

Certification Final Report
SAML 2.0 Interoperability Test
Third Quarter 2008 (3Q08)

Sept. 17, 2008

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

Table of Contents

Cover Letter	3
Disclaimer	4
Test Participants	5
Definitions	6
Interoperability Test Summary	7
Overview of Test Event	7
Final Test Results	8
Interoperability Test History	9
About SAML 2.0	9
About Liberty Alliance	9
Test Case and Conformance Mode Summary	10
Test Case and Conformance Mode Summary: Overview	10
Test Cases and Test Criteria	10
SAML Defined Conformance Modes	10
Optional Liberty Alliance Conformance Modes	11
POST Binding	11
eGov Profile	11
Test Cases Associated with Conformance Modes	12
Interoperability Caveats	13
Consensus Items	13
Configuration Setup	14
CA	14
NTT Software	14
Ping	15
RSA	15
Ubisecure	15
Browser Usage	16
Testing Requirements	17
Trading Partner Requirements	17
Metadata	17
Technical Requirements	17
General Test Case Requirements	17
IdP Authentication	18
Trivial Processing	18
Authentication Contexts	18
Name Identifier Formats	19
XML Signatures	19
XML Encryption	20
Attribute Profiles	20
Overview of the DGI Interoperability Compliance Process®	21
DGI Interoperability Test Round	21
References	22
About Drummond Group Inc.	24

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 3Q08 (SAML-3Q08) (see [Final Test Results](#)). This was the second Liberty Alliance sponsored SAML test event to require full-matrix interoperability between all products. Full-matrix testing certifies all of the products work with each other product 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.

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>CA Inc.</p> <p>http://www.ca.com/</p> <p>Product Name: CA SiteMinder Federation Security Services r12.1</p>	 <p>NTT Software Corporation</p> <p>http://www.nttsoft.com/</p> <p>Product Name: TrustBind/Federation Manager version 1.1</p>
 <p>Ubisecure Solutions, Inc.</p> <p>http://www.ubisecure.com/</p> <p>Product Name: Ubilogin SSO version 5.0</p>	 <p>Ping Identity</p> <p>http://www.pingidentity.com/</p> <p>Product Name: Ping Identity PingFederate® 5.2</p>
 <p>The Security Division of EMC</p> <p>http://www.rsasecurity.com/</p> <p>Product Name: RSA Federated Identity Manager version 4.1</p>	<p>RSA Security, The Security Division of EMC</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, in
38 which, the product test group exchanges among itself to verify conformance and
39 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 Vendors CA, NTT Software, Ping, RSA and Ubisecure participated in the 3Q08
47 SAML 2.0 interoperability test event. All participants have achieved Liberty
48 Alliance Interoperable certification for the SAML 2.0 3Q08 test event. They
49 performed full-matrix testing over different SAML conformance modes without
50 error or code changes during the SAML 2.0 3Q08 Certification Run on the dates
51 of September 2-4 to prove their interoperability. The time preceding the
52 Certification Run, July 14-August 29, was set aside for debugging interoperability
53 issues. The list of products and the conformance modes they certified for can be
54 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 [document](#) from the IOP.ProjectLiberty.org webpage.

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 containing a “P” 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												
	IDP	IDP Lite	SP	SP Lite	ECP	Attribute Authority Requestor	Attribute Authority Responder	Authentication Authority Requestor	Authentication Authority Responder	SP Extended	IDP Extended	POST Binding	eGov
CA Inc.		P		P									P
NTT Software	P		P		P	P	P	P	P	P	P	P	P
Ping Identity		P		P									
RSA Security	P	P	P	P		P	P	P	P			P	P
Ubisecure Solutions	P	P	P	P						P	P	P	

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

88 CA: IDP Lite, SP Lite, eGov

89 NTT Software: IDP, SP, SP Extended, IDP Extended, ECP, Attribute Authority
 90 (Requester/Responder), Authentication Authority (Requester/Responder), POST
 91 Binding, eGov

92 Ping: IDP Lite, SP Lite,

93 RSA: IDP, IDP Lite, SP, SP Lite, Attribute Authority (Requester/Responder),
94 Authentication Authority (Requester/Responder), POST Binding, eGov
95 Ubisecure: IDP, IDP Lite, SP, SP Lite, SP Extended, IDP Extended, POST
96 Binding

97 **Interoperability Test History**

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

- 101 • SAML 2.0 4Q07 Interoperability Test Event (Oct-Dec 2007)

102 Liberty Alliance has sponsored and administered previous non-full-matrix SAML
103 2.0 certification events. Please refer to the Liberty Alliance website for more
104 information on those past test events.

