# SAML Version 2.0 Scope and Work Items

## Working Draft 1~~7~~8, ~~5 April~~3 May 2004

**Document identifier:**

sstc-saml-scope-2.0-draft-1~~7~~8

**Location:**

http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

**Previous draft:**

http://www.oasis-open.org/committees/download.php/6113/sstc-saml-scope-2.0-draft-16-diff.pdf

**Editors:**

Scott Cantor, individual (cantor.2@osu.edu)
Prateek Mishra, Netegrity (pmishra@netegrity.com)
Eve Maler, Sun Microsystems (eve.maler@sun.com)

**Abstract:**

This non-normative document describes the scope of the V2.0 work of the OASIS Security Services Technical Committee (SSTC), including candidate work items and their status.

**Status:**

Revision 1~~7~~8 reflects the results of work done during April 2004~~the F2F meeting held 30 March to 1 April 2004 in Austin, TX~~. W-5, W-6, and W-7 were completed; W-15 was made inactive (though parts of it were completed in V2.0); notes for active work item were updated; and the official OASIS notice was added as an appendix.

# 1 Scope of the V2.0 Work

The SAML 2.0 effort intends to deliver on the following goals:

- Address issues and enhancement requests that have arisen from experience with real-world SAML implementations and with other security architectures that use SAML.
- Adding support for features that were deferred from previous versions of SAML.
- Develop an approach for unifying various identity federation models found in real-world SAML implementations and SAML-based security architectures.

## Design Principles

At its October 2003 face-to-face meeting, the TC ranked its design principles for the V2.0 roughly as follows:

- Must meet the schedule
- (Equally) Must meet the accepted use cases
- Retain the existing domain model (i.e., restructuring not acceptable; additions are acceptable)
- Clean versioning path from 1.x to 2.0 and beyond
- Selective backwards compatibility where it doesn't conflict with other goals

The TC also listed design non-principles:

- Minimally invasive to the 1.x design
- Overall backwards compatibility
- Maximally elegant design

# 2 Work Items

We are taking a use-case-based approach for each new area of functionality. The owner for each work item makes a proposal containing at least one use case and definitions of any new terms, possibly along with formal requirements. (Use cases for a priori accepted items are welcome too.) On acceptance of a use case, the owner is expected to make a proposal for SAML technology that solves the use case. (Others may submit proposals as well.) The work item table uses the following status values and colors.

> **Note:** Where it is noted in this section that solution proposals have been "accepted", design features may still change in accordance with TC wishes. Accepted solution proposals are typically just starting points for further refinement.

| Status: Color | Description | Work Items |
|---|---|---|
| Active: **green** on white background | Targeted for SAML V2.0; specs not yet feature-complete | W-2a, W-4, ~~W-5, W-6, W-7,~~ W-9, W-14, ~~W-15,~~ W-25, W-27, W-30 |
| Reassess: **orange** on light gray background | For non-core functionality that we may decide to include in V2.0 as we go | (none) |
| Liaison: **purple** on yellow background | For functionality farmed out to other efforts | W-18, W-20 |
| Inactive: **red** on gray background | Not considered part of the V2.0 work, but may be picked up later | W-5b, W-10, W-11, W-12, W-13, W-15 (but see below), W-16, W-17, W-22, W-23, W-24, W-26, W-28, W-28c |
| Completed: **black** on green background | Was previously active, but has now been fully implemented in the specifications; this does not preclude further discussion by the TC on technical particulars of the specs or further issues being reported by TC members or others | W-1, W-2, W-3, W-5, W-5a, W-6, W-7, W-8, portions of W-15, W-19, W-21, W-28a1, W-28a2, W-28b, W-28d, W-29 |

Documents in the SAML repository are referenced here by document ID root (for example, "draft-sstc-session-management") and download ID number (for example, "3659"). To retrieve the document, add the download ID number to the end of the following base URI:

http://www.oasis-open.org/committees/download.php/

For example:

http://www.oasis-open.org/committees/download.php/3659

Mail messages are referenced here by message month and ID. To retrieve a message, add the citation string to the following base URI (this link takes you to the whole mail archive):

