

Certification Final Report
SAML 2.0 Interoperability Test
First Quarter 2011 (1Q11)

March 31, 2011

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	8
Overview of Test Event	8
Final Test Results	9
Interoperability Test History	10
About SAML 2.0	10
About Kantara Initiative	10
Test Case and Conformance Mode Summary	12
Test Case and Conformance Mode Summary: Overview	12
Test Cases and Test Criteria	12
SAML Defined Conformance Modes	12
Optional Kantara Defined Conformance Modes	13
POST Binding	13
eGov 1.5 Profile	13
Test Cases Associated with Conformance Modes	14
Interoperability Caveats	15
Consensus Items	15
SAML 1Q11 Consensus Items	15
SAML 3Q09 Consensus Items	16
SAML 3Q08 Consensus Items	16
SAML 4Q07 Consensus Items	16
Configuration Setup	17
CA Technologies	17
IBM	18
SAP	Error! Bookmark not defined.
UNINETT	19
Browser Usage	20
Testing Requirements	21
Trading Partner Requirements	21
Metadata	21
Technical Requirements	21
IdP Authentication	21
Trivial Processing	22
Authentication Contexts	22
Name Identifier Formats	22
XML Signatures	23
XML Encryption	23
Attribute Profiles	24
Overview of the DGI Interoperability Compliance Process®	25
DGI Interoperability Test Round	25
References	26
About Drummond Group Inc.	27

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 1st Quarter 2011 (SAML-1Q11) (see [Final Test Results](#)). This is the first SAML full-matrix interoperability test event sponsored by the Kantara Initiative. Full-matrix testing is the best means to verify product group interoperability as it verifies that every product can successfully interact and interoperate with the other products in the test group using the test criteria.

This test marked the second time the SAML 2.0 eGovernment (eGov) Profile, Version 1.5, was included in the event. The eGov profile is a result of a multi-government effort to create a viable SAML conformance profile for government identity management.

This report provides the description of how these products were tested, the technical requirements and test cases required of them, lists the important consensus items determined and provides 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 key sections of the document.

Sincerely,

Timothy Bennett
SAML IOP Test Administrator
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 ("Participants"). At the end of the testing process, DGI may list the name of a
5 Participant in the final test report along with an indication that a Participant
6 passed the test. The fact that the name of a Participant appears in the final report
7 is not an endorsement of the Participant or its products or services. DGI therefore
8 makes no warranties, either expressed or implied, regarding any facet of the
9 business conducted by the Participant or its product.

10 **Test Participants**

 <p>CA Technologies</p> <p>Product Name: CA Federation Manager 12.5</p>	 <p>International Business Machines</p> <p>Product Name: IBM Tivoli Federated Identity Manager Version 6 Release 2</p>
 <p>SAP AG</p> <p>Product Name: SAP NetWeaver Identity Management 7.2</p>	 <p>SAP AG</p> <p>Product Name: SAP NetWeaver Application Server ABAP 7.02</p>
 <p>UNINETT AS</p> <p>Product Name: SimpleSAMLphp 1.8</p>	

11

12 **Definitions**

13 **Kantara Initiative Interoperable** – Products successfully demonstrating
14 interoperability at Kantara-sponsored test events.

15 **Interoperability** – The capability of two or more networks, systems, applications,
16 components or devices to exchange information and to use the information that
17 has been exchanged in a meaningful way.

18 **Interoperability Testing** – Interoperability testing is focused on testing that
19 information is properly exchanged from one network, system, application,
20 component or device to another to another in accordance with a defined interface
21 specification. Therefore, interoperability tests the ability of two or more products
22 to conform to a defined interface specification, rather than how the information is
23 used.

24 **Full-Matrix Interoperability Testing** – Interoperability testing where each test
25 participant is tested to demonstrate interoperability with all other test participants
26 for a defined interface specification and test procedure. A product is deemed
27 interoperable with all other products in the Interoperability Test Round if and only
28 if it successfully completes Full Matrix Interoperability Testing covering the *Test*
29 *Criteria* between all products in the Interoperability Test Round. A product is
30 either totally interoperable or it is not interoperable. Waivers or exceptions are
31 not given in demonstrating interoperability for the *Test Criteria* unless the entire
32 *Product Test Group*, DGI and Kantara Initiative agree.

