Drummond group

Certification Final Report

SAML 2.0 Interoperability Test

Fourth Quarter 2007 (4Q07)

Dec. 13, 2007

Prepared & Administered by:
DRUMMOND GROUP INC.
www.drummondgroup.com

Drummond group

Table of Contents

Drummond group

Cover Letter

DRUMMOND GROUP Inc. is pleased to announce that the participants listed in this report have completed all requirements and passed the test requirements for the SAML 2.0 Interoperability Certification Test Event 4Q07 (SAML-4Q07) (see Final Test Results). This was the first Liberty sponsored SAML test event to require full-matrix interoperability between each product. Full-matrix testing certifies all of the products work with each over the different conformance modes for which they tested. This report provides the description of how these products were tested, the technical requirements and test cases required of them, listing of important consensus items made and insight into product configuration setup used to achieve interoperability. The Overview of Test Event section highlights the scope of this report and provides hyperlinks to the key sections of the document.

Please note that a SAML interoperability certification indicates the interoperability of a specific product-with-version, such as SAML Product X vs. 5.2, within a specific group of other products-with-version for a given test round, such as 3Q07. Products certified in older tests may not be interoperable with the products-with-version from the most recent certification test round.

The relevance of a SAML test round certification within real world deployment diminishes with time, usually over 12-18 months. New products enter the market and existing products change with revisions and updates. Given such changes in the product test group, an interoperability certification does not guarantee perpetual interoperability within real world deployment, and interoperability test events must be repeated to include new products, unchanged existing products and existing products with new versions.

Sincerely,

Rik Drummond
CEO,
Drummond Group Inc.

Disclaimer

Drummond Group Inc. (DGI) conducts interoperability and conformance testing in a neutral test environment for various companies and organizations ("Participant"). At the end of the testing process, DGI may list the name of the Participant in the final test report along with an indication that the Participant passed the test. The fact that the name of the Participant appears in the final report is not an endorsement of the Participant or its products or services, and DGI therefore makes no warranties, either express or implied, regarding any facet of the business conducted by the Participant or their product.

Test Participants

Hewlett-Packard http://www.hp.com/ **Product Name: Select Federation 7.0 patch1**	**IBM Corporation** http://www.ibm.com/ **Product Name: Tivoli Federated Identity Manager version 6.2**
RSA, The Security Division of EMC http://www.rsa.com/ **Product Name: RSA Federated Identity Manager 4.0**	**Sun Microsystems, Inc.** http://www.sun.com/ **Product Name: Sun Java System Federated Access Manager 8.0**
Symlabs, Inc. http://www.symlabs.com **Product Name: Symlabs Federated Identity Suite version 3.3.0**	

Definitions

Interoperability – A product is deemed interoperable with all other products in the Interoperability Test Round if and only if it demonstrates in a full-matrix manner the pair wise exchange of data covering the *Test Criteria* between all products in the Interoperability Test Round. A product is either totally interoperable or it is not interoperable. Waivers or exceptions are not given in demonstrating interoperability for the *Test Criteria* unless the entire *Product Test Group,* DGI and Liberty Alliance agree.

Interoperable products – Group of products, from the *Product Test Group*, which successfully completed the *Test Criteria*, in a full–matrix manner with every other *Product Test Group* participant in an Interoperability Test Round without any errors in the final test Phase. Interoperable products receive a Liberty Alliance Interoperable™ seal.

Product Test Group – A group of products involved in an interoperability or conformant Test Round.

Product, product-with-version, or product-with-version-with-release – are interchangeable and are defined for the purpose of a Test Round as a product name, followed by a product version, followed by a single digit release. The assumption is that version and release syntax is as: "VV.Rx…x," where VV is the version numeral designator, R is the single digit release numeral designator and x is the sub-release multiple digit numeral designator. DGI assumes that any digits of less significance than the R place do not indicate code changes on the product-with-version-with-release tested in the Test Round. A vendor must list a product as product name, followed by version digits followed by a decimal point followed by a single release designator digit before the Test Round is complete.

Test Case – The test criteria is a set of individual test cases, often 10 to 50 which the product test group exchange among themselves to verify conformance and interoperability.

Test Criteria – A set of individual tests, based on one or more standard specifications, that is used to verify that a product is conformant to the specification(s) or that a set of Product-with-version's are interoperable under the *Test Criteria*.

Interoperability Test Summary

Overview of Test Event

The 4Q07 SAML 2.0 interoperability test event consisted of five vendor participants: HP, IBM, RSA, Sun and Symlabs. All five participants have achieved Liberty Alliance Interoperable certification for the SAML 2.0 4Q07 test event. They performed full-matrix testing over different SAML conformance modes without error or code changes during the SAML 2.0 4Q07 Certification Run on the dates of November 27-30 to prove their interoperability. The time preceding the Certification Run, October 1-November 26, was set aside for debugging interoperability issues. The list of products and the conformance modes they certified for can be found in the Final Test Results section.