105 **About SAML 2.0**

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

114 **About Liberty Alliance**

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

120 **Test Case and Conformance Mode Summary**

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

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

128 **Test Cases and Test Criteria**

129 The test criteria and the subsequent test cases cover all the conformance modes
130 for this test event and were approved by the Liberty Alliance Technology
131 Engineering Group (TEG). The actual test cases for this test event can be found
132 in this [document](#) from the IOP.ProjectLiberty.org webpage.

133 **SAML Defined Conformance Modes**

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

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

148 The test plan requirements for certification in SP Lite and IdP Lite conformance
149 modes are a subset of the requirements for SP and IdP conformance modes.
150 Thus, completion of the requirements for SP and IdP conformance modes

151 automatically cover the requirements for SP Lite and IdP Lite conformance
152 modes. After the test was completed, participants who certified in SP or IdP
153 conformance modes were given the opportunity to notify DGI and Liberty that
154 their products allow the user to switch between SP and SP Lite modes as well as
155 IdP and IdP Lite modes. Those participants who did were given certification
156 status in both SP and SP Lite modes as well as IdP and IdP Lite modes.

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

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

165

166 **Optional Liberty Alliance Conformance Modes**

167 **POST Binding**

168 Although the POST binding is not included in the SAML SCR, it is permitted with
169 the SAML specification and has some user deployment. POST Binding is an
170 optional Liberty Alliance designation conformance mode. It involves use of POST
171 binding for AuthnRequest, Name ID Management and SLO.

172 **eGov Profile**

173 The eGov Profile follows the SAML 2.0 requirements for the General Service
174 Administration (GSA) of the US Government. The technical requirements for this
175 test case come from the GSA SAML Profile in [GSAInterface], [GSAAdoptSchm]
176 and [GSATechAppr]. These documents should be consulted for further
177 explanation of the GSA requirements.

178 **Test Cases Associated with Conformance Modes**

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

188 IdP Lite and SP Lite modes require only a subset of the test steps in Test Cases
 189 A, B, E and F in accordance to the SAML Conformance [SAMLConf]
 190 requirements. Refer to the Test Plan [document](#) for details.
 191

Conformance Mode	Test Cases
IdP	A, B, E, F, G, H, I, J, K, P
IdP Extended	D
IdP Lite	A*, B*, E*, F*, G, H, I, J, K
SP	A, B, E, F, G, H, I, J, K, P
SP Extended	D
SP Lite	A*, B*, E*, F*, G, H, I, J, K, P
ECP	K
POST	C, P
SAML Attribute Authority	M, O
SAML Authorization Decision Authority	N, O
SAML Authentication Authority	L, O
eGov	Q

192 * - Denotes a subset of the test case and not all steps.

193 **Interoperability Caveats**

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

198 **Consensus Items**

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

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

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

- 210 • DSAwithSHA1 signature algorithm not supported. Section 4.1 of [SAMLConf]
211 states that the DSAwithSHA1 signature algorithm, while recommended, is not
212 required by SAML 2.0. Participants are only to use digital certificates with the
213 required RSAwithSHA1 signature algorithm.
- 214 • Ignore EncryptionMethod elements in metadata. There is some confusion of
215 interpretation implementation of the EncryptionMethod metadata elements
216 described in Section 2.4.1.1 of [SAMLMeta]. After confirming with OASIS
217 SSTC, EncryptionMethod is to be ignored.
- 218 • Encryption with NameIDPolicy and ID Encryption. A question had arisen on
219 interpreting NameIDPolicy from [SAMLCore] in lines 2136-2142. It was
220 decided that if NameIDPolicy of AuthnRequest says ID is to be encrypted, it
221 must be encrypted in the assertion, and if NameIDPolicy of AuthnRequest
222 does not state the ID is to be encrypted, the IDP MAY still encrypt the ID
223 based on its policy, specifically its policy with the SP.
- 224 • SSL Server-side Authentication Only for SOAP connections. To insure all
225 participants used the same security settings, it was agreed to only use SSL
226 server-side authentication for SOAP connections and not to use SSL client-
227 side authentication.

228 **Configuration Setup**

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

238 **CA**

239 CA SiteMinder signs the content of the assertion, but does not specifically sign
240 the Artifact resolve message.

241 SiteMinder expects the other participants to access SiteMinder resources using
242 FQDN and not IP address.

243 When authenticating the requester, SiteMinder supports back channel
244 authentication instead of Artifact query signing / verification.