33 **Interoperable products** – Subset of products, from the *Product Test Group*,
34 which successfully completed the *Test Criteria*, through full-matrix testing with
35 every other *Product Test Group* participant in an Interoperability Test Round
36 without any errors in the final test Phase. Interoperable products receive a
37 Kantara Initiative Interoperable™ seal.

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

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

50 **Test Case** – The test criteria is a set of individual test cases, often 10 to 50, in
51 which, members of the product test group engage to verify conformance and
52 interoperability.

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

57 **Test Phase** – One or more iterations of the Test Criteria executed during a Test
58 Round. Typically, a Test Round is divided into three Test Phases: a Debug
59 Phase, a Dry Run Phase, and finally the Certification Run. The Certification Run
60 is a single iteration of the Test Criteria that determines the Interoperable
61 Products for the Test Round.

62 **Test Round** – A Full-Matrix Interoperability Test Event.

63

64 Interoperability Test Summary

65 Overview of Test Event

66 SAP, IBM, CA Technologies, and UNINETT participated in the SAML 2.0
67 interoperability test event, with SAP testing two different products and UNINETT
68 testing an open source application. All products successfully achieved Kantara
69 Interoperable certification for the SAML 2.0 1Q11 test event. They performed full-
70 matrix testing over different SAML conformance modes without error or code
71 changes during the SAML 2.0 1Q11 Certification Run on the dates of February
72 23 - March 1 to prove their interoperability. The time preceding the Certification
73 Run, January 10 - February 22, was set aside for debugging interoperability
74 issues and preparing for the Certification Run. The list of products and the
75 conformance modes for which they were certified can be found in the [Final Test](#)
76 [Results](#) section.

77 There are several conformance modes for SAML testing, both those defined
78 within the SAML specification by OASIS and those defined by the Kantara
79 Initiative. In order to be certified in a SAML conformance mode, each vendor
80 was required to perform full-matrix testing in its chosen conformance mode(s).
81 Full-matrix testing requires each participant to test with every other participant for
82 all test criteria. For example, a product certifying as a SAML Service Provider
83 (SP) had to execute all required test cases with all the SAML Identity Provider
84 (IdP) products since SPs and IdPs must interoperate with each other. The list of
85 which test cases were required for each conformance mode can be found in the
86 section summarizing the [test cases and conformance modes](#).

87 The test criteria and the subsequent test cases cover all the conformance modes
88 for this test event and were approved by the Kantara Initiative Interoperability
89 Work Group (IOPWG) and Interoperability Review Board (IRB). The actual test
90 cases for this test event can be found in the [Kantara Initiative SAML 2.0 Test](#)
91 [Plan v3.3](#) available from the kantarainitiative.org website.

92 To assist in the deployment of these products into real-world deployments,
93 specific details required for achieving interoperability can be found in the
94 [Interoperability Caveats](#) section. This section explains how the products were
95 configured and key consensus items made to ensure their interoperability.
96 Information in this section may be beneficial for deployment interoperability in
97 federations.

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

102 Final Test Results

103 The table below shows the interoperable products and the conformance modes they successfully tested. The green boxes containing a "P" indicate the participant passed certification requirements in the corresponding conformance mode. The yellow boxes containing a "N" indicate IBM registered for interoperability testing in the corresponding conformance mode, but no other participants were available to execute those test cases and therefore certification could not be assessed for those modes. However, IBM achieved these conformance levels labeled as "N" during the previous 3Q09 interoperability event. The actual product version-with-release information can be found in the [Test Participant](#) section.