There are several conformance modes for SAML testing, both those defined within the SAML specification by OASIS and those defined by Liberty Alliance. In order to be certified in a SAML conformance mode, each vendor was required to perform full-matrix testing in its respective conformance mode(s). Full-matrix testing requires each participant to test with every other participant for all test criteria. For example, a product certifying as a SAML Service Provider (SP) had to execute all required test cases with all the SAML Identity Provider (IdP) products as SPs and IdPs must interoperate with each other. The list of what test cases were required for each conformance mode can be found in the section summarizing the test cases and conformance modes.

The test criteria and the subsequent test cases cover all the conformance modes for this test event and were approved by the Liberty Alliance Technology Engineering Group (TEG). The actual test cases for this test event can be found in this section of the report.

To assist in the deployment of these products into live networks, relevant information about achieving their interoperability can be found in the Interoperability Caveats section. This section explains how the products were configured and key consensus items made to insure their interoperability. Information in this section may be beneficial for deployment interoperability in user federations.

Finally, this report contains sections describing the trading partner requirements and technical requirements given to the participants in order to complete full-matrix interoperability testing, as well as a section summarizing the DGI Interoperability and Compliance Process.

Final Test Results

The table below shows the interoperable products and the conformance modes they successfully tested. The green boxes with the "P" within them indicate the participant passed certification requirements in the corresponding conformance mode. The actual product version-with-release information can be found in the Test Participant section.

Company	SAML Defined Conformance Modes											Liberty Alliance Defined Conformance Modes		
	IDP	SP	SP Extended	IDP Extended	ECP	Attribute Authority Requestor	Attribute Authority Responder	Authorization Decision Authority Requestor	Authorization Authority Decision Responder	Authentication Authority Requestor	Authentication Authority Responder	SP Complete	POST Binding	GSA
Hewlett-Packard	P	P	P	P	P	P	P					P	P	P
IBM Corporation	P	P				P	P					P	P	P
RSA, The Security Division of EMC	P	P										P	P	P
Sun Microsystems, Inc.	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Symlabs, Inc.	P	P	P	P	P	P	P	P	P	P	P	P		P

The participants and certified conformance modes from the table above are also listed below in a non-table form.

HP: IDP, SP, SP Extended, IDP Extended, ECP, Attribute Authority (Requester/Responder), SP Complete, POST Binding, GSA

IBM: IDP, SP, Attribute Authority (Requester/Responder), SP Complete, POST Binding, GSA

RSA: IDP, SP, SP Complete, POST Binding, GSA

Sun: IDP, SP, SP Extended, IDP Extended, ECP, Attribute Authority (Requester/Responder), Authorization Decision Authority (Requester/Responder), Authentication Authority (Requester/Responder), SP Complete, POST Binding, GSA

Symlabs: IDP, SP, SP Extended, IDP Extended, ECP, Attribute Authority (Requester/Responder), Authorization Decision Authority (Requester/Responder), Authentication Authority (Requester/Responder), SP Complete, GSA

Interoperability Test History

This is the first SAML 2.0 interoperability certification event administered by DGI, and it is also the first full-matrix interoperability test event for SAML 2.0. Liberty Alliance has sponsored and administered previous SAML 2.0 certification events. Please refer to the Liberty Alliance website for more information on those past test events.

About SAML 2.0

SAML 2.0 is an open standard developed by OASIS (http://www.oasis-open.org/committees/security/). SAML (Secured Assertion Markup Language) allows for communication of identity management among trusting partners by exchanging assertions about a principal's identity, authorization privileges and attributes. This enables an entity to perform a single sign-on (SSO) where the entity provides identity authentication, for example through a secure password, only once and this identification is shared among the other trusting partners without requiring the entity to re-enter the identity authentication.

About Liberty Alliance

Liberty Alliance is a consortium of companies focusing on identity management through open standards. Liberty Alliance's Liberty Interoperable™ program is designed for out-of-the-box interoperability among identity management products. More information about Liberty Alliance can be found at http://www.projectliberty.org/liberty/liberty_interoperable.

Test Case and Conformance Mode Summary

Test Case and Conformance Mode Summary: Overview

The certification event contained test cases which covered both conformance modes defined by the SAML 2.0 specifications and also Liberty Alliance defined conformance modes. All conformance modes, both SAML 2.0 and Liberty Alliance defined, were exclusive to the other modes, except for the SP Extended and IDP Extended modes, and could each be optionally tested by the participants. Each test case was part of one or more conformance mode.

