Drummond group

Certification Final Report

SAML 2.0 Interoperability Test

Third Quarter 2009 (3Q09)

Sept. 4, 2009

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

Drummond group

Table of Contents

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 3Q09 (SAML-3Q09) (see Final Test Results). This was the largest SAML full-matrix IOP test event ever sponsored by Liberty Alliance. Full-matrix testing is the best means to verify product group interoperability as it verifies every product can successfully interact and interoperate with the other products of the test group for the test criteria.

This test event was also the first SAML test event to test the eGovernment (eGov) Profile, version 1.5. The eGov profile was a result of pan-government effort to create a viable SAML conformance profile for government identity management.

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.

Sincerely,

Kyle Meadors
SAML IOP Test Administrator
Principal, Test Process
Drummond Group Inc.

Drummond group

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.

10 # Test Participants

Entrust, Inc. http://www.entrust.com/internet-access-control/features.htm **Product Name: Entrust GetAccess 8.0**	Entrust, Inc. http://www.entrust.com/strong-authentication/identityguard/ **Product Name: Entrust IdentityGuard Federation Module 9.2**
IBM Corporation http://www-01.ibm.com/software/tivoli/products/federated-identity-mgr/ **Product Name: IBM Tivoli Federated Identity Manager 6.2**	Microsoft http://www.microsoft.com/geneva **Product Name: Active Directory Federation Services 2.0**
Novell http://www.novell.com/products/accessmanager/ **Product Name: Novell Access Manager 3.1**	Ping Identity http://www.pingidentity.com/products/pingfederate.cfm **Product Name: PingFederate 6.1**
SAP AG http://www.sdn.sap.com/irj/sdn/nw-identitymanagement **Product Name: SAP NetWeaver Identity Management 7.2**	Siemens http://www.siemens.com/iam **Product Name: DirX Access V8.1**

11

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, in which, the product test group exchanges among itself 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

Vendors Entrust, who tested two products, IBM, Microsoft, Novell, Ping, SAP and Siemens participated in the 3Q09 SAML 2.0 interoperability test event. All participants have achieved Liberty Alliance Interoperable certification for the SAML 2.0 3Q09 test event. They performed full-matrix testing over different SAML conformance modes without error or code changes during the SAML 2.0 3Q09 Certification Run on the dates of August 31-September 3 to prove their interoperability. The time preceding the Certification Run, July 14-August 30, 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 Expert Group (TEG). The actual test cases for this test event can be found in this document from the IOP.ProjectLiberty.org webpage.

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 containing a "P" 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.

Product	CONFORMANCE MODES													
	IDP	IDP Lite	IDP Extended	SP	SP Lite	SP Extended	Attribute Authority Requestor	Attribute Authority Responder	Authentication Authority Requestor	Authentication Authority Responder	Authorization Decision Authority Requestor	Authorization Decision Authority Responder	POST Binding	eGov 1.5
Entrust GetAccess	P	P		P	P			P						P
Entrust IdentityGuard	P	P		P	P								P	P
IBM	P	P		P	P		P	P	P	P			P	P
Microsoft		P			P									P
Novell	P	P		P	P								P	P
Ping		P			P									P
SAP		P			P									
Siemens		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.

Entrust GetAccess: IDP, IDP Lite, SP, SP Lite, Attribute Authority Responder, eGov 1.5

Entrust IdentityGuard: IDP, IDP Lite, SP, SP Lite, eGov 1.5, POST Binding

IBM: IDP Lite, SP Lite, Attribute Authority (Requester/Responder), Authentication Authority (Requester/Responder), eGov 1.5, POST Binding

Microsoft: IDP Lite, SP Lite, eGov 1.5

Novell: IDP, IDP Lite, SP, SP Lite, eGov 1.5, POST Binding

Ping: IDP Lite, SP Lite, eGov 1.5

SAP: IDP Lite, SP Lite

Siemens: IDP Lite, SP Lite, Attribute Authority (Requester/Responder), Authentication Authority (Requester/Responder)