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

For example:

http://lists.oasis-open.org/archives/security-services/200310/doc00001.doc

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-1** Completed | John Kemp | **Session Support**<br><br>Keywords: profiles, SSO, sessions, logout<br><br>Global signout and similar would be considered simple sessions. Complex sessions would include things like global timeout. Boeing has provided input on their requirements around this. | Base use case (accepted in principle): support for sessions as found in liberty-architecture-overview-v1.1.pdf (**3895**) Sections 3.2.4 and 5.6<br><br>Advanced use case (needs to be voted on): support for time-out and session linking as discussed in draft-sstc-session-management and mail message **200310/doc00001.doc**<br><br>John K.'s further elucidation of use cases, resulting in a P1 through P5: message **200312/msg00038.html**<br><br>All of P1 through P5 were accepted on 9 December 2003 (see message **200312/msg00054.html** ), with the understanding that a logically separate session authority would be specified. If this imposes too much of a design burden, we may reconsider.<br><br>Solution proposal: See liberty-architecture-protocols-schema-v1.1.pdf (**3896**) Sections 3.2 and 3.5; also message **200402/msg00013.html** and draft-sstc-kemp-sessions-proposal-01.pdf (**5256**)<br><br>Original issues: See sstc-saml-1.1-issues-draft-02 (**3690**) UC-3-01, UC-3-08, UC-3-09, DS-13-01<br><br>Additional input: see Boeing input in message **200308/msg00008.html**<br><br>Motion to “Incorporate ID-FF v1.2 logout protocol, with extension into SAML v2.0” was accepted at F2F on 3-5 Feb 2004; see message **200402/msg00123.html**<br><br>Discussion on timeout feature has not been resolved/decided yet |

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-2**<br>Completed | Scott Cantor<br>John Linn | **Identity Federation**<br><br>Keywords: account linking, pseudonyms, SSO, privacy<br><br>NameIdentifier Exchange between sites.<br><br>Peristent pseudonyms for principals.<br><br>This should also include privacy and anonymity features à la Shibboleth and Liberty. This should include the notion of an anonymous name identifier. It was noted that Liberty V1.2 has anonymity features. | Base use case: support as described in liberty-architecture-overview-v1.1.pdf (**3895**) Sections 3.2.1 and 5.4<br><br>Extension use case: includes use of "one-time" identifier as discussed in mail message **200310/doc00002.doc**<br><br>Sum of these use cases accepted on 9 December 2003; see message **200312/msg00054.html**<br><br>Solution proposal: draft-sstc-nameid (**4587**); also see liberty-architecture-protocols-schema-v1.1.pdf (**3896**) Sections 3.2, 3.3, and 3.4, along with the Shibboleth architecture at http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v05.pdf. SAML core spec (sstc-saml-core-2.0-draft-05, **5519**) now contains a nearly complete solution proposal, which was accepted at F2F on 3-5 Feb 2004; see message **200402/msg00123.html**<br><br>Original issues: see sstc-saml-1.1-issues-draft-02 (**3690**) DS-1-02 |
| **W-2a**<br>Active | Prateek Mishra | **SSO with Attribute Exchange**<br><br>Keywords: attributes<br><br>This can be used to achieve a kind of federation without using an account-linking model. This may have some impact on W-12. | Use case proposal: sstc-sso-attribute-exchange (**3966**)<br><br>Use case accepted on 9 December 2003; see message **200312/msg00054.html**<br><br>Additional input: see Boeing input in message **200308/msg00008.html**<br><br>Solution proposal: mail message **200401/msg00079.html**<br><br>Discussion at F2F on 3-5 Feb 2004 (see message **200402/msg00123.html** ) resulted in an instruction to describe use cases more thoroughly for comparison with existing ID-FF solutions to see if there's already a match |