SAML Defined Conformance Modes

SAML 2.0 specifies eleven operational conformance modes of and the specific features that are required or optional for each mode. The details of each mode are provided in [SAMLConf], and the conformance modes a listed here:

- IdP – Identity Provider
- IdP Lite – Identity Provider Lite
- SP – Service Provider
- SP Lite – Service Provider Lite
- ECP – Enhanced Client/Proxy
- IdP Extended – Identify Provider Extended
- SP Extended – Service Provider Extended
- SAML Attribute Authority
- SAML Authorization Decision Authority
- SAML Authentication Authority
- SAML Requester

Certification in conformance modes IdP Extended and SP Extended can only be given if a participant has met the certification requirements of one of the standard SP or IdP modes.

Since SAML 2.0 makes all requirements for SAML Requester mode optional, Liberty Alliance clarifies the results by showing SAML authority mode with the requester mode tested. Since each requester needs an authority responder, the certification designation is assigned for both. For example, Attribute Authority Requester and Attribute Authority Responder.

Optional Liberty Alliance Conformance Modes

SP Complete

Liberty Interoperability Testing Program has created an additional designation "SP Complete" to recognize and differentiate implementations that demonstrate interoperability of all optional features for the SP mode. SP Complete indicates all SP optional features were tested. Every test participant testing for SP also tested the optional SP features so that all participants have certification in SP Complete.

POST Binding

Although the POST binding is not included in the SAML SCR, it is permitted with the SAML specification and has some user deployment. POST Binding is an optional Liberty Alliance designation conformance mode. It involves use of POST binding for AuthnRequest, Name ID Management and SLO. Certification in the POST Binding mode is done through successfully completing Test Case C.

GSA Profile

The GSA Profile Test Case O is an optional test case. It follows the SAML 2.0 requirements for the General Service Administration (GSA) of the US Government. The technical requirements for this test case come from the GSA SAML Profile in [GSAInterface], [GSAAdoptSchm] and [GSATechAppr]. These documents should be consulted for further explanation of the GSA requirements.

Test Cases Associated with Conformance Modes

In order to achieve certification in one or more of the SAML Conformance Modes, the associated test cases had to be completed with all test participants with aligning modes. Aligning modes are modes which are used in conjunction with each other. For example, a product testing for an IdP conformance mode must complete Test Cases A, B, C, E, F, G, H and I against all products testing for a SP conformance mode. The individual test cases provide details of who each mode interacts with each other and test steps that may or must be omitted depending on the conformance mode.

Conformance Mode	Test Cases
IdP	A, B, E, F, G, H, I, N
IdP Extended	D
SP / SP Complete	A, B, C, E, F, G, H, I, N
SP Extended	D
ECP	I
SAML Authentication Authority (Requester/Responder)	J, M
SAML Attribute Authority (Requester/Responder)	K, M
SAML Authorization Decision Authority (Requester/Responder)	L, M
Liberty Alliance POST Binding	C
GSA Profile	O

Interoperability Caveats

While all products-with-version successfully tested with each other, there are some caveats to consider in interpreting these results and implementing these products. This information may assist successful rollout and backward version interoperability.

Consensus Items

Consensus Items contains standards/implementation issues the product test group reached consensus on in order to achieve interoperability among the group. Some consensus items may be temporary solutions necessary to facilitate interoperability among the group until a standard body can more formally address the concern.

- DSAwithSHA1 signature algorithm not supported. Section 4.1 of [SAMLConf] states that the DSAwithSHA1 signature algorithm, while recommended, is not required by SAML 2.0. As it was not required, one participant was not able to support DSAwithSHA1 algorithm in a partner's certificate. The group agreed to only use digital certificates with the required RSAwithSHA1 signature algorithm.
- Understanding EncryptionMethod elements. Section 4.2 of [SAMLConf] lists different block encryption ciphers and key transports which must be supported within SAML 2.0. Section 2.4.1.1 of [SAMLMeta] addresses the EncryptionMethod element which specifies the ciphers and key transports supported by the entity. There was a question on how to interpret metadata which only listed a subset of the ciphers and key transports required by SAML. For the interoperability test, it was agreed to support any of the ciphers and key transports listed in section 4.2 of [SAMLConf] regardless of the metadata values. DGI will follow up with SSTC group within OASIS for guidance and clarification on this question.
- NameIDPolicy and ID Encryption. During testing, a question arose on interpreting NameIDPolicy from [SAMLCore] in lines 2136-2142. The understanding was reached that if NameIDPolicy of AuthnRequest says ID is to be encrypted, it must be encrypted in the assertion and if NameIDPolicy of AuthnRequest does not state the ID is to be encrypted, the IDP MAY still encrypt the ID based on its policy, specifically its policy with the SP.
- SSL Server-side Authentication. To insure all participants used the same security settings, it was agreed to only use SSL server-side authentication for SOAP connections and not to use SSL client-side authentication.