Interoperability Test History

This is the third SAML 2.0 interoperability certification event administered by DGI, and it is also the third full-matrix interoperability test event for SAML 2.0. The previous full-matrix interoperability test events are:

- SAML 2.0 3Q08 Interoperability Test Event (July-Sept. 2008)
- SAML 2.0 4Q07 Interoperability Test Event (Oct.-Dec. 2007)

Liberty Alliance has sponsored and administered previous non-full-matrix 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 (Security Assertion Markup Language) allows for communication of identity management among trusted 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 (e.g., through a secure password) only once and this identification is shared among the other trusted 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 modes.

Test Cases and Test Criteria

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 document from the IOP.ProjectLiberty.org webpage.

[SAMLConf] states that SOAP Binding for SLO is optional for SP Lite and IdP Lite applications. In Test Case B, SP Lite and IdP Lite participants may choose to use Redirect Binding for test steps performing SLO actions instead of SOAP Binding. Microsoft chose to use Redirect Binding, and the other SP Lite and IdP Lite participants chose SOAP Binding.

[SAMLConf] states that SOAP Binding for MNI is optional for SP applications. In Test Case D, SP participants may choose to use Redirect Binding for test steps performing MNI actions instead of SOAP Binding. All SP participants chose to use SOAP binding.

[SAMLConf] states that IdP Discovery is optional for SP and SP Lite applications. In Test Case H, SP and SP Lite participants may option out of this test case. All SP and SP Lite participants chose to participate in this test case.

SAML Defined Conformance Modes

SAML 2.0 specifies several operational conformance modes with specific features that are either required or optional for each mode. The details of each mode are provided in [SAMLConf], and the conformance modes available for certification in this test event are listed here:

- IdP – Identity Provider
- IdP Lite – Identity Provider Lite
- SP – Service Provider
- SP Lite – Service Provider Lite

- IdP Extended – Identify Provider Extended
- SP Extended – Service Provider Extended
- SAML Attribute Authority (Requester/Responder)
- SAML Authorization Decision Authority (Requester/Responder)
- SAML Authentication Authority (Requester/Responder)

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.

Optional Liberty Alliance Conformance Modes

POST Binding

Although the POST binding is not included in [SAMLConf], 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.

eGov 1.5 Profile

The eGov 1.5 Profile is a conformance profile developed by Liberty TEG and Liberty eGovernment SIG. The test cases within this test plan to achieve eGov certification are based on the requirements stated in the eGov 1.5 profile. The eGov 1.5 profile should be consulted for further explanation of the eGov requirements.

http://www.projectliberty.org/liberty/liberty_interoperable/documents

Test Cases Associated with Conformance Modes

In order to achieve certification in one or more of the Liberty SAML Conformance Modes, the associated test cases must be completed with all test participants with aligning modes. For example, a product testing for an IdP conformance mode must complete Test Cases A, B, C, D, H, I, J, K and L against all products testing for a SP conformance mode and SP Lite conformance mode (note – Test Case P is a SAML Conformance Error test case where participants interact with an error testing tool). The specific pairing among participants will be given at the beginning of the certification event. A conformance mode may not require completion of all the test steps in the associated test cases. The individual test cases provide details of test steps that may or must be omitted depending on the conformance mode.

Conformance Mode	Test Cases
IdP	A, B, C, D, H, I, J, K, L, P
IdP Extended	F, G
IdP Lite	A, B, H, I, J, K, L, P
SP	A, B, C, D, H, I, J, K, L, P
SP Extended	F, G
SP Lite	A, B, H, I, J, K, L, P
POST	E, P
SAML Attribute Authority (Requester/Responder)	N
SAML Authorization Decision Authority (Requester/Responder)	O
SAML Authentication Authority (Requester/Responder)	M
eGov 1.5 profile	A, B, H, I, J, K, L, P, Q, R, S, T

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 contain standards/implementation issues, on which, the product test group reached consensus in order to achieve interoperability among the group. Some consensus items may be temporary solutions necessary to facilitate interoperability among the group and are noted as such until a standard body can more formally address the concern.

