



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

**Sept. 17, 2008**

Prepared & Administered by:  
DRUMMOND GROUP INC.  
[www.drummondgroup.com](http://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
Oracle .....	15
Ping .....	15
RSA .....	15
Ubisecure .....	16
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><a href="http://www.ca.com/">http://www.ca.com/</a></p> <p><b>Product Name: CA SiteMinder Federation Security Services r12.1</b></p>	<p><b>NTT SOFT</b></p> <p>NTT Software Corporation</p> <p><a href="http://www.nttsoft.com/">http://www.nttsoft.com/</a></p> <p><b>Product Name: TrustBind/Federation Manager version 1.1</b></p>
<p><b>ORACLE®</b> Oracle</p> <p><a href="http://www.oracle.com/">http://www.oracle.com/</a></p> <p><b>Product Name: Oracle Identity Federation 11.1.1</b></p>	<p><b>PingIdentity™</b> Ping Identity</p> <p><a href="http://www.pingidentity.com/">http://www.pingidentity.com/</a></p> <p><b>Product Name: Ping Identity PingFederate® 5.2</b></p>
 <p>RSA Security, The Security Division of EMC</p> <p>The Security Division of EMC</p> <p><a href="http://www.rsasecurity.com/">http://www.rsasecurity.com/</a></p> <p><b>Product Name: RSA Federated Identity Manager version 4.1</b></p>	<p><b>UBISECURE.</b> Ubisecure Solutions, Inc.</p> <p><a href="http://www.ubisecure.com/">http://www.ubisecure.com/</a></p> <p><b>Product Name: UbiLogin SSO version 5.0</b></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 The 3Q08 SAML 2.0 interoperability test event consisted of six vendor  
47 participants: CA, NTT Software, Oracle, Ping, RSA and Ubisecure. All six  
48 participants have achieved Liberty Alliance Interoperable certification for the  
49 SAML 2.0 3Q08 test event. They performed full-matrix testing over different  
50 SAML conformance modes without error or code changes during the SAML 2.0  
51 3Q08 Certification Run on the dates of September 2-4 to prove their  
52 interoperability. The time preceding the Certification Run, July 14-August 29, was  
53 set aside for debugging interoperability issues. The list of products and the  
54 conformance modes they certified for can be found in the [Final Test Results](#)  
55 section.

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

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

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

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

## 80 Final Test Results

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

86

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
Oracle	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	

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

89 CA: IDP Lite, SP Lite, eGov

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

93 Oracle: IDP, IDP Lite, SP, SP Lite, Attribute Authority (Requester/Responder),  
94 Authentication Authority (Responder), POST Binding, eGov

95 Ping: IDP Lite, SP Lite,

96 RSA: IDP, IDP Lite, SP, SP Lite, Attribute Authority (Requester/Responder),  
97 Authentication Authority (Requester/Responder), POST Binding, eGov

98 Ubisecure: IDP, IDP Lite, SP, SP Lite, SP Extended, IDP Extended, POST  
99 Binding

## 100 **Interoperability Test History**

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

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

105 Liberty Alliance has sponsored and administered previous non-full-matrix SAML  
106 2.0 certification events. Please refer to the Liberty Alliance website for more  
107 information on those past 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 trusted 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, (i.e., through a secure password) only  
115 once and this identification is shared among the other trusted partners without  
116 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](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 modes.

### 131 **Test Cases and Test Criteria**

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

### 136 **SAML Defined Conformance Modes**

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

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

151 The test plan requirements for certification in SP Lite and IdP Lite conformance  
152 modes are a subset of the requirements for SP and IdP conformance modes.  
153 Thus, completion of the requirements for SP and IdP conformance modes

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

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

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

## 168 **Optional Liberty Alliance Conformance Modes**

### 169 **POST Binding**

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

### 174 **eGov Profile**

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

180 **Test Cases Associated with Conformance Modes**

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

190 IdP Lite and SP Lite modes require only a subset of the test steps in Test Cases  
 191 A, B, E and F in accordance to the SAML Conformance [SAMLConf]  
 192 requirements. Refer to the Test Plan [document](#) for details.  
 193

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

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

## 195 **Interoperability Caveats**

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

## 200 **Consensus Items**

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

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

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

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

## 230 **Configuration Setup**

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

## 240 **CA**

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

243 SiteMinder expects the other participants to access SiteMinder resources using  
244 FQDN and not IP address.

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

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

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

## 262 **NTT Software**

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

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

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

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

## 271 **Oracle**

272 The SLO binding has to be configured by setting the default binding. For MNI,  
273 federation update and termination must be enabled on both SP/IDP.

274 For Unsolicited Response, the default SSO Response binding and the default  
275 Name ID format have to be set on the IDP.

276 For IDP Discovery, CDC must be enabled and the domain name specified in both  
277 SP and IDP.

278 For eGov, IDP Discovery Service must also be enabled on the SP.

279 Attributes in SSO Response must be enabled and the attributes must be defined  
280 in the IDP.

281 For Attribute Requester/Authority, Authentication Authority and Assertion ID  
282 Requester/Authority, the profile must be enabled.

283 For Assertion ID Authority, HTTP Basic Authentication was enabled. Users were  
284 created in the security realm of the Weblogic Server where the application is  
285 deployed.

## 286 **Ping**

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

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

## 292 **RSA**

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

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

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

## 302 **Ubisecure**

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

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

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

314 By default, the metadata only contained the RSAKeyValue element. Also if the  
315 entity supports both signing and encryption, then the use attribute of the  
316 KeyDescriptor element is not specified. In the future, the default operation is  
317 expected to change to allow producing metadata files as were used in the  
318 interop.

