to be considered in nailing down a design. Some of them are..

D1. if one uses a URL or URL-like flavor of URI as an identifier, we need to specify how comparisons between said identifier and other blobs of data are made. [3] details some of these subtleties in sections 1.5 and 2.1. The lowest-common-denominator option of specifying that such comparisons are made by performing a byte-by-byte octet string comparison will only technically work if certain restrictions are specified for the URI-based values. The SAML specs may need to consider/specify/incorporate one or more or all of..

* charset restrictions for all or some SAML elements,

* charset specifications, and bounds on said specifications, for SAML

elements whose value syntaxes are URI [3],

* charset(s) specified/allowed by underlying protocols and interaction

thereof with the prior items in this list,

* [perhaps others/more]

Of note is "Character Model for the World Wide Web 1.0" [14] which defines an algorithm called "String Identity matching" (in section 6), which has implications for the above. (it also has implications for SAML in general, see D6).

D1.1. See also [16] [17] for further musing about internationalization for URI and other identifiers.

D1.2. See also "Considerations for URI and FQDN Protocol Parameters" [18] for further musings about using DNS domain names and/or URI as identifiers in protocol elements.

D1.3. If URI are used as identifiers in protocol elements, software modules that handle them (this includes people as a boundary condition ;) may wonder just what the heck their semantics are, because their semantics can be so varied. "URI Relationship Discovery via RESCAP" [19] touches upon and enumerates these questions, as well as sketch a protocol-based approach that specifies a service providing such info. Additionally, the more recent I-D, "URI Resolution using the Dynamic Delegation Discovery System" [20], also provides some relevant background info.

D1.4. Registration issues -- URI (nee URL) schemes should be registered, same with URN namespaces. See [9] for pointers to relevant RFCs on how to accomplish such registrations.

D2. some-issuer-identifier -- should this simply be a DNS fully-qualified-domain-name? Should it be a URN [6]? Should it be something else?

D3. use of URNs -- URNs have semantics of persistence and location-independence. Their use may or may not be appropriate in the context of SAML assertions depending upon the semantics of the thing they're being called upon to identify [6] [7]. E.g. it is questionable to use a URN to identity a given non-persistent, indeed likely ephemeral, artifact such as an instantiation of a SAML assertion. However, it is

D4. if URNs are used, what namespace identifiers are appropriate? Any? Only a selected one(s)? Formal or informal? [7] [12]

D5. the DOI work [13] is likely not appropriate for SAML's purposes due to that effort's Intellectual Property emphasis and also because of the implied (required?) dependency upon the Handle System. The latter is an nascent, intended-to-be-scalable-to-the-Internet, naming and name resolution system [13] (I haven't yet read the internet-drafts in detail).

D6. The emergent "Character Model for the World Wide Web 1.0" MAY have various implications for SAML's specification, beyond that noted in D1.

D7. IMHO, "tag:" URIs [15] are not appropriate for our problem space, given their present specification, but reading about them and the discussion thereof on the uri@w3.org list is educational.

D9. If an artifact is not persistent, then it's identifier may be reused under certain conditions. Something to keep in mind and think about.

Notes and References...

[1] URIsForAssertionIDs discussion, from Focus subgroup concall, 22-May-2001:

http://lists.oasis-open.org/archives/security-services/200105/msg00139.html

>- URIsForAssertionIDs: What are the pros and cons? What other methods

>   are there?

DS-4-04: URIs for Assertion IDs: (still open after today)

Eve, with help from Dave, gave a short tutorial on the problems with URI identity in XML namespace names.

Thomas: The DOI people are working on this general problem. (http://www.doi.org, http://www.handle.net/)

Eve: It would be acceptable to use URIs if we apply constraints. E.g., they should be absolute (or even should be absolute URNs) and we should define what equality means. Dave: Solving the "whole URI problem" is way bigger than SAML's scope.

Jeff: There was recently an IETF BOF on the future of URIs, and W3C was investigating these issues, but nothing has really happened.

Eve: See W3C's Character Model spec for recommendations on normalization and internationalized URIs. (http://www.w3.org/TR/charmod/)

Dave: Cautioned that we have to be concerned with real-world websites and their behavior, which is not precisely the same as the standards. For example, http://www.jamcracker.com and http://www.jamcracker.com/index.html point to the same resource, but how can people know that?

BobB: Aliases, symbolic links, etc. are a problem if you have policies on different aliases that conflict.