Configuration Setup

Because of the numerous configurations with SAML, it is important to have a products properly setup in order to achieve interoperability. For all products, proper metadata setup was needed. Basic partner configuration, such as binding to use and security, was determined from the test case steps and configured as expected through the product interface. However, any different, unique or unexpected configurations apart from the normal settings found in metadata or the typical user interface are listed below. This is information collected directly from the participants. This was the configuration for the products within this test, and it may be different for individual user deployments.

HP

For IdP Discovery, discovery service is enabled on the IDP and SP to support introduction. In addition the cookie reader and writer service needs to be set up for SP and IDP, respectively. A domain must be specified for the cookie to be written to.

The HP ECP client is standalone proxy that simulates a WAP gateway. It supports both WAP based and form based (user/pass) authentication contexts. The header attribute used is x-msisdn which was associated with “MobileContract” authentication context. Being a standalone client it does not support any intermediary forms or HTML pages that need to be filled in. For this test event, Symlabs supported WAP authentication context so authorization was through WAP headers. IBM, RSA and Sun had to provide a way to bypass these intermediary forms.

The HP SP and IDP must be enabled for working with ECP. In working with the Sun ECP, the HP IDP was set to bypass the HTML form and provide authentication through URL name value parameter. For Symlabs ECP, HP has built in support in IDP for WAP header authentication.

For IDP Proxy, IDP was configured to enable proxy. For Name ID Mapping, this also must be enabled.

For Attribute Authority, basic authentication was setup for SOAP requests. Partners must mutually agree on the set of attributes and their SAML formats that are used in the Attribute query, and then these need to be setup on the IDP. No modification of HP metadata required.

IBM

IBM SP disabled AuthnResponse signature validation for the IDPs of HP, RSA, Sun and Symlabs as they did not use a signature for this message.

IBM SP disabled ArtifacResolve Response signature validation for the IDPs of HP, Sun and Symlabs as they did not use a signature for this message.

IBM IDP disabled ArtifacResolve Response signature validation for the SPs of HP, Sun and Symlabs as they did not use a signature for this message.

For working with the HP ECP, IBM IDP enabled HTTP header session tracking and authentication using x-msisdn header.

For working with the Sun ECP, IBM IDP enabled HTTP header session tracking and authentication using x-msisdn header.

For working with the Symlabs ECP, IBM SP enabled HTTP header session tracking, and the IBM IDP enabled HTTP header session tracking and authentication using x-msisdn header.

Use of common domain cookie in IDP Discovery and the attribute query of Attribute Authority used standard setup.

RSA

For ECP connecting to the RSA SP, ECP needs to authenticate SP. This will be form based authentication. Also, ECP client has to be cookie aware because FIM authentication manager on SP would create cookie after authentication and authorization to resource is based on if cookie is set. Also, RSA SP must set a default IDP to send ECP request. The code to authenticate the user at RSA IDP was given to the HP, Sun and Symlabs ECPs.

For ECP connecting to the RSA IDP, if you set a header cookie over SOAP/HTTP call, the RSA IDP will assume you are already authenticated.

Sun

Partner needed to inform Sun out of band which AuthnContext they were expecting. If binding for Response message not specified, Sun used the first one in the metadata.

The validity period of the assertion was adjusted in the configuration setting.

For IDP Discovery, cookie domain needs to be configured at Sun product where the IDP Introduction is deployed. Partners could either federate the name ID or can go to the Sun IDP Driver page and set CDC cookie.

Sun has both an ECP Java client and ECP Java proxy, but for the certification event, only the ECP Java client was tested. Sun ECP needed its metadata loaded at the SP and IDP of their test partners.

Sun published an SP-ECP filter URL for the HP-ECP and Symlabs-SP products to use in order to initiate ECP base requests to the Sun SP.

When HP-SP and Symlabs-SP connected to the Sun-IDP Proxy, a list of preferred IDPs was displayed which the SP partners could communicate with.

For Attribute Authority, HTTP Basic Authentication with user/password was used for authentication.

Symlabs

The default signature settings matched the requirements, i.e. assertion signed. Encryption setting is a global setting for all partners and is toggled through the web GUI.

ECP is a stand-alone enhanced client. Symlabs-ECP uses x-msisdn trusted header.

Browser Usage

Since SAML SSO is primarily a web browser based action, each participant was required to use the web browser or web browsers of their choice for certification testing. The browsers used are listed below.