SAML 3Q09 Consensus Items

- An Assertion element does not need to be constructed so that namespace definitions can be validated apart from the enveloping Response message. This was confirmed by OASIS SSTC.
- The Product Test Group accepted this approach for implementing and resolving signatures of Artifact Resolution messages, given the wording from [SAMLCore], section 5.3…
    1. As the test group is using SSL Server-Side Authentication, the responder does not have to sign the <ArtifactResponse> as the responder has authenticated itself.
    2. A responder MAY also add a signature to the <ArtifactResponse> and any requester MUST be able to accept it.
    3. Because of the SHOULD key word from section 5.3, requesters need to add XML Signature to the <ArtifactResolve> message.
- If a responder is authenticated through SSL, the XML signature can be omitted from the SLO Response.
- If an XML Signature is applied to any part of a SAML message, it MUST be verified.
- SAML partner MAY add a valid SPNameQualifier and NameQualifier when building a LogoutRequest even if the IDP omitted them from the NameID included on the assertion.
- After consulting with OASIS SSTC, it was agreed that if a SP (SP-B) returns a non-Success status in a LogoutResponse to an IDP and the IDP is able to terminate the authenticated session, the IDP is to send to any other session

SP (SP-A) a LogoutResponse with a top-level status of Success and a second-level status of PartialLogout. If SP-B does return a Success status to the IDP, the IDP, assuming it is able to terminate the session itself, returns to SP-A a Success status.

The consensus items below are from the previous SAML interoperability test event and applied to the current test event as well.

SAML 3Q08 Consensus Items

- In an authentication request message, an interoperable implementation must accept a RequestedAuthnContext if it can meet the authentication context requirements of the specified element and not require that such information be specified out-of-band.

SAML 4Q07 Consensus Items

- 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. Participants are only to use digital certificates with the required RSAwithSHA1 signature algorithm.
- Ignore EncryptionMethod elements in metadata. There is some confusion of interpretation implementation of the EncryptionMethod metadata elements described in Section 2.4.1.1 of [SAMLMeta]. After confirming with OASIS SSTC, EncryptionMethod is to be ignored.
- Encryption with NameIDPolicy and ID Encryption. A question had arisen on interpreting NameIDPolicy from [SAMLCore] in lines 2136-2142. It was decided 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 Only for SOAP connections. 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 set up in order to achieve interoperability. For all products, proper metadata setup was needed. Basic partner configuration, such as binding to use and security settings, 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.

Entrust GetAccess

With some exceptions, we configured the system to always sign requests and responses and always require and verify signatures for incoming requests and responses.

To validate signatures, Microsoft required that Entrust GetAccess be configured to include the certificate in the signature data in both the IDP and SP

By default GetAccess performs XML type normalization. Some partners do not perform XML type normalization on large binary objects before signing them. This is particularly an issue when encryption is enabled since the signature is calculated after encryption. To address this issue, Entrust GetAccess was configured with XML type normalization disabled for partners Ping, Novell and Siemens in both the IDP and SP.

Microsoft required that Entrust GetAccess be configured to omit the inclusion of the Assertion OneTimeUse option.

By default, encryption of the NameID and Assertion were disabled for each partner. When running TC B/D, Entrust GetAccess configuration had to be changed to enable encryption.

Entrust GetAccess requires that the AuthnContexts used by partners be specified in configuration. The same configuration was used for each partner. The supported AuthnContexts were:

- urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
- urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
- urn:oasis:names:tc:SAML:2.0:ac:classes:Password
- urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransp
- urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified (for Ping only)

Entrust GetAccess includes configuration that maps internal attribute names into SAML Attributes. The same configuration was used for each partner and mapped the required eGov attributes.