Hal: We can take a hard line on URIs for assertion IDs, but for resources, we may have to deal with the vagaries of real-world URIs.

Evan: URIs are opaque strings, and XML makes data's structure more transparent.

Hal: There will probably be more cases than just AssertionID where identifiers will have properties of uniqueness (RequestID?) and are just "internal to SAML." We should pull out the description of these properties into a separate section and have it referred to from the various sections.

Hal: We should register a new URI scheme, e.g. "saml:" Thomas: We could

just use URNs and have the same effect. Jeff: It's pretty easy to register

a new scheme with IANA. (http://www.ietf.org/rfc/rfc2717.txt)

Eve: It's surprisingly hard to register a new URN namespace (http://www.ietf.org/rfc/rfc2611.txt)

NEW ACTION: Jeff to send out email about possible URI constraints and identity definitions we should consider imposing in the case of SAML's unique identifiers.

[2] from draft-sstc-core-07: http://www.oasis-open.org/committees/security/docs/draft-sstc-core-07.pdf

> 1.4.2 Element <AssertionID>

>

> Each assertion MUST specify exactly one unique assertion identifier.

> All identifiers are encoded as a Uniform Resource Identifier (URI)

> and are specified in full (use of relative identifiers is not

> permitted).
>
> The URI is used as a name for the assertion and not as a locator. It
> is only necessary to ensure that no two assertions share the same
> identifier. Provision of a service to resolve an identifier into an
> assertion is not a requirement.
>
> The following schema defines the <AssertionID> element:
>
> <element name="AssertionID" type="string"/>
>
>
> 1.4.3 Element <Issuer>
>
> The Issuer element specifies the issuer of the assertion by means of a
> URI. It is defined by the following XML schema:
>
> The following schema defines the <Issuer> element:
>
> <element name="Issuer" type="string"/>

[3] Uniform Resource Identifiers (URI): Generic Syntax http://www.ietf.org/rfc/rfc2396.txt

[4] URIs encompass both URLs and URNs. The former [5] often (but not always) depend upon the Domain Name System (DNS) namespace, which enables the capability to mint globally unique URLs in a decentalized fashion. The latter [6] define a hierarchical namespace that is DNS-independent but centrally mediated [7] in order to provide "location independent identification of a resource, as well as longevity of reference".

`This picture is from [8]...`

```
 ____________________________________________________________
|                                                            |
|         _________________                                  |
|        |  ftp:            |                                 |
|        |  gopher:         |                                 |
|        |  http:         __|_____________                    |
|        |  etc          |  |  urn:        |                  |
|        |_______________|__|              |                  |
|                URLs    |                 |                  |
|                        |_________________|                  |
|                               URNs                          |
|____________________________________________________________|
                         URIs
```

URIs, URLs, and URNs are described by a plethora of documents. An attempt to tie them all together is given in [9].

[5] Uniform Resource Locators (URL) http://www.ietf.org/rfc/rfc1738.txt

[6] URN Syntax http://www.ietf.org/rfc/rfc2141.txt

[7] URN Namespace Definition Mechanisms http://www.ietf.org/rfc/rfc2611.txt

[8] Naming and Addressing: URIs, URLs, ...http://www.w3.org/Addressing/

[9] Uniform Resource Identifiers: Comprehensive Standard http://www.ietf.org/internet-drafts/draft-daigle-uri-std-01.txt

[10] PKIX Certificate and CRL Profile http://www.ietf.org/rfc/rfc2459.txt

[11] Future of Uniform Resource Identifiers BOF (furi) [50th IETF, Minneapolis MN, Mar-2001] http://www.ietf.org/proceedings/01mar/ietf50-39.htm#TopOfPage

[12] URI.NET -- a clearing house for information on URIs in general and on specific URI schemes and software http://www.uri.net/

[13] Digital Object Identifiers, The Handle System http://www.doi.org, http://www.handle.net/

[14] Character Model for the World Wide Web 1.0 http://www.w3.org/TR/charmod/

[15] "Tag" URI Scheme http://www.taguri.org/ see also the thread on uri list "Proposal: 'tag' URIs", from Tim Kindberg <timothy@hpl.hp.com>...http://lists.w3.org/Archives/Public/uri/2001Apr/0013.html

http://www.taguri.org/2001-04-26/draft-kindberg-tag-uri-00.txt

[16] Internationalization: URIs and other identifiers http://www.w3.org/International/O-URL-and-ident.html