- HP: Firefox, vs. 2.0.0.7
- IBM: Firefox, vs. 1.5/2.x
- RSA: Firefox, vs. 2.0.0.7 and IE 6.0
- Sun: Firefox, vs. 1.5.0.4
- Symlabs: Firefox, vs. 2.0.0.11

Testing Requirements

In order to be part of the product test group, each participant was required to meet certain trading partner requirements and technical requirements.

Trading Partner Requirements

All participants were required to establish trading partner relationships with each other. In doing so, participants were able to do full-matrix testing where every participant sent and received all test cases with each other for aligned conformance modes. Thus, each participant was a sender and receiver of a test case with all other participants. All participants were remote from each other, and all test messages were exchanged over the public Internet. Participants were responsible for creating their own certificates, distributing their network information to each other and configuring their firewalls to allow all other participants access to their product-with-version.

Metadata

There are no normative requirements in [SAMLConf] regarding the content or processing of metadata as described in [SAMLMeta]. However, for purposes of this certification event, implementations are required to:

- Furnish correct metadata, and
- Process metadata furnished by other testing partners

While metadata is not specified for SAML Attribute Requesters, interoperability with SAML Authorities is very difficult without it, and for this certification event it is required that SAML Attribute Requesters provide metadata as described in the draft metadata extension specification [SAMLMetaExt]. It is not necessary or meaningful for an ECP to produce or consume metadata.

Participants were responsible for creating their own certificates for testing, except for the GSA Test Case which used special certificate created by GSA. Certificates were included in metadata.

Technical Requirements

General Test Case Requirements

For all test cases, the following requirements were followed unless a test case specifically stated otherwise:

- SAML AuthnRequest MUST be signed.
- For POST bindings, the assertion MUST be signed.

- For POST bindings, the entire response message MAY be signed, but if signed, the receiving partner MUST validate the signature.
- Encryption of NameIDs and Assertions MUST be enabled.

IdP Authentication

SAML does not normatively specify any requirements for user authentication at IdP for Web SSO. In fact, user authentication is explicitly described as “out of scope” [SAMLProf]. However, for purposes of interoperability testing, it is required that IdP implementations offer at least one of these authentication methods:

1. HTTP Basic Auth.
2. HTTP Form Post
3. HTTP Get

Similarly, it is required that user agents, particularly ECP implementations, be able to authenticate using at least one of these methods.

Trivial Processing

Several features specified by SAML (e.g., IdP Proxy) can be implemented such that any request simply returns an error response. While this trivial behavior is, strictly speaking, in conformance with the specifications, it is not meaningful in the context of interoperability testing. Except where explicitly indicated (e.g., for certain Name Identifier formats) all testing steps will require non-trivial responses in order to be deemed successful.

Authentication Contexts

Some of the SAML Modes rely on a well-defined ordering of authentication contexts. The SAML specifications do not normatively specify an ordering [SAMLAuthnCxt] and leave the comparison decisions up to the implementation [SAMLCore]. However, for purposes of testing we arbitrarily define an ordering of authentication contexts to be used in the tests. This arbitrary listing of authentication class URIs, in order of increasing strength, is:

1. any defined authentication context not listed below
2. urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
3. urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
4. urn:oasis:names:tc:SAML:2.0:ac:classes:Password

Complete implementation of these authentication contexts was not required. These authentication context URIs were asserted in requests and responses to demonstrate interoperability of authentication context processing rules.

Name Identifier Formats

The following Name Identifier Formats are defined by [SAMLCore]:

1. Unspecified
2. Email
3. X.509 Subject
4. Windows
5. Kerberos
6. Entity
7. Persistent
8. Transient

Every implementation wass required to accept messages containing any of these formats, but [SAMLCore] only requires that the last two be processed.

XML Signatures

The [SAMLConf] does not specifically indicate where XML Signatures are required, but the underlying specifications in [SAMLProf] make signing required for certain profiles. Specifically, these are:

1. Web SSO: The assertion element(s) in the <Response> MUST be signed for the HTTP POST binding.
2. ECP Profile: The assertion element(s) in the <Response> issued by the IdP MUST be signed.
3. Single Logout: The <LogoutRequest> and <LogoutResponse> MUST be signed for the HTTP redirect binding.
4. Name Identifer Management: The <ManageNameIDRequest> and <ManageNameIDResponse> MUST be signed for the HTTP redirect binding.

SP and IdP implementations could indicate via metadata a desire for requests or responses to be signed for other bindings than those indicated above. However, such stipulations in metadata were not binding and adherence was not required.

XML Encryption

[SAMLConf] stipulates several different encryption algorithms and key transport mechanisms that MUST be implemented. However, these testing procedures do not require demonstration of support for all these combinations and instead rely on successful interoperability as a measure of conformance.