When performing TC S, we configured two users in Entrust GetAccess for each partner. One user had the local attributes defined and one did not. For the first user, Entrust GetAccess included the SAML attributes in the assertion. For the second user, Entrust GetAccess did not include the SAML attributes in the assertion.

For MNI, the Entrust GetAccess interop UIs included a page that allowed the partner to perform MNI operations including local removal of the persistent identifier name. MNI links were not provided for the different bindings.

For CDC, the hostname using the CDC domain had to be configured in the Entrust GetAccess configuration. CDC support can be enabled or disabled within Entrust GetAccess. For the interop testing, CDC functionality was enabled for all tests.

When using POST vs. Artifact at the Entrust GetAccess SP (ex. TC J, or TC A/C vs. B/D), Entrust GetAccess needs to be reconfigured and restarted (i.e. it is either POST or Artifact configured per partner).

Entrust IdentityGuard

With some exceptions, we configured the system to always sign requests and responses and always require and verify signatures for incoming requests and responses.

To validate signatures, Microsoft and Siemens required that Entrust IdentityGuard was configured to include the certificate in the signature data in both the IDP and SP

By default Entrust IdentityGuard performs XML type normalization. Some partners do not perform XML type normalization on large binary objects before signing them. This is particularly an issue when encryption is enabled since the signature is calculated after encryption. To address this issue, Entrust IdentityGuard was configured with XML type normalization disabled for partners Ping, Novell and Siemens in both the IDP and SP.

Microsoft required that Entrust IdentityGuard was configured to omit the inclusion of the Assertion OneTimeUse option.

By default, encryption of the NameID and Assertion were disabled for each partner. When running TC B/D, configuration had to be changed to enable encryption. Both the Entrust IdentityGuard IDP and SP interop test interfaces provided a UI to allow the partner to change this configuration.

Entrust IdentityGuard requires that the AuthnContexts used by partners be specified in configuration. The same configuration was used for each partner. The supported AuthnContexts were:

- urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
- urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
- urn:oasis:names:tc:SAML:2.0:ac:classes:Password
- urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

- urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified (for Ping only)

Entrust IdentityGuard includes configuration that maps internal attribute names into SAML Attributes. The same configuration was used for each partner and mapped the required eGov attributes.

When performing TC S, we configured two users in Entrust IdentityGuard for each partner. One user had the local attributes defined and one did not. For the first user, Entrust IdentityGuard included the SAML attributes in the assertion. For the second user, Entrust IdentityGuard did not include the SAML attributes in the assertion.

For MNI, the Entrust IdentityGuard interop UIs for both the IDP and SP included a page that allowed the partner to perform MNI operations including local removal of the persistent identifier name.

Entrust IdentityGuard does not locally logout the user after an MNI terminate. In TC E after step 6, the partner should perform a local logout from Entrust IdentityGuard before performing step 7.

For CDC, the hostname using the CDC domain had to be configured in the Entrust IdentityGuard configuration. CDC support can be enabled or disabled within Entrust IdentityGuard. For the interop testing, CDC functionality was enabled for all tests.

IBM

The configuration is pretty much standard. The only things to point out is that we have setup all partners to do what we call is typical signature validation option when importing metadata to your environments. That means that AuthnResponse and ArtifactResolve signatures are not mandated but will get validated if the document is signed.

Microsoft

AuthnRequest signing was enabled during testing. Except Test Case B, assertion encryption was disabled; the default is to encrypt assertions.

Test Case B was accomplished using SLO over redirect instead of SOAP. When Microsoft is the IDP, some partners would include SPNameQuailifer or NameQualifier in the NamID of the SLO messages. By default AD FS 2.0 does not set these attributes. To enable SLO these attributes were added to the assertions to match what was in the SLO message.