113

Product	CONFORMANCE MODES													
	IDP	IDP Lite	IDP Extended	SP	SP Lite	SP Extended	Attribute Authority Requestor	Attribute Authority Responder	Authentication Authority Requestor	Authentication Authority Responder	Authorization Decision Authority Requestor	Authorization Decision Authority Responder	POST Binding	eGov 1.5
CA Federation Manager		P			P									P
IBM Tivoli	P	P		P	P		N	N	N	N			P	P
SAP NetWeaver Application Server ABAP 7.02					P									P
SAP NetWeaver Identity Management 7.2	P	P		P	P								P	P
UNINETT SimpleSAMLphp		P			P									

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

116 CA: IDP Lite, SP Lite, eGov 1.5

117 IBM: IDP, IDP Lite, SP, SP Lite, eGov 1.5, POST Binding

118 SAP NetWeaver Application Server ABAP 7.02: SP Lite, eGov 1.5

119 SAP NetWeaver Identity Management 7.2: IDP, IDP Lite, SP, SP Lite, eGov 1.5,
120 POST Binding

121 UNINETT: IDP Lite, SP Lite

122 **Interoperability Test History**

123 This is the fourth SAML 2.0 interoperability certification event administered by
124 DGI, and it is also the fourth full-matrix interoperability test event for SAML 2.0. It
125 is the first SAML 2.0 interoperability test event sponsored by the Kantara
126 Initiative.

127 Liberty Alliance sponsored three previous full-matrix interoperability test events
128 administered by DGI:

- 129 • SAML 2.0 3Q09 Interoperability Test Event (July-Sept. 2009)
- 130 • SAML 2.0 3Q08 Interoperability Test Event (July-Sept. 2008)
- 131 • SAML 2.0 4Q07 Interoperability Test Event (Oct.-Dec. 2007)

132 Liberty Alliance has sponsored and administered previous non-full-matrix SAML
133 2.0 certification events. Please refer to the Liberty Alliance website for more
134 information on those past test events and the products that were previously
135 certified as interoperable.

136 **About SAML 2.0**

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

145 **About Kantara Initiative**

146 Kantara Initiative is a global, open, public-private, technology-agnostic forum
147 comprised of identity ecosystem stakeholders. Its inspired mission is to promote
148 technical interoperability and harmonization; to develop policy frameworks for
149 operational interoperability and to provide certification and assessment programs

150 to grow trust in the standards, products, and service deployments. For more
151 information about getting involved in Kantara Initiative, visit
152 <http://kantarainitiative.org/>

153 **Test Case and Conformance Mode** 154 **Summary**

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

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

162 **Test Cases and Test Criteria**

163 The test criteria and the subsequent test cases cover all the conformance modes
164 for this test event and were approved by the Kantara Initiative Interoperability
165 Work Group (IOPWG) and Interoperability Review Board (IRB). The actual test
166 cases for this test event can be found in the [Kantara Initiative SAML 2.0 Test](#)
167 [Plan v3.3](#) available from the kantarainitiative.org website.

168 [SAMLConf] states that SOAP Binding for SLO is optional for SP Lite and IdP
169 Lite applications. In Test Case B, SP Lite and IdP Lite participants may choose to
170 use Redirect Binding for test steps performing SLO actions instead of SOAP
171 Binding. CA and UNINETT chose to use Redirect Binding, while the SP Lite
172 product from SAP chose SOAP Binding.

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

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

180 **SAML-Defined Conformance Modes**

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

- 185 • IdP – Identity Provider
- 186 • IdP Lite – Identity Provider Lite

- 187 • SP – Service Provider
 - 188 • SP Lite – Service Provider Lite
 - 189 • IdP Extended – Identify Provider Extended
 - 190 • SP Extended – Service Provider Extended
 - 191 • SAML Attribute Authority (Requester/Responder)
 - 192 • SAML Authorization Decision Authority (Requester/Responder)
 - 193 • SAML Authentication Authority (Requester/Responder)
- 194 Certification in conformance modes IdP Extended and SP Extended can only be
195 given if a participant has met the certification requirements of one of the standard
196 SP or IdP modes.

197 **Optional Kantara-Defined Conformance Modes**

198 **POST Binding**

199 Although the POST Binding is not included in [SAMLConf], it is permitted with the
200 SAML specification and has some user deployment. POST Binding is an optional
201 Kantara-defined conformance mode. It involves use of POST binding for
202 AuthnRequest, Name ID Management and SLO.

