

Certification Final Report
SAML 2.0 Interoperability Test
Fourth Quarter 2007 (4Q07)

Dec. 13, 2007

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

Table of Contents

Cover Letter	4
Disclaimer	5
Test Participants	6
Definitions	7
Interoperability Test Summary	8
Overview of Test Event	8
Final Test Results	9
Interoperability Test History	10
About SAML 2.0	10
About Liberty Alliance	10
Test Case and Conformance Mode Summary	11
Test Case and Conformance Mode Summary: Overview	11
SAML Defined Conformance Modes	11
Optional Liberty Alliance Conformance Modes	12
SP Complete	12
POST Binding	12
GSA Profile	12
Test Cases Associated with Conformance Modes	13
Interoperability Caveats	14
Consensus Items	14
Configuration Setup	15
HP	15
IBM	15
RSA	16
Sun	16
Symlabs	17
Browser Usage	17
Testing Requirements	18
Trading Partner Requirements	18
Metadata	18
Technical Requirements	18
General Test Case Requirements	18
IdP Authentication	19
Trivial Processing	19
Authentication Contexts	19
Name Identifier Formats	20
XML Signatures	20
XML Encryption	20
Attribute Profiles	21
Overview of the DGI Interoperability Compliance Process®	22
DGI Interoperability Test Round	22
References	23
Appendix A: Test Case Details	25
Test Case A – Redirect Binding	25
Test Case B – SOAP Binding	26
Test Case C – POST Binding	27
Test Case D – Extended SAML Modes	28
Test Case E – IDP Introduction	29
Test Case F – Single Session Logout	30

Test Case G – Unsolicited <Response>.....	31
Test Case H – Affiliations.....	32
Test Case I – ECP	33
Test Case J – SAML Authentication Authority.....	34
Test Case K – SAML Attribute Authority.....	35
Test Case L – SAML Authorization Decision Authority	36
Test Case M – Request for Assertion by ID and SAML URI Binding	37
Test Case N – Error Testing	38
Test Case O – GSA Profile.....	39
About Drummond Group Inc.....	40

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.


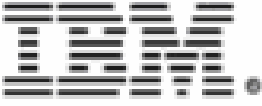



Sincerely,

Rik Drummond
CEO,
Drummond Group Inc.

1 **Disclaimer**

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

10 Test Participants

 <p>Hewlett-Packard</p> <p>http://www.hp.com/</p> <p>Product Name: Select Federation 7.0 patch1</p>	 <p>IBM Corporation</p> <p>http://www.ibm.com/</p> <p>Product Name: Tivoli Federated Identity Manager version 6.2</p>
 <p>RSA, The Security Division of EMC</p> <p>The Security Division of EMC</p> <p>http://www.rsa.com/</p> <p>Product Name: RSA Federated Identity Manager 4.0</p>	 <p>Sun Microsystems, Inc.</p> <p><i>The Network is the Computer™</i></p> <p>http://www.sun.com/</p> <p>Product Name: Sun Java System Federated Access Manager 8.0</p>
 <p>Symlabs, Inc.</p> <p><i>Identity Management Infrastructure</i></p> <p>http://www.symlabs.com/</p> <p>Product Name: Symlabs Federated Identity Suite version 3.3.0</p>	

11

12 **Definitions**

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

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

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

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

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

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

44 Interoperability Test Summary

45 Overview of Test Event

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

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

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

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

75 Finally, this report contains sections describing the [trading partner requirements](#)
76 and [technical requirements](#) given to the participants in order to complete full-
77 matrix interoperability testing, as well as a section summarizing the [DGI](#)
78 [Interoperability and Compliance Process](#).

79 Final Test Results

80 The table below shows the interoperable products and the conformance modes
 81 they successfully tested. The green boxes with the “P” within them indicate the
 82 participant passed certification requirements in the corresponding conformance
 83 mode. The actual product version-with-release information can be found in the
 84 [Test Participant](#) section.