245 SiteMinder is both a Web Access management tool and a Federation gateway.
246 When a user logs into SiteMinder for web access management, the CDC cookie
247 is not immediately created by default. In this use case, SiteMinder must be
248 configured to create the CDC cookie. This can be done by redirecting a user to
249 the SiteMinder setIPDCookie service using a Siteminder redirect response. For
250 retrieving the information from a common domain cookie,
251 “/affwebservices/public/IdPDiscovery.jsp” was used.

252 When working with the NTT Software ECP, it was observed that the FQDN was
253 added to the URI of the inbound request. This was causing some URI mapping
254 issues within our Servlet container. To remedy this, the URI stems for the
255 assertion consumer services were replicated to include the FQDN. The only
256 configuration difference for communicating through an ECP instead of direct
257 browser based federation was that a Proxy checkbox had to be enabled in the
258 SiteMinder auth scheme and the affiliate. If this checkbox was enabled for non
259 ECP testing, no negative results were observed.

260 **NTT Software**

261 For IDP Proxy, IDP must be configured to enable proxy.

262 For IDP Discovery, IDP must be configured to enable common domain cookie,
263 and SP uses an Interface to read the cookie from common domain.

264 The ECP is a standalone proxy. It supports the form based (user/password)
265 authentication and maintains the cookie based session between browser and
266 server.

267 HTTP Basic Authentication was enabled for SAML URI binding requester test at
268 both Attribute Authority and Authentication Authority.

269 **Ping**

270 IdP Discovery is not enabled by default with PingFderate. Following instructions
271 in Section Configuring IdP Discovery of the Administrator's Manual to configure
272 IdP Discovery. The endpoint for SP using IdP Discovery is /sp/cdcstartSSO.ping.

273 For working with NTT Software ECP, the related bindings (PAOS and SOAP)
274 need to be configured.

275 **RSA**

276 Partners need to decide the AuthnContext out of the band.

277 For ECP connecting to the RSA SP, ECP needs to authenticate SP. This will be
278 form based authentication. Also, ECP client has to be cookie aware because
279 RSA authentication manager on SP would create cookie after authentication and
280 authorization to resource is based on whether cookie is set. RSA SP must set a
281 default IDP to send ECP request. The code to authenticate the user at RSA IDP
282 was given to the NTT Software.

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

285 **Ubisecure**

286 The default settings of Ubisecure SP and IDP matched mostly the requirements
287 for interoperability in the test cases. A test driver application was used with the
288 IDP to configure the IDP for the different test cases, with settings such as
289 bindings, encryption, affiliation, etc. The configuration options that the test driver
290 used are also available in the standard IDP management application.

291 For signature validation, a configuration option in Ubisecure SP was used to
292 disable signature validation of top-level Response and ArtifactResponse
293 messages, where an embedded signed Assertion existed.

294 The metadata files produced by Ubisecure SP and IDP were converted to include
295 X.509 certificates and to specify the "use" attribute for the KeyDescriptor
296 element.

297 By default, the metadata only contained the RSAKeyValue element. Also if the
298 entity supports both signing and encryption, then the use attribute of the
299 KeyDescriptor element is not specified. In the future, the default operation is

300 expected to change to allow producing metadata files as were used in the
301 interop.

302 For ECP testing, the Ubisecure IDP uses HTTP basic authentication.

303 A CDC cookie reader and writer application was installed in the CDC domain
304 ubisecure.cot.projectliberty.org. The url of the CDC application was configured to
305 Ubilogin IDP and SP.

306 **Browser Usage**

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

310 CA: Firefox 3.0.1, IE 6

311 NTT Software: Firefox 3.0.1, IE 7

312 Ping: FireFox 2.0 and IE 7.0. Used Firefox only with NTT Software.

313 RSA: IE 7, Firefox 2, Firefox 3

314 Ubisecure: IE 7, Firefox 2, Firefox 3

315 **Testing Requirements**

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

318 **Trading Partner Requirements**

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

328 **Metadata**

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

- 332 • Furnish correct metadata, and
- 333 • Process metadata furnished by other testing partners.

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

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

342 **Technical Requirements**

343 **General Test Case Requirements**

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

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

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

351 **IdP Authentication**

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

- 357 1. HTTP Basic Auth.
- 358 2. HTTP Form Post
- 359 3. HTTP Get

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

362 **Trivial Processing**

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

369 **Authentication Contexts**

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

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

380 This ordering should be observed by all implementations testing SAML modes
381 where authentication contexts must be compared. The overall concept of the
382 testing of the Authentication Authority is to create several different assertions
383 using different authentication contexts. Then these are queried using the query

384 terms (“exact”, “better”, “maximum”, “minimum”) and a reference authentication
385 context.