203 **eGov 1.5 Profile**

204 The eGov 1.5 Profile is a conformance profile developed by Liberty TEG and
205 Liberty eGovernment SIG and subsequently contributed to the Kantara Initiative.
206 The test cases within this test plan to achieve eGov certification are based on the
207 requirements stated in the eGov 1.5 profile. The eGov 1.5 profile should be
208 consulted for further explanation of the eGov requirements:

209
210 [http://kantarainitiative.org/confluence/download/attachments/42139929/LibertyAlli](http://kantarainitiative.org/confluence/download/attachments/42139929/LibertyAlliance_eGov_Profile_1.5.pdf)
211 [ance_eGov_Profile_1.5.pdf](http://kantarainitiative.org/confluence/download/attachments/42139929/LibertyAlliance_eGov_Profile_1.5.pdf)

212 **Test Cases Associated with Conformance Modes**

213 In order to achieve certification in one or more of the Kantara SAML
 214 Conformance Modes, the associated test cases must be completed with all test
 215 participants with aligning modes. For example, a product testing for an IdP
 216 conformance mode must complete Test Cases A, B, C, D, H, I, J, K and L
 217 against all products testing for a SP conformance mode and SP Lite
 218 conformance mode (note – Test Case P is a SAML Conformance Error test case
 219 where participants interact with an error testing tool). The specific pairing among
 220 participants will be given at the beginning of the certification event. A
 221 conformance mode may not require completion of all the test steps in the
 222 associated test cases. The individual test cases described in the [Kantara](#)
 223 [Initiative SAML 2.0 Test Plan v3.3](#) provide details of test steps that may or must
 224 be omitted depending on the conformance mode.
 225

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

226 **Interoperability Notes**

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

231 **Consensus Items**

232 Consensus Items are standards/implementation issues on which the product test
233 group reached consensus in order to achieve interoperability among the group.
234 Some consensus items may be temporary solutions necessary to facilitate
235 interoperability among the group (and are noted as such) until a standard body
236 can more formally address the concern.

237 **SAML 1Q11 Consensus Items**

- 238 • During this test event, a possible SSL interoperability issue surfaced between
239 OpenSSL and VeriSign SSL certificates that is noteworthy for current
240 deployments to be advised to consider, and may be explored more fully in
241 future interoperability test events.¹ The details are described below:
- 242 ○ One vendor product implementing the OpenSSL library had difficulty
243 negotiating an SSL connection with another vendor product that
244 acquired and installed a VeriSign SSL certificate. There was at least
245 one other product using OpenSSL for their implementation and did not
246 experience the same connection issues.
 - 247 ○ The Google Chrome browser, believed to implement the same
248 OpenSSL library, also was not able to access the same vendor's
249 secure test site using the VeriSign SSL certificate. However, both
250 Firefox and IE browsers had no connection problems to the web
251 server.
 - 252 ○ The issue was addressed during the Test Event by setting up a
253 secondary test system using a self-signed SSL certificate instead of
254 the VeriSign SSL certificate.

255
256 The consensus items below are from the previous SAML interoperability test
257 event and applied to the current test event as well.

¹ The technical opinion of the involved participants indicated the issue was likely an SSL interoperability issue as opposed to a SAML 2.0 interoperability issue, and therefore full resolution of this issue was deemed out of scope for the SAML 2.0 interoperability test. As such, switching to a different deployment configuration instead of resolving the issue does not impact the validity or the outcome of this SAML 2.0 interoperability test.

258 **SAML 3Q09 Consensus Items**

- 259 • An Assertion element does not need to be constructed so that namespace
260 definitions can be validated apart from the enveloping Response message.
261 This was confirmed by OASIS SSTC.
- 262 • The Product Test Group accepted this approach for implementing and
263 resolving signatures of Artifact Resolution messages, given the wording from
264 [SAMLCore], section 5.
- 265 1. As the test group is using SSL Server-Side Authentication, the responder
266 does not have to sign the <ArtifactResponse> as the responder has
267 authenticated itself.
- 268 2. A responder MAY also add a signature to the <ArtifactResponse> and any
269 requester MUST be able to accept it.
- 270 3. Because of the SHOULD key word from section 5.3, requesters need to
271 add XML Signature to the <ArtifactResolve> message.
- 272 • If a responder is authenticated through SSL, the XML signature can be
273 omitted from the SLO Response.
- 274 • If an XML Signature is applied to any part of a SAML message, it MUST be
275 verified.
- 276 • SAML partner MAY add a valid SPNameQualifier and NameQualifier when
277 building a LogoutRequest even if the IDP omitted them from the NameID
278 included on the assertion.