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-3** Completed | Jahan Moreh | **Metadata and Exchange Protocol**<br><br>Keywords: metadata, interoperability, discovery, trust<br><br>This work has already begun. It should include SAML feature discovery through a WSDL file. SAML metadata might want to include a way to discover supported types of authentication protocols, as outlined in closed issue DS-7-06. | Use case proposals: sstc-cantor-w3-metadata (**4122**) and **200311/msg00018.html**<br><br>Use cases accepted on 9 December 2003; see message **200312/msg00054.html**<br><br>Solution proposals: now in a spec draft: sstc-saml-metadata-2.0-draft (**5960**) ; also see liberty-architecture-protocols-schema-v1.1.pdf (**3896**) Section 4, along with the Shibboleth architecture at http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v05.pdf<br><br>Original issues: see sstc-saml-1.1-issues-draft-02 (**3690**) DS-7-06, MS-5-08<br><br>At F2F on 3-5 Feb 2004; see message **200402/msg00123.html**, items at sstc-cantorandmoreh-w3 (5260) were discussed; proposal to consider ID-FF V1.2 metadata as basic of SAML V2.0 (removing Liberty-specific references) was accepted |
| **W-4** Active | Jahan Moreh | **Profile Enhancements for Metadata**<br><br>Keywords: protocol, metadata<br><br>Implications for the profiles (and profile creation guidelines) regarding metadata usage. | Use cases are covered by W-3.<br><br>Solution proposal: sstc-saml-MetadataInBindings-2.0-draft (**3697**)<br><br>As of the F2F on 3-5 Feb 2004 (see message **200402/msg00123.html** ), we are waiting until the metadata spec is stable to go back and enhance the profiles as necessary (including any new profiles done by then) |

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-5** ~~Active~~Completed **(see also W-5a, W-5b, W-17, W-25)** | Prateek Mishra | **SSO Profile Enhancements**<br><br>Keywords: profiles, SSO, metadata, discovery, authentication<br><br>Richer SSO profiles, including (signed) requests from destination sites, control over authentication, passivity, extensibility, and source site discovery. Boeing has provided input on their requirements around "destination site first" scenarios.<br><br>Candidate solution should reference both Liberty and SAML 1.1 draft. Need to conduct survey of "typical" data items transfer from SP to IdP. | Use case: Add flows from SP to IdP as discussed in mail message **200310/msg00162.html**<br><br>Use cases accepted on 9 December 2003 (see message **200312/msg00054.html**).<br><br>Need to choose profile extensions among W-5 and W-5a that we want to cover.<br><br>Solution proposal: sstc-bindings-extensions (**3893**); see also liberty-architecture-protocols-schema-v1.1.pdf (**3896**) Section 3.2, liberty-architecture-bindings-profiles-v1.1.pdf (**3898**), the Boeing input in message **200308/msg00008.html**, and the Shibboleth architecture at http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v05.pdf<br><br>Use cases accepted.<br><br>Proposal at message **200402/msg00013.html** accepted at F2F on 3-5 Feb 2004; see message **200402/msg00123.html**<br><br>Design work for this related set of items ~~is largely taking~~ took place in the area of AuthnRequest/Response; see solution proposal at thread starting at message 200402/msg00047.html and other threads in month 200402/threads.html. The core-08ff drafts contain the final work on this protocol. |

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-5a** Completed (see also **W-5**, **W-5b**, **W-17**, **W-25**) | Frederick Hirsch | **Enhanced Client Profiles**<br><br>Keywords: profiles, clients<br><br>Some profiles rely on enhanced clients and proxies ("Liberty-enabled client" or LECP). This might need enhancement to account for general considerations of clients that are web services, and also non-mobile clients. | Use case: 03-09-18-lecp-proposal (**3802**)<br><br>See also additional input in Fidelity presentation (**3585**)<br><br>Use case accepted on 9 December 2003; see message **200312/msg00054.html**<br><br>Solution proposals: hirsch-sstc-lecp-draft (**4641**), hirsch-paos-lecp-draft (**4948**)<br><br>Proposal to adopt LECP and PAOS+LECP proposal and integrate into SAML 2.0 Bindings and Profiles spec accepted at F2F on 3-5 Feb 2004; see message **200402/msg00123.html**; implemented in the newly separated Bindings spec (sstc-saml-bindings-2.0, **5489** ) and Profiles spec (sstc-saml-profiles-2.0, **5510** ) |
| **W-5b** Inactive (see also **W-5**, **W-5a**, **W-17**, **W-25**) | Tony Nadalin, Jeff Hodges | **SOAP Client Profile** | Use case: mail message **200310/doc00003.doc**<br><br>Use case accepted on 9 December 2003; see message **200312/msg00054.html**<br><br>Additional use cases and beginnings of solution proposal: draft-sstc-solution-profile-soap (**5330**)<br><br>See also additional input in Fidelity presentation (**3585**)<br><br>See also details in W-17, which has been merged in with this<br><br>Discussion at F2F on 3-5 Feb 2004 (see message **200402/msg00123.html** ); some new use cases presented late in the cycle don't seem to have consensus yet<br><br>During the telecon of 2 March 2004, IBM withdrew the work item for V2.0 consideration |