[17] Internationalized Resource Identifiers (IRI) http://www.ietf.org/internet-drafts/draft-

masinter-url-i18n-07.txt

[18] Considerations for URI and FQDN Protocol Parameters http://www.ietf.org/internet-drafts/draft-eastlake-uri-fqdn-param-00.txt

[19] URI Relationship Discovery via RESCAP http://www.ietf.org/internet-drafts/draft-mealling-uri-rdf-00.txt

[20] URI Resolution using the Dynamic Delegation Discovery System http://www.ietf.org/internet-drafts/draft-ietf-urn-uri-res-ddds-03.txt

Status: Open

Group 5: Reference Other Assertions

A number of requirements have been identified to reference an assertion with in another assertion or within a request.

Phillip Hallam-Baker observes: “there is more than one way to support this requirement,

“[A] The first is to simply cut and paste the assertion into the <Subject> field so we have <Subject><Assertion><Claims><Subject>[XYZ]. This approach is simple and direct but does not seem to achieve much since it essentially comes down to ‘you can unwrap this structure to find the information you want’. Why not just cut to the chase and specify <Subject>[XYZ] ?

“[B] The problem with cutting to the chase is that it means that the application is simply told the <subject> without any information to specify where that data came from. In many audit situations one would need this type of information so that if something bad happens it is possible to work out exactly where the bogus information was first introduced and how many inferences were derived from it. So we might have <Subject><AssertionRef>[XYZ]

“[C] The above is my preferred representation since the assertion can be used immediately by the simplest SAML application without the need to dereferrence the assertion reference to discover the subject of the assertion. However one could argue that an application might want to specify simply <Subject><AssertionRef> and then specify the referenced assertion in the advice container.

“I think that the choice is really between [B] and [C] since the first suggestion in [A] is unwieldy and the second is simply the status quo.

“Of these [B] is more verbose, [C] requires applications to perform some pointer chasing and could be seen as onerous.”

The following four scenarios have been identified where this is required:

ISSUE:[DS-5-01: Dependency Audit]

One issue with draft-sstc-core-07.doc is a lack of support for audit of assertion dependency between co-operating authorities. As one explicit goal of SAML was to support inter-domain security (i.e., each authority may be administered by a separate business entity) this seems to be a serious "gap" in reaching that goal.

Consider the following example:

(1) User Ravi authenticates in his native security domain and receives

Assertion A:

```
          <Assertion>
      <AssertionID>http://www.small-company.com/A</AssertionID>
      <Issuer>URN:small-company:DivisionB</Issuer>
      <ValidityInterval> . . . </ValidityInterval>
      <Claims>
        <subject>"cn=ravi, ou=finance, id=325619"</subject>
        <attribute>manager</attribute>
      </Claims>
    </Assertion>
```

(2) User Ravi authenticates to the Widget Marketplace using assertion A and based on the policy:

All entities with "ou=finance" authenticated thru small-company.com with attribute manager have purchase limit $100,000 receives Assertion B from the Widget Marketplace:

```
          <Assertion>
     <AssertionID>http://www.WidgetMarket.com/B<AssertionID>
     <Issuer>URN:WidgetMarket:PartsExchange</Issuer>
     <ValidityInterval>. . . </ValidityInterval>
     <Claims>
       <subject>"cn=ravi, ou=finance, id=325619"</subject>
       <attribute>max-purchase-limit-$100,000</attribute>
     </Claims>
   <Assertion>
```

(3) User Ravi purchases farm machinery from a parts provider hosted at the Widget Marketplace. The parts provider authorizes the transaction based on Assertion B.

Even though Assertion B has been issued by the Widget Marketplace in response to assertion A (I guess another way to look at this to view assertion A as the subject of B as in [1]) there is no way to represent this information within SAML.

If there is a problem with Ravi's purchases at the Widget Marketplace (Ravi wont pay his bills) there is nothing in the SAML flow that ties Assertion B to Assertion A. This appears to be a significant missing piece to me.

Status: Open

ISSUE:[DS-5-02: Authenticator Reference]

The authenticator element of an assertion should be able to reference another assertion, used solely for authentication.

Status: Open

ISSUE:[DS-5-03: Role Reference]

The role element should be able to reference another assertion that asserts the attributes of the role.