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

320 A CDC cookie reader and writer application was installed in the CDC domain  
321 `ubisecure.cot.projectliberty.org`. The url of the CDC application was configured to  
322 Ubilogin IDP and SP.

## 323 **Browser Usage**

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

327 CA: Firefox 3.0.1, IE 6

328 NTT Software: Firefox 3.0.1, IE 7

329 Oracle: IE 6

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

331 RSA: IE 7, Firefox 2, Firefox 3

332 Ubisecure: IE 7, Firefox 2, Firefox 3

## 333 **Testing Requirements**

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

## 336 **Trading Partner Requirements**

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

## 346 **Metadata**

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

- 350 • Furnish correct metadata, and
- 351 • Process metadata furnished by other testing partners.

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

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

## 360 **Technical Requirements**

### 361 **General Test Case Requirements**

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

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

366       • For POST bindings, the entire response message MAY be signed, but if  
367       signed, the receiving partner MUST validate the signature.

368       • Encryption of NameIDs and Assertions MUST be enabled.

## 369   **IdP Authentication**

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

- 375       1. HTTP Basic Auth.
- 376       2. HTTP Form Post
- 377       3. HTTP Get

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

## 380   **Trivial Processing**

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

## 387   **Authentication Contexts**

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

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

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

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

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

## 408 **Name Identifier Formats**

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

- 410 1. Unspecified
- 411 2. Email
- 412 3. X.509 Subject
- 413 4. Windows
- 414 5. Kerberos
- 415 6. Entity
- 416 7. Persistent
- 417 8. Transient

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

## 420 **XML Signatures**

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

- 424 1. Web SSO: The assertion element(s) in the <Response> MUST be signed  
425 for the HTTP POST binding.
- 426 2. ECP Profile: The assertion element(s) in the <Response> issued by the  
427 IdP MUST be signed.
- 428 3. Single Logout: The <LogoutRequest> and <LogoutResponse> MUST be  
429 signed for the HTTP redirect binding.
- 430 4. Name Identifier Management: The <ManageNameIDRequest> and  
431 <ManageNameIDResponse> MUST be signed for the HTTP redirect  
432 binding.

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

## 436 **XML Encryption**

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

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

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

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

## 459 **Attribute Profiles**

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

465 **Overview of the DGI Interoperability Compliance**  
466 **Process®**

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

472 **DGI Interoperability Test Round**

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

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

482 Products-with-version which demonstrate complete interoperability among the  
483 passing members of the Product Test Group are given a Liberty Alliance  
484 Interoperable™ seal and are listed with Interoperability Status on the  
485 [www.projectliberty.org](http://www.projectliberty.org) website. Interoperability Test Rounds are periodically  
486 repeated to verify that as product names, versions or releases change, the  
487 products remain interoperable.

## 488 **References**

- 489 [SAMLAuthnCxt] J. Kemp et al, "Authentication Context for the OASIS  
490 Security Assertion Markup Language (SAML) V2.0," OASIS  
491 SSTC (March 2005), [http:// docs.oasis-  
492 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).
- 493 [SAMLConf] Prateek Mishra et al, "Conformance Requirements for the  
494 OASIS Security Assertion Markup Language (SAML) V2.0,"  
495 OASIS SSTC (March 2005). [http://docs.oasis-  
496 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).
- 497 [SAMLCore] S. Cantor et al, "Assertions and Protocols for the OASIS  
498 Security Assertion Markup Language (SAML) V2.0," OASIS  
499 SSTC (March 2005), [http://docs.oasis-  
500 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).
- 501 [SAMLErrata] Eve Maler, et al, "Errata for the OASIS Security 2 Assertion  
502 Markup Language (SAML) V2.0, Working Draft 28," OASIS  
503 SSTC (August 14, 2007), [http://docs.oasis-  
504 open.org/security/saml/v2.0/sstc-saml-approved-errata-  
505 2.0.pdf](http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf).
- 506 [SAMLMeta] S. Cantor et al, "Metadata for the OASIS Security Assertion  
507 Markup Language (SAML) V2.0," OASIS SSTC (March  
508 2005), [http://docs.oasis-open.org/security/saml/v2.0/saml-  
509 metadata-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf).
- 510 [SAMLMetaExt] Tom Scavo et al, "SAML Metadata Extension for Query  
511 Requesters, Committee Draft 01", OASIS SSTC (March  
512 2006), [http://www.oasis-  
513 open.org/committees/download.php/18052/sstc-saml-  
514 metadata-ext-query-cd-01.pdf](http://www.oasis-open.org/committees/download.php/18052/sstc-saml-metadata-ext-query-cd-01.pdf)
- 515 [SAMLProf] S. Cantor et al, "Profiles for the OASIS Security Assertion  
516 Markup Language (SAML) V2.0," OASIS SSTC (March  
517 2005), [http://docs.oasis-open.org/security/saml/v2.0/saml-  
518 profiles-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf).
- 519 [GSATechAppr] Dave Silver et al, "Technical Approach for the Authentication  
520 Service Component" vs. 2.0.0 GSA (May 2007),  
521 <http://www.cio.gov/eauthentication/TechnicalArchitecture.htm>
- 522 [GSAAadoptSchm] Dave Silver et al, "E-Authentication Federation Adopted  
523 Schemes" vs. 1.0.0 GSA (May 2007),  
524 <http://www.cio.gov/eauthentication/TechnicalArchitecture.htm>

525 [GSAInterface] Dave Silver et al, "E-Authentication Federation Architecture  
526 2.0 Interface Specifications" vs. 1.0.0 GSA (May 2007),  
527 <http://www.cio.gov/eauthentication/TechnicalArchitecture.htm>

## 528 **About Drummond Group Inc.**

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