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-6** ~~Active~~Completed | Scott Cantor | **Proxied SSO**<br><br>Keywords: profiles, SSO, intermediaries<br><br>Liberty 1.2 adds dynamic proxying into the SSO profiles, including non-Liberty services. | Use case: sstc-cantor-w6-proxy (**4388**)<br><br>Use case accepted on 9 December 2003; see message **200312/msg00054.html**<br><br>See liberty-architecture-protocols-schema-v1.1.pdf (**3896**) and the Liberty V1.2 dynamic proxying capability described at http://www.projectliberty.org/specs/liberty-idff-protocols-schema-v1.2.pdf Section 3.2.2.7<br><br>Discussion at F2F on 3-5 Feb 2004 (see message **200402/msg00123.html** ); ~~need to~~ final design reflected in ~~track progress in~~ the AuthnRequest/Response ~~to close this~~protocol, which was completed in revs core-08ff. |
| **W-7** Completed ~~Active~~ | Scott Cantor | **Discovery Protocol**<br><br>Keywords: discovery, metadata<br><br>For example, this includes common domain and cookie mechanisms. | Use case for finding an IdP when at an SP: liberty-architecture-overview-v1.1.pdf (**3895**) Section 5.5<br><br>Use case accepted on 9 December 2003; see message **200312/msg00054.html**<br><br>Solution proposal: liberty-architecture-bindings-profiles-v1.1.pdf (**3898**); see also the Shibboleth architecture at http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v05.pdf<br><br>Accepted proposal to incorporate introduction cookie mechansim at F2F on 3-5 Feb 2004; see message **200402/msg00123.html** ; solution was incorporated in profiles-06. |

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-8**<br>Completed | John Kemp | **Authentication Context**<br><br>Keywords: SSO, authentication<br><br>Liberty authentication context exchange and control. | Use case for indicating SP-requested authentication characteristics and reporting actual characteristics used: mail message **200310/msg00216.html**<br><br>Use case accepted on 9 December 2003; see message **200312/msg00054.html**<br><br>Solution proposals: liberty-architecture-authentication-context-v1.1.pdf (**3899**), draft-sstc-authn-context-v1.0 (**5188**); also draft-sstc-authn-context-v1.0-02 (**5244**)<br><br>Proposal to adopt solution proposal accepted at F2F on 3-5 Feb 2004; see message **200402/msg00123.html** |
| **W-9**<br>Active | Scott Cantor<br>Hal Lockhart | **XML Encryption**<br><br>Keywords: security, encryption, privacy<br><br>Incorporate XML-based encryption of assertions and/or other SAML constructs. | Use cases: messages **200311/msg00116.html** and **200312/msg00039.html**<br><br>On 9 December 2003, agreed to allow for encrypting requests and responses and to provide schema validity selectively on a case-by-case basis; see message **200312/msg00054.html**<br><br>Additional input: see the usage of XML Encryption in Liberty V1.2, described at http://www.projectliberty.org/specs/liberty-idff-protocols-schema-v1.2.pdf Section 3.2.2.3 and http://www.projectliberty.org/specs/liberty-idff-bindings-profiles-v1.2.pdf Section 3.8<br><br>Most recent use cases and solution proposal: message **200403/msg00127.html** |
| **W-10**<br>Inactive | – | **Back Office Profiles**<br><br>Keywords: profiles, web services<br><br>B2B, A2A, and other similar profiles. | |