Status: Open

ISSUE:[DS-5-04: Request Reference]

There should be a way to reference an assertion as the subject of a request. For example, a request might reference a Attribute Assertion and ask if the subject of that assertion could access a specified object.

Status: Open

Group 6: Attributes

ISSUE:[DS-6-01: Nested Attributes]

Should SAML support nested attributes? This means that for example, a role could be a member of another role. This is one standard way of distinguishing the semantics of roles from groups.

There are many issues of semantics and pragmatics related to this. These include:

1. Limit of levels if any
2. Circular references
3. Distributed definition
4. Mixed attribute types.

Status: Open

ISSUE:[DS-6-02: Roles vs. Attributes]

Should Attributes and Roles be identified as separate objects?

Status: Open

ISSUE:[DS-6-03: Attribute Values]

Should Attributes have some ‘attribute-value’ type structure to them?

Status: Open

ISSUE:[DS-6-04: Negative Roles]

Should there be a way to state that someone does not have a role?

Status: Open

Group 7: Authentication Assertions

ISSUE:[DS-7-01: AuthN Datetime]

An Authentication Assertion should contain the date and time that the Authentication occurred. This could be done by explicitly assigning this meaning to the IssueInstant or NotBefore elements or create a new element containing a datetime.

Possible Resolutions:

1. Use IssueInstant in a AuthN Assertion to indicate datetime of AuthN.
2. Use NotBefore in a AuthN Assertion to indicate datetime of AuthN.
3. Create a new element to indicate datetime of AuthN.

Status: Open

ISSUE:[DS-7-02: AuthN Method]

An element is required in AuthN Assertions to indicate the method of AuthN that was used. This could be a simple text field, but the values should be registered with some central authority. Otherwise different identifiers will be created for the same methods, harming interoperability.

Status: Open

ISSUE:[DS-7-03: AuthN Method Strength]

SAML has identified a requirement to indicate that a negative AuthZ decision might be changed if a “stronger” means of AuthN was used. In support of this it is useful to introduce the concept of AuthN strength. AuthN strength is an element containing an integer representing strength of AuthN, where a larger number is considered stronger. Individual deployments could assign numbers to particular AuthN methods according to their policies. This would allow an AuthZ policy to state that the required AuthN must exceed some value.

Possible Resolutions:

1. Add an AuthN strength element.
2. Do not add an AuthN strength element.

Status: Open

Group 8: Authorities and Domains

The following points are generally agreed.

- An Assertion is issued by an Authority.
- Assertions may be signed.
- The name of a subject must be qualified to some security domain.
- Attributes must be qualified by a security domain as well.
- Nigel Edwards has suggested that resources also need to be qualified by domain.

ISSUE:[DS-8-01: Domain Separate]

Stephen Farrell has pointed out that there may be a requirement to encrypt, for example, the user name but not the domain. Therefore they should be in separate elements. If domains are going to appear all over the place, maybe we need a general way of having element pairs or domain and "thing in domain."

Possible Resolutions:

1. Domains will always appear in a distinct element from the item in the domain
2. The domain and item may be combined in a single element.

Status: Open

ISSUE:[DS-8-02: AuthorityDomain]

Should SAML take any position on the relationship between the 1) Authority, 2) the entity that signed the assertion, and 3) the various domains scattered throughout the assertion? For example, the Authority and Domain could be defined to be the same thing. Alternatively, Authorities could assert for several domains, but each domain would have only one authority. Another possibility would be to require that the domain asserted for be the same as that found in the Subject field of the PKI certificate used to sign the assertion.

The contrary view is that is a matter for private arrangement among asserting and relying parties.

Status: Open

Group 9: Request Handling

ISSUE:[DS-9-01: AssertionID Specified]

SAML should define the responses to requests that specify a particular AssertionID. For example,

- What if the assertion doesn’t exist or has expired?
- What if the assertion contents do not match the request?
- Is it ever legal to send a different assertion?

Status: Open

Group 10: Assertion Binding

ISSUE:[DS-10-01: AttachPayload]

There is a requirement for assertions to support some structure to support their "secure attachment" to payloads. This is a blocking factor to creating a SOAP profile or a MIME profile. If needed, the bindings group can make a design proposal in this space but we would like input from the broader group.