412 Encryption coupled with deflation and URL encoding may create URLs that
413 exceed the maximum length supported by some browsers. Consequently,
414 encryption is contraindicated for the MNI HTTP-Redirect testing steps.

415 **Attribute Profiles**

416 [SAMLConf] makes no normative statements about which Attribute Profiles in
417 [SAMLProf] are required to be supported by SAML Attribute Authority or a SAML
418 Requestor. This document only describes testing procedures for the Basic
419 profile, and does not describe any testing procedures regarding the other
420 profiles.

Overview of the DGI Interoperability Compliance Process®

Interoperability of B2B products for the Internet is essential for the long-term acceptance and growth of electronic commerce. To foster interoperability, DGI facilitates interoperability and conformance tests. This section contains a description of the test process involved with creating and listing interoperable products.

DGI Interoperability Test Round

Products-with-version come together in a vendor-neutral and non-competitive environment to test with each other in order to become interoperable with each other. In an Interoperability Test Round, each product-with-version must successfully test with each other in order to be certified as interoperable.

The DGI Interoperability Test Round verifies conformance to a standard and then verifies that members of the Product Test Group are interoperable among themselves. Interoperability is an all or nothing within the Product Test Group over the Test Criteria. A product is either interoperable with all other products in the Test Group or not.

Products-with-version which demonstrate complete interoperability among the passing members of the Product Test Group are given a Liberty Alliance Interoperable™ seal and are listed with Interoperability Status on the www.projectliberty.org website. Interoperability Test Rounds are periodically repeated to verify that as product names, versions or releases change, the products remain interoperable.

References

[SAMLAuthnCxt] J. Kemp et al, "Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS SSTC (March 2005), http:// docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf.

[SAMLConf] Prateek Mishra et al, "Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS SSTC (March 2005). http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf.

[SAMLCore] S. Cantor et al, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS SSTC (March 2005), http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[SAMLErrata] Jahan Moreh, "Errata for the OASIS Security 2 Assertion Markup Language (SAML) V2.0, Working Draft 28," OASIS SSTC (May 8, 2006), http://www.oasis-open.org/committees/download.php/18070/sstc-saml-errata-2.0-draft-28.pdf

[SAMLMeta] S. Cantor et al, "Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS SSTC (March 2005), http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.

[SAMLMetaExt] Tom Scavo et al, "SAML Metadata Extension for Query Requesters, Committee Draft 01", OASIS SSTC (March 2006), http://www.oasis-open.org/committees/download.php/18052/sstc-saml-metadata-ext-query-cd-01.pdf

[SAMLProf] S. Cantor et al, "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS SSTC (March 2005), http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.

[GSATechAppr] Dave Silver et al, "Technical Approach for the Authentication Service Component" vs. 2.0.0 GSA (May 2007), http://www.cio.gov/eauthentication/TechnicalArchitecture.htm

[GSAAdoptSchm] Dave Silver et al, "E-Authentication Federation Adopted Schemes" vs. 1.0.0 GSA (May 2007), http://www.cio.gov/eauthentication/TechnicalArchitecture.htm

[GSAInterface] Dave Silver et al, “E-Authentication Federation Architecture 2.0 Interface Specifications” vs. 1.0.0 GSA (May 2007), http://www.cio.gov/eauthentication/TechnicalArchitecture.htm

Appendix A: Test Case Details

Each test case contains a table presenting an overview of the test steps written in shorthand. Preconditions and other relevant testing notes are also included in each test case. These are the same test cases and instructions as used in the certification event.

Test Case A – Redirect Binding

Preconditions: Metadata exchanged and loaded

Conformance Modes: IdP, SP, IdP Lite, SP Lite

NOTE – IdP Lite and SP Lite actors are to ignore Name ID Management steps

Test Step Overview

Steps	Action/Message/Setting
1	Encryption Enabled
2	Web SSO HTTP redirect / Persistent / Federate
3	MNI IdP-Initiated / HTTP redirect (signed)
4	SLO SP-Initiated / HTTP redirect (signed)
5	Web SSO HTTP redirect / Not Federated
6	SLO IdP-initiated / HTTP redirect (signed)
	Destroy Federation and NameIds
7	Web SSO HTTP redirect / Federate
8	MNI SP-Initiated / HTTP redirect (signed)
9	SLO SP-Initiated / HTTP redirect (signed)
10	Web SSO HTTP redirect
11	SLO IdP-Initiated / HTTP redirect (signed)
12	Encryption Disabled