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-11**<br>Inactive | – | **Mid-Tier Usage**<br><br>Keywords: profiles, web services, intermediaries, delegation<br><br>Profile or other specification for SAML usage in the middle tier for XML firewalls and similar. This is related to W-15. | |
| **W-12**<br>Inactive | | **Attribute Retrieval Enhancement**<br><br>Keywords: attributes, XACML, protocol<br><br>Finer-grained attribute retrieval, for example, "All attributes in namespace X." It has also been suggested that just the attribute schema or just the attribute names could be requested, that it should be possible to boxcar multiple assertion types in a request, and that requests with assertion ID references should also be allowed to contain attributes. Any solutions here should take into account the differences between SAML and XACML attributes. This may be impacted by W-2a. | Original issues: see sstc-saml-1.1-issues-draft-02 (**3690**) DS-12-03, DS-12-04, DS-9-02, DS-9-03<br><br>Decided at the March 2004 F2F to make inactive for V2.0. However, a number of design elements of other work items have involved various types of enhancements to attribute retrieval. |
| **W-13**<br>Inactive | – | **Hierarchical Privilege Delegation**<br><br>Keywords: attributes, authorization<br><br>Hierarchical delegation of privileges among federated attribute authorities. | |
| **W-14**<br>Active | Jeff Hodges | **SAML Server Trust**<br><br>Keywords: interoperability, trust<br><br>Standardized trust between SAML-enabled servers, apart from what we're already doing in the metadata work. It may be that the only appropriate action at this stage is to flesh out the security considerations and/or discuss it briefly in the SAML Primer. Some feel that it's premature to address this, although Liberty has done some work in this area.<br><br>Awaiting a proposal on how to put a framework around SAML and trust relationships. | Liberty Alliance has contributed a new document addressing this area; see message **200402/msg00007.html**<br><br>Document submitted is liberty-trust-models-guidelines-v1.0.pdf (**5242**)<br><br>Discussion at F2F on 3-5 Feb 2004 (see message **200402/msg00123.html** ) resulted in request to cast document in SAML-specific terms for TC consideration; this has been done in sstc-saml-trustmodels-2.0 (**6158**) |

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-15** Inactive~~Active~~ | Scott Cantor<br>Bob Morgan<br>Jeff Hodges | **Delegation and Intermediaries**<br><br>Keywords: profiles, web services, intermediaries, delegation<br><br>Use cases that support arbitrary multi-hop delegation. Liberty WSF supports one-hop impersonation. The relationship of this to WSS needs to be sorted out. This relates to the Fidelity need for a WSRP profile. This is related to W-11. The item "multi-participant transactional workflows" was folded into this one. | Delegation/intermediaries use case model: draft-morgan-sstc-delegation-model (**4402**) introduced in message **200312/msg00004.html**<br><br>Library meta-search use case from Scott Cantor: see messages **200312/msg00035.html** and **200312/msg00040.html** and **200312/msg00041.html**<br><br>Use case accepted on 9 December 2003, with additional exploration into existing proposed profiles, with view to the assertions being communicated further to a backend system – what are the security considerations and changes necessary? (see message **200312/msg00054.html** )<br><br>Additional input: see Ron Monzillo's slides in mail message **200309/msg00059.html**<br><br>At F2F on 3-5 Feb 2004 (see message **200402/msg00123.html** ), discussed this but concluded that more progress is needed on the AuthnRequest/Response design work in order to determine what is needed here; also see Ron's issue at thread starting at message **200402/msg00049.html** and other threads in month **200402/threads.html** (recorded in the issues list (**5428**) as TECH-3), plus proposal in **200401/msg00102.html**<br><br>The work to enable proper intermedary functioning has been done, meaning that this work item can be considered "mostly closed", but we have decided to defer to a later version any development of an actual profile that exploits SAML mechanisms to address various intermediary use cases. |
| **W-16** Inactive | – | (Merged with W-15.) | – |