Status: Open

Miscellaneous Issues

Group 1: Terminology

ISSUE:[MS-1-01: MeaningofProfile]

The bindings group has selected the terminology:

- SAML Protocol Binding, to describe the layering of SAML request-response messages on "top" of a substrate protocol, Example: SAML HTTP Binding (SAML request-response messages layered on HTTP).
- a profile for SAML, to describe the attachment of SAML assertions to a packaging framework or protocol, Example: SOAP profile for SAML, web browser profile for SAML

This terminology needs to be reflected in the requirements document, where the generic term "bindings" is used. It needs also to be added to the glossary document.

The conformance group has used the term Profile to define a set of SAML capabilities, with a corresponding set of test cases, for which an implementation or application can declare conformance. This use of profile is consistent with other conformance programs, as well as in ISO/IEC 8632. In order to resolve this conflict, the conformance group has proposed, in sstc-draft-conformance-spec-004, to substitute the word partition instead.

Status: Open

Group 2: Administrative

ISSUE:[MS-2-01: RegistrationService]

There is a need for a permanent registration service for publishing bindings and profiles. The bindings group specification will provide guidelines for creating a protocol binding or profile, but we also need to point to some form of registration service.

DS-7-02: AuthN Method also implies a need to register AuthN methods.

How can we take this forward? Is OASIS wiling to host a registry?

Another possibility is IANA.

Status: Open

Document History

- 5 Feb 2001 First version for Strawman 2.
- 26 Feb 2001 Made the following changes:
    - Changed references to [SAML] to SAML.
    - Added rewrites of Group 1 per Darren Platt.
    - Added rewrites of Group 3 per David Orchard.
    - Added rewrites of Group 5 per Prateek Mishra.
    - Added rewrites of Group 11 per Irving Reid.
    - Converted the abbreviation "AuthC" (for "authentication") to "AuthN."
    - Added Group 13.
    - Added UC-1-12:SignOnService.
    - Converted candidate requirement naming scheme from [R-Name] (as used in the main document) to [CR-issuenumber-Name], per David Orchard.
    - Added UC-0-02:Terminology.
    - Added UC-0-03:Arrows.
    - Updated UC-9-02:PrivacyStatement with suggested requirements from Bob Morgan and Bob Blakley.
    - Added UC-1-13:ProxyModel per Irving Reid.
    - Added status indications for each issue.
    - Recorded votes and conclusions for issue groups 1, 3, and 5.
    - Added Zahid Ahmed's use cases for B2B transactions.
    - Added Maryann Hondo's use case scenario for ebXML.
    - Added comments to votes by Jeff Hodges, Bob Blakley.
- 10 Apr 2001 Made the following changes:
    - Added re-written versions of issue group 2, 3, 6, 7, 8, 9, 10, and 13 by Darren Platt and Evan Prodromou.

  - Added re-written versions of issue groups 11 and 12 by Irving Reid.
  - Added re-written version of issue group 4 by Prateek Mishra.
  - Added voting results for groups 2, 3, 4, 6, 7, 8, 9, 10, 11, 12, and 13.
- 22 May 2001 Made the following changes:
    - Changed introduction to reflect conversion to general issues list
    - Added color scheme
    - Closed large number of issues per F2F #2
    - Changed OSSML to SAML everywhere
    - Added design issues section and groups 1-4
    - Added UC-13-07
    - Various minor edits
- 25 May 2001 Made the following changes
    - Various format improvements
    - Closed all Group 0 issues
    - Added DS-4-04
    - Did NOT promote blue issues to gray
- 11 June 2001 Made the following changes
  - Various format improvements, CLOSED in headers
  - Renumber Anonymity to DS-1-02 (was a duplicate)
  - Changed all Blue to Gray
  - Downgraded from Yellow to White UC-13-07, DS-1-01, DS-1-02, DS-4-02 (no recent discussion)
  - Closed DS-2-01 Wildcarded Resources
  - Added new text for DS-3-01, DS-3-02, DS-4-04
  - Added DS-2-02, Groups 5,6,7,8 and 9

- 18 June 2001 Made the following changes
  - Changed from Blue to Gray DS-2-01
  - Downgraded from Yellow to White UC-13-07, DS-2-02, DS-3-01, DS-3-02, DS-3-03, DS-6-01, DS-6-02, DS-6-03, DS-6-04, DS-7-01, DS-7-02, DS-7-03, DS-8-01, DS-8-02, DS-9-01
  - Created Miscellaneous Issues section, added MS-1-01 and MS-2-01
  - Created issue DS-10-01
  - Modified DS-4-01 & DS-4-03