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

390 **Name Identifier Formats**

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

- 392 1. Unspecified
- 393 2. Email
- 394 3. X.509 Subject
- 395 4. Windows
- 396 5. Kerberos
- 397 6. Entity
- 398 7. Persistent
- 399 8. Transient

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

402 **XML Signatures**

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

- 406 1. Web SSO: The assertion element(s) in the <Response> MUST be signed
407 for the HTTP POST binding.
- 408 2. ECP Profile: The assertion element(s) in the <Response> issued by the
409 IdP MUST be signed.
- 410 3. Single Logout: The <LogoutRequest> and <LogoutResponse> MUST be
411 signed for the HTTP redirect binding.
- 412 4. Name Identifier Management: The <ManageNameIDRequest> and
413 <ManageNameIDResponse> MUST be signed for the HTTP redirect
414 binding.

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

418 **XML Encryption**

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

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

427 Note that, while the <ds:KeyInfo> and <xenc:EncryptedKey> elements are not
428 required in the SAML specifications or related schemas, these elements MUST
429 be included in messages for interoperability testing. There is no normative
430 mechanism for exchanging these keys out-of-band. The precise location of these
431 elements in the message is underspecified; the most common practice among
432 interoperable SAML implementations is that, in each encrypted element, there be
433 one <xenc:EncryptedKey> element in parallel with the <xenc:EncryptedData>, and that this
434 <xenc:EncryptedKey> be inferred as the relevant key information for decryption without
435 relying on any references within the sub-elements. An erratum has been created to clarify this;
436 see PE43 in [SAMLErrata]. For this certification event, this most common practice stated above
437 SHOULD be done.

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

441 **Attribute Profiles**

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

447 **Overview of the DGI Interoperability Compliance**
448 **Process®**

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

454 **DGI Interoperability Test Round**

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

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

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

470 **References**

- 471 [SAMLAuthnCxt] J. Kemp et al, "Authentication Context for the OASIS
472 Security Assertion Markup Language (SAML) V2.0," OASIS
473 SSTC (March 2005), [http:// docs.oasis-
474 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).
- 475 [SAMLConf] Prateek Mishra et al, "Conformance Requirements for the
476 OASIS Security Assertion Markup Language (SAML) V2.0,"
477 OASIS SSTC (March 2005). [http://docs.oasis-
478 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).
- 479 [SAMLCore] S. Cantor et al, "Assertions and Protocols for the OASIS
480 Security Assertion Markup Language (SAML) V2.0," OASIS
481 SSTC (March 2005), [http://docs.oasis-
482 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).
- 483 [SAMLErrata] Eve Maler, et al, "Errata for the OASIS Security 2 Assertion
484 Markup Language (SAML) V2.0, Working Draft 28," OASIS
485 SSTC (August 14, 2007), [http://docs.oasis-
486 open.org/security/saml/v2.0/sstc-saml-approved-errata-
487 2.0.pdf](http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf).
- 488 [SAMLMeta] S. Cantor et al, "Metadata for the OASIS Security Assertion
489 Markup Language (SAML) V2.0," OASIS SSTC (March
490 2005), [http://docs.oasis-open.org/security/saml/v2.0/saml-
491 metadata-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf).
- 492 [SAMLMetaExt] Tom Scavo et al, "SAML Metadata Extension for Query
493 Requesters, Committee Draft 01", OASIS SSTC (March
494 2006), [http://www.oasis-
495 open.org/committees/download.php/18052/sstc-saml-
496 metadata-ext-query-cd-01.pdf](http://www.oasis-open.org/committees/download.php/18052/sstc-saml-metadata-ext-query-cd-01.pdf)
- 497 [SAMLProf] S. Cantor et al, "Profiles for the OASIS Security Assertion
498 Markup Language (SAML) V2.0," OASIS SSTC (March
499 2005), [http://docs.oasis-open.org/security/saml/v2.0/saml-
500 profiles-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf).
- 501 [GSATechAppr] Dave Silver et al, "Technical Approach for the Authentication
502 Service Component" vs. 2.0.0 GSA (May 2007),
503 <http://www.cio.gov/eauthentication/TechnicalArchitecture.htm>
- 504 [GSAAadoptSchm] Dave Silver et al, "E-Authentication Federation Adopted
505 Schemes" vs. 1.0.0 GSA (May 2007),
506 <http://www.cio.gov/eauthentication/TechnicalArchitecture.htm>

507 [GSAInterface] Dave Silver et al, "E-Authentication Federation Architecture
508 2.0 Interface Specifications" vs. 1.0.0 GSA (May 2007),
509 <http://www.cio.gov/eauthentication/TechnicalArchitecture.htm>

510 **About Drummond Group Inc.**

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