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-17** Inactive (see **W-5**, **W-5a**, **W-5b**, **W-25**) | Tim Moses<br>Jeff Hodges | (Merged with W-5b.)<br><br>**Credentials Collector and Assertions**<br><br>Keywords: protocol<br><br>This includes pass-through authentication. This is related to W-18. | Use case proposal: oasis-sstc-v2_0-credentials_collector-use_cases-moses (**4119**)<br><br>Use case accepted on 9 December 2003; see message **200312/msg00054.html**<br><br>Additional input: see mail messages by Adams **200206/msg00007.html** and Lockhart **200303/msg00033.html**<br><br>Original issues: see sstc-saml-1.1-issues-draft-02 (**3690**) UC-1-14 |
| **W-18** Liaison | Jeff Hodges<br>Bob Morgan | **SASL support**<br><br>Keywords: authentication<br><br>Defining SAML as a SASL security mechanism. | Jeff and Bob will create an activity in IETF around this topic and function as our liaisons.<br><br>Original issues: see sstc-saml-1.1-issues-draft-02 (**3690**) UC-1-05, UC-5-02<br><br>Discussed this at the March 2004 F2F. This activity is not on the critical path for V2.0. The Kerberos work may be able to use the SASL mechanism. Discussions are ongoing. |
| **W-19** Completed | Scott Cantor | **HTTP-Based Assertion Referencing**<br><br>Keywords: bindings<br><br>Additional protocol binding for direct HTTP use. | Use case and solution proposal: draft-sstc-assertion-uri (**3651**)<br><br>Use case accepted on 9 December 2003; see message **200312/msg00054.html**<br><br>Accepted solution proposal at F2F on 3-5 Feb 2004 (see message **200402/msg00123.html** ); TC will pursue SAML-specific media (MIME) type registration; solution incorporated into Bindings doc |
| **W-20** Liaison | Dale Moberg<br>Matt MacKenzie | **ebMS Binding/Profile**<br><br>Keywords: bindings<br><br>Additional protocol binding for ebXML Message Service use and/or additional profile for using SAML to allow for authentication and authorization of ebMS messages. The eGov TC has discussed this latter notion a little. The ebxml-msg TC will take on both questions. | Dale and Matt will examine this in the ebxml-msg TC<br><br>Discussed this at the March 2004 F2F. This is not on the critical path for V2.0. |

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-21** Completed | Scott Cantor Bob Morgan | **Baseline Attribute Namespaces**<br><br>Keywords: attributes, XACML<br><br>For example, a DSML or X.500 profile for a person's attributes expressed in SAML. | Use case and solution proposal for convention for using X.500/LDAP attribute types in SAML: draft-morgan-saml-attr-x500 (**4124**); see also message **200401/msg00060.html**<br><br>Use case that proposes going beyond X.500/LDAP to RDB and/or UDDI: **200311/msg00010.html**<br><br>Further elucidation of use cases, resulting in P1 and P2: message **200312/msg00052.html**<br><br>Use case P1 accepted on 9 December 2003; see message **200312/msg00054.html**<br><br>Additional input: see also the Shibboleth architecture at http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v05.pdf and the XML-Enabled Directory work described in message **200312/msg00052.html**<br><br>At F2F on 3-5 Feb 2004 (see message **200402/msg00123.html** ), John Hughes agreed to be editor of new "Baseline Identities and Attributes" specification |
| **W-22** Inactive | | **Assertion Caching**<br><br>Keywords: assertions, web services, auditing<br><br>Persistent caching or mirroring of assertions at multiple sites. We think the WSS SAML token may be related to this; SAML has a protocol to obtain assertions, and there's also STR. Ideally this would be coordinated with the designs for W-13 through W-15, so that it's possible to express "I trust this server to cache assertions." | Decided at the March 2004 F2F to make inactive for V2.0. |
| **W-23** Inactive | | **Security Workflow**<br><br>Keywords: protocol<br><br>Expressing security processing workflow definitions. | Decided at the March 2004 F2F to make inactive for V2.0. |
| **W-24** Inactive | | (Merged with W-2.) | |