To enable IsPassive and ForceAuthn testing, no changes were required to the IDP. However, these attributes are set on the SP through page customization, calling documented APIs.

NameID encrypting for Test Case B is also a non-default configuration and can be configured according to documentation.

Redirect requests can be configured at the SP by setting the default endpoint on a per IdP basis. The IdP requires no additional configuration to accept redirect binding.

Artifact binding response can be configured at the IdP as the default response, this is required for IdP initiated sign in scenarios. For SP initiated scenarios, the IdP will honor the requested protocolBinding. At the SP a request protocolBinding can be configure per documentation. The same holds for POST responses.

IdP discovery is not enabled by default, but may be deployed following product documentation.

The NameID format returned by the IdP must be configured manually, following documentation.

Novell

Novell's software being tested in the 2009 SAML2 Conformance event is both an SP and an IDP. The product tested, including the User Interface is what ships as part of the product. A configuration utility (which is not part of the product) was used to allow participants to quickly configure the software to operate in modes being tested. A more comprehensive admin utility ships with the Novell IDP, but does not allow for changes to be made quickly on-the-fly. The conformance admin utility allowed setting a subset of functions that the product admin can. Exceptions include:

1. The conformance utility provided a mechanism to specify the binding to be used (SOAP, POST, Redirect) for given tests. The product normally will select the most secure binding to use based on supported bindings identified in provider metadata and those allowed at the Novell IDP. This still required that the binding be supported by both sides.

2. The conformance utility allowed setting “Passive” authentication requests. In the product, this setting is only used when doing Introductions, and can be tested by selecting an authentication option only available when Introducable IDPs are detected.

No other configurations which are not offered by the product were required.

Tests run by Novell were done primarily using Firefox 1.7.5 and IE 7.0.5730.

Ping

With Microsoft, we always include the certificate in signed messages.

IdP Discovery is not enabled by default with PingFederate. You should follow instruction in the Administrator's Manual in the Section on Configuring IdP Discovery to enable this. The endpoint for an SP using IdP Dicovery is /sp/cdcstartSSO.ping.

SAP

Browser:

When testing with Microsoft in test case B we had to explicitly use Firefox because the SLO URLs exceed the maximum supported length by IE 6 and IE 7.

Signature/Encryption:

The default signature settings in SAP NetWeaver Identity Management 7.2 match the requirements for all IdP Lite/SP Lite test cases except for test case B. For SSO profile by default the AuthnRequest will be signed by the SP and only the Assertion will be signed by the IdP (the Response is unsigned). The encryption of Assertions and NameIDs has to be enabled explicitly. All signature and encryption settings are maintained per trusted provider (partner).

Bindings:

The bindings to be used for the different profiles are again configured per trusted provider (partner). By default HTTP-Redirect for AuthnRequest (SSO), HTTP-POST for Response (SSO) and HTTP-Redirect for LogoutRequest/LogoutResponse (SLO) are used. The SP could be configured to require the Response (SSO) over HTTP-Artifact binding. This is done by setting AssertionConsumerServiceIndex attribute in the AuthnRequest.

For SOAP communication (both SLO and ARS profiles) SAP NW IdM 7.2 supports authentication through username/password, client/server certificate and through digital signature of the corresponding SAML protocol messages.

IdP Discovery:

For IdP Discovery, the IdP and SP has to be configured to use external CDC write/read services. Such services come as part of the product. By default their usage is disabled.

ForceAuthn/IsPassive:

The settings for forced authentication (ForceAuthn) and passive authentication (IsPassive) are maintained per web application and apply for all trusted providers (partners).

Siemens

By default, samlp:AuthnRequest elements are digitally signed (can be disabled through a configuration setting). Details regarding the attributes (e.g.

samlp:ForceAuthn, samlp:IsPassive, samlp:AssertionConsumerServiceIndex or samlp:AssertionConsumerServiceURL/samlp:ProtocolBinding) and child elements (e.g. samlp:NameIDPolicy, samlp:RequestedAuthnContext) of samlp:AuthnRequest elements depend on the configuration settings described below.