Test Case B – SOAP Binding

Preconditions: Metadata exchanged and loaded

Conformance Modes: IdP, SP, IdP Lite, SP Lite

NOTE – IdP Lite and SP Lite actors are to ignore Name ID Management steps

Test Step Overview

Steps	Action/Message/Setting
1	Encrypted IDs and Assertions
2	Web SSO Artifact / Persistent / Federate / Artifact Resolution SOAP
3	MNI IdP-Initiated / SOAP (SP may use HTTP Redirect)
4	SLO SP-Initiated / SOAP (SP Lite / IdP Lite may use HTTP Redirect)
5	Web SSO Artifact / Persistent / Not Federated / Artifact Resolution SOAP
6	SLO IdP-initiated / SOAP (SP Lite / IdP Lite may use HTTP Redirect)
7	Web SSO Artifact / Artifact Resolution SOAP
8	MNI SP-Initiated / SOAP (SP may use HTTP Redirect)
9	SLO IdP-Initiated / SOAP (SP Lite / IdP Lite may use HTTP Redirect)
10	Web SSO Artifact / Artifact Resolution SOAP
11	SLO IdP-Initiated / HTTP redirect (signed)

Test Case C – POST Binding

Preconditions: Metadata exchanged and loaded

Conformance Modes: POST Binding for both IdP and SP functionality.

Test Step Overview

Steps	Action/Message/Setting
1	Encrypted Enabled
2	Web SSO / POST (signed) / Persistent / Federate
3	MNI IdP-Initiated / POST (signed)
4	SLO SP-Initiated / POST (signed)
5	Web SSO POST (signed) / Not Federated
6	SLO IdP-initiated / POST (signed)
7	Web SSO POST (signed)
8	MNI IdP-initiated / POST / Terminate
9	Web SSO POST (signed)
10	MNI SP-Initiated / POST (signed)
11	SLO SP-Initiated / POST (signed)
12	Web SSO POST (signed)
13	SLO IdP-Initiated / POST (signed)

Test Case D – Extended SAMLModes

Preconditions: Metadata exchanged and loaded

Conformance Modes: IdP Extended, SP Extended

Test Step Overview

Steps	Action/Message/Setting
1	Encryption Enabled
2	ProxyCount=0 (proxy disallowed)
3	Web SSO HTTP Redirect (signed) to IdP_A
4	SLO SP-initiated / HTTP Redirect
5	ProxyCount missing (proxy allowed)
6	Web SSO / HTTP Redirect (signed) to IdP_A
7	SLO SP-initiated / HTTP Redirect
8	ProxyCount=1 (proxy allowed)
9	Web SSO / HTTP Redirect (signed)
10	SLO SP-initiated / HTTP Redirect
11	Web SSO HTTP Redirect (signed) / Persistent
12	SLO IdP-initiated / HTTP Redirect
13	NameIDMappingRequest / NameIDMappingResponse

Test Case E – IDP Introduction

Preconditions: Metadata exchanged and loaded

Conformance Modes: IdP, SP, IdP Lite, SP Lite

NOTE – IdP Lite and SP Lite actors are to ignore Name ID Management steps

Test Step Overview

Steps	Action
1	Enables Encryption / Clear Cookies
2	IdP Login / Federate / Set Cookie
3	SSO at SP using common domain cookie
4	MNI Destroy Federation / IdP-Initiated / HTTP Redirect

Test Case F – Single Session Logout

Preconditions: Metadata exchanged and loaded

Conformance Modes: IdP, SP, IdP Lite, SP Lite

NOTE – IdP Lite and SP Lite actors are to ignore Name ID Management steps

Test Step Overview

Steps	Action/Message/Setting
1	Web SSO (Browser A) / Federate / HTTP Redirect
2	Web SSO (Browser B) HTTP Redirect
3	SLO (Browser A) SP-Initiated / HTTP redirect (signed) Browser B session remains active
4	Web SSO (Browser A) HTTP Redirect
5	SLO (Browser A) IdP-Initiated / HTTP redirect (signed) Browser B session remains active
6	MNI SP-initiated (Browser B) / Redirect (signed) / Terminate

Test Case G – Unsolicited <Response>

Preconditions: Metadata exchanged and loaded
Conformance Modes: IdP, SP, IdP Lite, SP Lite

Test Step Overview

Steps	Action
1	IdP Unsolicited SSO Response / Transient / HTTP POST (signed)
2	SLO SP-Initiated / HTTP redirect (signed)
3	IdP Unsolicited SSO Response / Transient / HTTP artifact / Artifact Resolution (SOAP)
4	SLO IdP-Initiated / HTTP redirect (signed)

Test Case H – Affiliations

Preconditions: Metadata exchanged and loaded
Conformance Modes: IdP, SP, IdP Lite, SP Lite

Test Step Overview

Steps	Action
1	SPNameQualifier=[affiliation id]
2	Web SSO HTTP Redirect / Persistent / Federate
3	SLO IdP-initiated / HTTP Redirect (signed)
4	Web SSO HTTP Redirect / Not Federate
5	SLO SP-initiated / HTTP Redirect (signed)
6	SPNameQualifier=[sp provider id]

Test Case I – ECP

Preconditions: Metadata exchanged and loaded

Conformance Modes: IdP, SP, IdP Lite, SP Lite, ECP

Note: Since ECP facilitates the SSO-SLO between an SP and IDP, each ECP product tested with the different combinations of SP products and IDP products in a full-matrix manner. The only combinations which were excluded were ones where either the SP or IDP products were the same as the ECP product.