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-25** Active (see also **W-5**, **W-5a**, **W-5b**, **W-17**) | John Hughes | **Kerberos Support**<br><br>Keywords: authentication, profiles | Use case proposals for both the bridge server situation and the basic browser/Kerberos situation: draft-sstc-use-kerberos (**3760**)<br><br>Use case accepted on 9 December 2003; see message **200312/msg00054.html**<br><br>Solution proposal: draft-sstc-solution-profile-kerberos (**5935**)<br><br>At the March 2004 F2F, we agreed to take on a small portion of the work in V2.0, and the proposers will continue their offline work and possibly publish a draft intended for post-V2.0 adoption. The V2.0-scope material has not yet been added to the specs. |
| **W-26** Inactive | Prateek Mishra | **Dependency Audit**<br><br>Keywords: assertions, auditing<br><br>A "validity-depends-on" feature. | Discussed at the March 2004 F2F; suggested this can be achieved through special conditions. Decided to make it inactive for V2.0. |
| **W-27** Active | Tony Nadalin | **Security Analysis Enhancements**<br><br>Keywords: security, profiles<br><br>Suggestions from researcher who has done a formal security analysis. | The security analysis has been published at http://www.acsac.org/2003/abstracts/73.html. Tony/Scott/Prateek/Maryann will propose new issues based on this. |
| **W-28** Inactive | – | **XACML-Proposed Changes**<br><br>See the individually broken out work items below. | Input: see the combined XACML/OGSA proposal at **200309/msg00058.html** and the original OGSA proposal at **200306/msg00018.html** |
| **W-28a1** Completed | Rebekah Lepro | **Existing Attribute Usage Codification**<br><br>Keywords: attributes, interoperability<br><br>This is codification of existing namespace usage within the specs.<br><br>XACML and SAML structure their attribute information differently. | Use case proposal: sstc-cantor-w28a-attrib (**4035**)<br><br>Solution proposal: draft-sstc-attribute (**5312**)<br><br>At F2F on 3-5 Feb 2004 (see message **200402/msg00123.html** ) did a detailed walkthrough of the solution proposal and tasked Eve with a comprehensive revision (now at sstc-maler-w28a-attribute, **5946**)<br><br>(This item should be considered re-merged with W28a2 for all intents and purposes) |

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-28a2** Completed (see also **W-28a1**) | Rebekah Lepro | **Reconciling Attribute Usage with XACML**<br><br>Keywords: XACML, attributes<br><br>This should also acknowlege existing usage (W-28a1). | Use cases and solution proposal: 28b-draft-solution (note that the document ID should properly be "28a" or "28a2") (**3666**)Use case accepted on 9 December 2003; see message **200312/msg00054.html**<br><br>Additional input: see the combined XACML/OGSA proposal at **200309/msg00058.html** |
| **W-28b** Completed | Hal Lockhart | **XACML Proposal for Policy Transport and Authorization Decision Reconciliation**<br><br>Keywords: XACML, policy, authorization, grid<br><br>XACML has asked for a SAML-based solution to transporting requests for policies and the policies themselves. This ties into how to coordinate the XACML and SAML versions of authorization decisions. | This was sent back to the XACML TC. It is up to them to profile this use case from SAML foundations.<br><br>Additional input: see the combined XACML/OGSA proposal at **200309/msg00058.html**<br><br>Proposal to freeze Authz Decision functionality as is for V2.0, with no futher enhancement planned and with referral to XACML for those need more fnality accepted at F2F on 3-5 Feb 2004; see message **200402/msg00123.html** |
| **W-28c** Inactive | | Merged with 28b above. | |
| **W-28d** Completed | Rebekah Lepro | **IssuerName Enhancement**<br><br>Keywords: XACML<br><br>XACML would like to have "datatyping" of issuers. | Use case and solution proposal: 28d-draft-solution (**3667**), draft-sstc-AssertIssuer (**5158**)<br><br>Additional input: see the combined XACML/OGSA proposal at **200309/msg00058.html**<br><br>The acceptance of draft core-04 at F2F on 3-5 Feb 2004 (see message **200402/msg00123.html** and W-2 above) included core spec features implementing enhancement of issuer names |

| ID/Status | Owner(s) | Description | Documents and Dispositions |
|---|---|---|---|
| **W-29** Completed | Eve Maler | **Promised V2.0 Changes**<br><br>Plans to make backwards-incompatible changes in V2.0 that were promised in V1.0 or V1.1:<br><br>Removing AuthorityBinding element (core)<br><br>Removing RespondWith element (core)<br><br>Removing deprecated NameIdentifier URIs (core)<br><br>Requiring URI references to be absolute (core)<br><br>Disallowing Status element as the only child of a SOAP Body element (bindings)<br><br>Removing deprecated artifact URI (bindings) | Implemented. |
| **W-30** Active | Scott Cantor<br>Prateek Mishra | **Migration Paths**<br><br>Document the migration paths from SAML V1.1 to SAML V2.0, and from Liberty V1.2 to SAML V2.0. This is likely to go in the *Implementation Guidelines* document, though this may change. | Waiting for implementation<br><br>At the March-April 2004 F2F, we agreed to begin by creating a "diffs" document that describes the changes and rationales briefly; see the presentation at message **200404/msg00094.html** for a list of substantive diffs through core-10, profiles-05, etc. |

# A. Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.