By default, samlp:Response elements are digitally signed (can be disabled through a configuration setting). Embodied saml:Assertion elements are also digitally signed by default (also configurable) and may be encrypted (i.e. provided as saml:EncryptedAssertion). The actual contents of embodied saml:Assertion elements are subject to:

i. Directives obtained from samlp:AuthnRequest elements received from SPs

ii. Applicable configuration settings esp. the configured saml:Assertion templates. These are product-specific configuration data objects which control the issuance of saml:Assertion elements at a granular level.

iii. Applicable authentication states of acting users. This includes identity management data esp. the user records and their LDAP attributes, transient information obtained from security protocols (e.g. X.509 certificate contents, contents of [other] saml:Assertion elements) used to authenticate at the IdP as well as information produced by the IdP-side authentication process (e.g. assurance level).

By default, samlp:LogoutRequest and samlp:LogoutResponse elements are digitally signed (can be disabled through a configuration setting). In the samlp:LogoutRequest elements, the SAML name identifier can be provided as saml:NameID or saml:EncryptedID element (configurable). The optional child element samlp:SessionIndex and attribute samlp:NotOnOrAfter (case of an IdP) are provided.

The federation configuration can be managed in the Web-based administrative user interface. The underlying configuration subsystem also provides Web services for managing system configuration. The federation configuration settings are managed by an administrator and may be overridden in a request-specific way by actual end users (respectively the applications that support users) as far as SAML protocol primitives support “negotiation” means i.e. allow requesters to provide directives on how to satisfy a request. This concerns features represented by samlp:ForceAuthn, samlp:IsPassive, samlp:Format, samlp:AllowCreate where samlp:AuthnRequest and its child element samlp:NameIDPolicy provide such “negotiation” means.

Support for SSO / SLO exchanges via the HTTP-Redirect binding is activated at deployment time by providing SAML metadata files with md:SingleSignOnService / md:SingleLogoutService endpoints for the HTTP-Redirect binding. No specific

484 configuration for the HTTP-Redirect binding is needed. There are no
485 assumptions on peers beyond their ability to honor the provided configuration
486 contract (SAML metadata file).

487 The same statements/assumptions as for the HTTP-Redirect binding hold for the
488 HTTP-POST and Artifact bindings.

489 The IdP discovery via CDC is a configurable functionality i.e. this functionality
490 needs to be enabled in the configuration subsystem and provided with a setup
491 (esp. common domain name).

492 Support for the attribute query responder is activated at deployment time by
493 providing SAML metadata files with md:AttributeService endpoints. Moreover, the
494 responder needs to be configured with saml:Assertion templates. Structurally
495 these are the same configuration objects as those described above but a
496 md:AttributeService will typically work with different instances of saml:Assertion
497 templates than a md:SingleSignOnService. The saml:Assertion templates allow
498 attribute encryption to be configured on a per-attribute granularity-level (i.e.
499 saml:EncryptedAttribute). Moreover the assertion can be provided in encrypted
500 form i.e. as a saml:EncryptedAssertion

501 The attribute query requester functionality is provided through an SDK i.e. it is
502 envisioned that deployments will integrate the attribute requester in a
503 programmatic way with their own code and create own frontends. A Web
504 frontend for the attribute requester is also supplied as an off-the-shelf application.

505 Support for the authentication query responder is activated at deployment time
506 by providing SAML metadata files with md:AuthnQueryService endpoints. In
507 contrast to the attribute query responder (which is working with saml:Assertion
508 templates) no further configuration setup is needed.

509 For the authentication query requester the same statements as for the attribute
510 query requester hold.

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.