85

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

86

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

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

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

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

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

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

102 **Interoperability Test History**

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

108 **About SAML 2.0**

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

117 **About Liberty Alliance**

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

123 **Test Case and Conformance Mode Summary**

124 **Test Case and Conformance Mode Summary: Overview**

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

131 **SAML Defined Conformance Modes**

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

- 135 • IdP – Identity Provider
- 136 • IdP Lite – Identity Provider Lite
- 137 • SP – Service Provider
- 138 • SP Lite – Service Provider Lite
- 139 • ECP – Enhanced Client/Proxy
- 140 • IdP Extended – Identify Provider Extended
- 141 • SP Extended – Service Provider Extended
- 142 • SAML Attribute Authority
- 143 • SAML Authorization Decision Authority
- 144 • SAML Authentication Authority
- 145 • SAML Requester

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

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

154

155 **Optional Liberty Alliance Conformance Modes**

156 **SP Complete**

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

163 **POST Binding**

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

169 **GSA Profile**

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

175 **Test Cases Associated with Conformance Modes**

176 In order to achieve certification in one or more of the SAML Conformance Modes,
 177 the associated test cases had to be completed with all test participants with
 178 aligning modes. Aligning modes are modes which are used in conjunction with
 179 each other. For example, a product testing for an IdP conformance mode must
 180 complete Test Cases A, B, C, E, F, G, H and I against all products testing for a
 181 SP conformance mode. The individual test cases provide details of who each
 182 mode interacts with each other and test steps that may or must be omitted
 183 depending on the conformance mode.
 184

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

185 **Interoperability Caveats**

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

190 **Consensus Items**

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

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

221 **Configuration Setup**

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

231 **HP**

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

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

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

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

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

254 **IBM**

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

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

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

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

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

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

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

270 **RSA**

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

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

279 **Sun**

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

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

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

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

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

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

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

296 **Symlabs**

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

300 ECP is a stand-alone enhanced client. Symlabs-ECP uses x-msisdh trusted
301 header.

302 **Browser Usage**

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

306 HP: Firefox, vs. 2.0.0.7

307 IBM: Firefox, vs. 1.5/2.x

308 RSA: Firefox, vs. 2.0.0.7 and IE 6.0

309 Sun: Firefox, vs. 1.5.0.4

310 Symlabs: Firefox, vs. 2.0.0.11

311 **Testing Requirements**

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

314 **Trading Partner Requirements**

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

324 **Metadata**

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

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

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

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

338 **Technical Requirements**

339 **General Test Case Requirements**

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

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

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

347 **IdP Authentication**

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

- 353 1. HTTP Basic Auth.
- 354 2. HTTP Form Post
- 355 3. HTTP Get

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

358 **Trivial Processing**

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

365 **Authentication Contexts**

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

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

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

379 **Name Identifier Formats**

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

- 381 1. Unspecified
- 382 2. Email
- 383 3. X.509 Subject
- 384 4. Windows
- 385 5. Kerberos
- 386 6. Entity
- 387 7. Persistent
- 388 8. Transient

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

391 **XML Signatures**

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

- 395 1. Web SSO: The assertion element(s) in the <Response> MUST be signed
396 for the HTTP POST binding.
- 397 2. ECP Profile: The assertion element(s) in the <Response> issued by the
398 IdP MUST be signed.
- 399 3. Single Logout: The <LogoutRequest> and <LogoutResponse> MUST be
400 signed for the HTTP redirect binding.
- 401 4. Name Identifier Management: The <ManageNameIDRequest> and
402 <ManageNameIDResponse> MUST be signed for the HTTP redirect
403 binding.

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

407 **XML Encryption**

408 [SAMLConf] stipulates several different encryption algorithms and key transport
409 mechanisms that MUST be implemented. However, these testing procedures do
410 not require demonstration of support for all these combinations and instead rely
411 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.