Test Step Overview

Steps	Action
1	Federate (NameIDPolicy, AllowCreate=True)
2	Enhanced ClientProxy SSO, PAOS
3	ECP conveys Response to SP

Test Case J – SAML Authentication Authority

Conformance Modes: SAML Authentication Authority, SAML Requester

Preconditions: Metadata exchanged and loaded

Note: Section [AuthenticationContexts] within this document describes the strength of the AuthnContext classes used for comparison.

Test Step Overview

Steps	Action/Message/Setting
1	Web SSO / POST (signed) / Persistent
2	AC Comparison=”exact” / HTTP Basic Authentication
3	Authentication Query / SOAP
4	AC Comparison=”better”
5	Authentication Query / SOAP
6	AC Comparison=”minimum”
7	Authentication Query / SOAP
8	AC Comparison=”maximum”
9	Authentication Query / SOAP

Test Case K – SAML Attribute Authority

Conformance Modes: SAML Attribute Authority, SAML Requester
Preconditions: Metadata exchanged and loaded

Test Step Overview

Steps	Action/Message/Setting
1	Web SSO / POST (signed) / Persistent
2	Attribute Query No Attributes
3	Attribute Query / SOAP
4	Attribute Query Attribute Named
5	Attribute Query / SOAP
6	Attribute Query Attribute Value
7	Attribute Query / SOAP
8	Encrypted Attribute / Attribute Query Attribute Named
9	Attribute Query / SOAP

Test Case L – SAML Authorization Decision Authority

Conformance Modes: SAML Authorization Decision Authority, SAML Requester
Preconditions: Metadata exchanged and loaded

Test Step Overview

Steps	Action/Message/Setting
1	Web SSO / POST (signed) / Persistent
2	HTTP Basic Authentication
3	AuthzQuery Resource=never (never permitted)
4	Authorization Decision Query / SOAP
5	AuthzQuery Resource=maybe (permitted if auth match)
6	Authorization Decision Query / SOAP
7	AuthzQuery Resource=always (always permitted)
8	Authorization Decision Query / SOAP

Test Case M – Request for Assertion by ID and SAML URI Binding

Conformance Modes: SAML Attribute Authority, SAML Authorization Decision Authority, SAML Authentication Authority, SAML Requester

Preconditions: Metadata exchanged and loaded

Test Step Overview

Steps	Action/Message/Setting
1	HTTP Basic Authentication
2	Request for Assertion by Identifier / SOAP
3	HTTP Basic Authentication
4	SAML URI Binding

Test Case N – Error Testing

Conformance Modes: IdP, SP, SP Lite

Preconditions: Metadata exchanged and loaded

Test Step Overview

Steps	Action/Message/Setting
1	Artifact Refused
2	Successful Response Message
3	Repost of Assertion
4	Altered data, signature mismatch
5	Wrongkey used to sign
6	SubjectConfirmation Recipient !=assertion service consumer URL
7	Unknown SubjectConfirmationMethod
8	IncorrectAudienceRestriction != requestor
9	SubjectConfirmation NoOnOrAfter expired
10	Unknown Condition

Test Case O – GSA Profile

Preconditions: Metadata exchanged and loaded

Conformance Modes: GSA for both IdP and SP functionality

Test Step Overview

Steps	Action/Message/Setting
1	IdP Discovery
2	Web SSO AuthnRequest / HTTP Redirect (signed)
3	Web SSO AuthnResponse / HTTP POST (signed)
4	SLO SP-initiated / HTTP Redirect(signed)
5	IdP Discovery
6	Web SSO at IdP AuthnResponse / HTTP POST (signed)
7	SLO SP-initiated / HTTP Redirect(signed)

About Drummond Group Inc.

Drummond Group Inc. (DGI) is an independent, privately held company that works with software vendors, vertical industries and the standards community to drive adoption for standards by conducting interoperability and conformance testing, publishing related strategic research and developing vertical industry strategies. Founded in 1999, DGI represents best-of-breed in the industry on linking horizontal infrastructure technologies, standards and interoperability issues with the needs of vertical industries such as retail, grocery, health care, transportation, government and automotive. For more information, please visit www.drummondgroup.com or email: info@drummondgroup.com.