During testing, participants reported problems using Microsoft Internet Explorer (IE) browser when encountering long URL values in HTTP Redirect bindings. IE does not accept URLs longer than 2083 characters (http://support.microsoft.com/kb/208427). This was particularly an issue when encryption was enabled in Test Cases B/D which results in very long URLs stings. Participants worked around this limitation by using a browser other than IE.

Also, a participant reported that it was necessary to accept their self-signed common domain certificate prior to executing Test Case H for IdP Discovery. If not and the certificate was accepted when redirected to the common domain URL, IE would redirect the user back to the original URL after the certificate was accepted.

Entrust GetAccess: Primarily used IE 7 (7.0.5730.13), FireFox 3.5.2 and Google Chrome 0.2.149.29

Entrust IdentityGuard: Primarily used Firefox 3.0 and 3.5 in testing. Also used IE 7, IE 8 and Google Chrome 2.0.

IBM: Firefox 3.0.13

Microsoft: Majority of testing was done with Internet Explorer 8, additional testing was done with Firefox 3.5.2

Novell: Primarily using Firefox 1.7.5 and IE 7.0.5730

Ping: Firefox 3.0.1 and IE 7.0

SAP: IE 6, IE 7, Firefox 3.5

Siemens: Firefox 3.5.2 and Internet Explorer 7.0

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]. Participants were responsible for creating their own certificates for testing.

Technical Requirements

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 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

This ordering should be observed by all implementations testing SAML modes where authentication contexts must be compared. The overall concept of the testing of the Authentication Authority is to create several different assertions using different authentication contexts. Then these are queried using the query terms (“exact”, “better”, “maximum”, “minimum”) and a reference authentication context.

NOTE: 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 was 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. Single Logout: The <LogoutRequest> and <LogoutResponse> MUST be signed for the HTTP redirect binding.
3. Name Identifer Management: The <ManageNameIDRequest> and <ManageNameIDResponse> MUST be signed for the HTTP redirect binding.

Note that when a test step refers to a “signed SAML Response message” this implies the assertion element itself is signed per the requirements in [SAMLProf].

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. Instead, they rely on successful interoperability as a measure of conformance.

Implementations should take care to ensure that elements to be encrypted include any XML namespace prefix declarations so that, when decrypted, the element will remain valid independent of context. One method for achieving this is described in [ExcXMLCan], but other approaches will work as well.

Note that, while the <ds:KeyInfo> and <xenc:EncryptedKey> elements are not required in the SAML specifications or related schemas, these elements MUST be included in messages for interoperability testing. There is no normative mechanism for exchanging these keys out-of-band. The precise location of these elements in the message is underspecified; the most common practice among

interoperable SAML implementations is that, in each encrypted element, there be one <xenc:EncryptedKey> element in parallel with the <xenc:EncryptedData>, and that this <xenc:EncryptedKey> be inferred as the relevant key information for decryption without relying on any references within the sub-elements. An erratum has been created to clarify this; see PE43 in [SAMLErrata]. For this certification event, this most common practice stated above SHOULD be done.

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

Attribute Profiles

[SAMLConf] makes no normative statements about which Attribute Profiles in [SAMLProf] are required to be supported by SAML Attribute Authority. This document only describes testing procedures for the Basic profile, and does not describe any testing procedures regarding other 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 is 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] Eve Maler, et al, "Errata for the OASIS Security 2 Assertion Markup Language (SAML) V2.0, Working Draft 28," OASIS SSTC (August 14, 2007), http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.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.

Drummond group

About Drummond Group Inc.

Drummond Group Inc. (DGI) is the trusted interoperability test lab offering global testing services through the product life cycle. Auditing, QA, conformance testing, custom software test lab services, and consulting are offered in addition to interoperability testing. Founded in 1999, DGI has tested over a thousand international software products used in vertical industries such as automotive, consumer product goods, healthcare, energy, financial services, government, petroleum, pharmaceutical and retail. For more information, please visit www.drummondgroup.com or email: info2@drummondgroup.com.