421 **Overview of the DGI Interoperability Compliance**
422 **Process®**

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

428 **DGI Interoperability Test Round**

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

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

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

444 **References**

- 445 [SAMLAuthnCxt] J. Kemp et al, "Authentication Context for the OASIS
446 Security Assertion Markup Language (SAML) V2.0," OASIS
447 SSTC (March 2005), [http:// docs.oasis-
448 open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf).
- 449 [SAMLConf] Prateek Mishra et al, "Conformance Requirements for the
450 OASIS Security Assertion Markup Language (SAML) V2.0,"
451 OASIS SSTC (March 2005). [http://docs.oasis-
452 open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf).
- 453 [SAMLCore] S. Cantor et al, "Assertions and Protocols for the OASIS
454 Security Assertion Markup Language (SAML) V2.0," OASIS
455 SSTC (March 2005), [http://docs.oasis-
456 open.org/security/saml/v2.0/saml-core-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf).
- 457 [SAMLErrata] Jahan Moreh, "Errata for the OASIS Security 2 Assertion
458 Markup Language (SAML) V2.0, Working Draft 28," OASIS
459 SSTC (May 8, 2006), [http://www.oasis-
460 open.org/committees/download.php/18070/sstc-saml-errata-
461 2.0-draft-28.pdf](http://www.oasis-open.org/committees/download.php/18070/sstc-saml-errata-2.0-draft-28.pdf)
- 462 [SAMLMeta] S. Cantor et al, "Metadata for the OASIS Security Assertion
463 Markup Language (SAML) V2.0," OASIS SSTC (March
464 2005), [http://docs.oasis-open.org/security/saml/v2.0/saml-
465 metadata-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf).
- 466 [SAMLMetaExt] Tom Scavo et al, "SAML Metadata Extension for Query
467 Requesters, Committee Draft 01", OASIS SSTC (March
468 2006), [http://www.oasis-
469 open.org/committees/download.php/18052/sstc-saml-
470 metadata-ext-query-cd-01.pdf](http://www.oasis-open.org/committees/download.php/18052/sstc-saml-metadata-ext-query-cd-01.pdf)
- 471 [SAMLProf] S. Cantor et al, "Profiles for the OASIS Security Assertion
472 Markup Language (SAML) V2.0," OASIS SSTC (March
473 2005), [http://docs.oasis-open.org/security/saml/v2.0/saml-
474 profiles-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf).
- 475 [GSATechAppr] Dave Silver et al, "Technical Approach for the Authentication
476 Service Component" vs. 2.0.0 GSA (May 2007),
477 <http://www.cio.gov/eauthentication/TechnicalArchitecture.htm>
- 478 [GSAAadoptSchm] Dave Silver et al, "E-Authentication Federation Adopted
479 Schemes" vs. 1.0.0 GSA (May 2007),
480 <http://www.cio.gov/eauthentication/TechnicalArchitecture.htm>

481 [GSAInterface] Dave Silver et al, "E-Authentication Federation Architecture
482 2.0 Interface Specifications" vs. 1.0.0 GSA (May 2007),
483 <http://www.cio.gov/eauthentication/TechnicalArchitecture.htm>

484 **Appendix A: Test Case Details**

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

489 **Test Case A – Redirect Binding**

490 Preconditions: Metadata exchanged and loaded

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

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

494 **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 Namelds
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

496 **Test Case B – SOAP Binding**

497 Preconditions: Metadata exchanged and loaded

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

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

501

502 **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)

503 **Test Case C – POST Binding**
 504 Preconditions: Metadata exchanged and loaded
 505 Conformance Modes: POST Binding for both IdP and SP functionality.

506
 507 **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)

508 **Test Case D – Extended SAML Modes**

509 Preconditions: Metadata exchanged and loaded

510 Conformance Modes: IdP Extended, SP Extended

511

512 **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

513 **Test Case E – IDP Introduction**

514 Preconditions: Metadata exchanged and loaded

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

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

518 **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

519 **Test Case F – Single Session Logout**

520 Preconditions: Metadata exchanged and loaded

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

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

524

525 **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

526 **Test Case G – Unsolicited <Response>**

527 Preconditions: Metadata exchanged and loaded

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

529

530 **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)

531 **Test Case H – Affiliations**

532 Preconditions: Metadata exchanged and loaded

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

534

535 **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]

536 **Test Case I – ECP**

537 Preconditions: Metadata exchanged and loaded

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

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

544

545 **Test Step Overview**

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

546 **Test Case J – SAML Authentication Authority**

547 Conformance Modes: SAML Authentication Authority, SAML Requester

548 Preconditions: Metadata exchanged and loaded

549 Note: Section [[AuthenticationContexts](#)] within this document describes the
550 strength of the AuthnContext classes used for comparison.
551

552 **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

553 **Test Case K – SAML Attribute Authority**

554 Conformance Modes: SAML Attribute Authority, SAML Requester

555 Preconditions: Metadata exchanged and loaded

556

557 **Test Step Overview**

558

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

559 **Test Case L – SAML Authorization Decision Authority**

560 Conformance Modes: SAML Authorization Decision Authority, SAML Requester

561 Preconditions: Metadata exchanged and loaded

562

563 **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

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

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

568 Preconditions: Metadata exchanged and loaded

569

570 **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

571 **Test Case N – Error Testing**

572 Conformance Modes: IdP, SP, SP Lite

573 Preconditions: Metadata exchanged and loaded

574

575 **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

576 **Test Case O – GSA Profile**

577 Preconditions: Metadata exchanged and loaded

578 Conformance Modes: GSA for both IdP and SP functionality

579

580 **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)

581 **About Drummond Group Inc.**

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