279 After consulting with OASIS SSTC, it was agreed that if a SP (SP-B) returns a
280 non-Success status in a LogoutResponse to an IDP and the IDP is able to
281 terminate the authenticated session, the IDP is to send to any other session SP
282 (SP-A) a LogoutResponse with a top-level status of Success and a second-level
283 status of PartialLogout. If SP-B does return a Success status to the IDP, the IDP,
284 assuming it is able to terminate the session itself, returns to SP-A a Success
285 status.

286 **SAML 3Q08 Consensus Items**

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

291 **SAML 4Q07 Consensus Items**

- 292 • DSAwithSHA1 signature algorithm not supported. Section 4.1 of [SAMLConf]
293 states that the DSAwithSHA1 signature algorithm, while recommended, is not

294 required by SAML 2.0. Participants are only to use digital certificates with the
295 required RSAwithSHA1 signature algorithm.

296 • Ignore EncryptionMethod elements in metadata. There is some confusion of
297 interpretation implementation of the EncryptionMethod metadata elements
298 described in Section 2.4.1.1 of [SAMLMeta]. After confirming with OASIS
299 SSTC, EncryptionMethod is to be ignored.

300 • Encryption with NameIDPolicy and ID Encryption. A question had arisen on
301 interpreting NameIDPolicy from [SAMLCore] in lines 2136-2142. It was
302 decided that if NameIDPolicy of AuthnRequest says ID is to be encrypted, it
303 must be encrypted in the assertion, and if NameIDPolicy of AuthnRequest
304 does not state the ID is to be encrypted, the IDP MAY still encrypt the ID
305 based on its policy, specifically its policy with the SP.

306 • SSL Server-side Authentication Only for SOAP connections. To insure all
307 participants used the same security settings, it was agreed to only use SSL
308 server-side authentication for SOAP connections and not to use SSL client-
309 side authentication.

310 **Configuration Setup**

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

320 **CA Technologies**

321 As of special configuration, other than the SSL requirement for UNINETT, there
322 are really no special requirements. To that, it can be summarized as following:

323 Based on our discussions and experiences with UNINETT, it seems that the
324 openssl library UNINETT uses has some difficulty negotiating with the VeriSign
325 SSL certificate CA acquired and installed. This was also proven by the usage of
326 the Google Chrome Browser which was believed to use the same/similar openssl
327 library. The Google Chrome Browser was not able to access our Web Site
328 <https://idp.ca.com/> even though a VeriSign issued SSL certificate was used on
329 our server. Our choices at the time included replacing our SSL certificate with a
330 self-signed certificate and re-doing all the tests with all partners. For the sake of
331 saving the time to redo all the tests, we decided to setup a separate system that

332 used a self-signed certificate for the tests where UNINETT needed to use https to
333 retrieve information from a CA server.

334 **IBM**

335 The configuration is pretty much standard. The only thing to point out is that IBM
336 has set up all partners to do what is called "typical signature validation option"
337 when importing metadata to partner environments. That means that
338 AuthnResponse and ArtifactResolve signatures are not mandated but will get
339 validated if the document is signed.

340

341 **SAP NetWeaver Application Server ABAP 7.02**

342 *Signature/Encryption:*

343 The default signature and encryption settings in SAP NetWeaver Application
344 Server ABAP 7.02 match the requirements for all SP Lite test cases except for
345 test case B. For SSO profile by default the AuthnRequest will be signed by the
346 SP. The encryption of NameIDs has to be enabled explicitly. All signature and
347 encryption settings are maintained per trusted provider (partner).

348 *Bindings:*

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

354 *IdP Discovery:*

355 For IdP Discovery, the SP has to be configured to use external Common Domain
356 Cookie (CDC) read service. Such service comes as part of the product. By
357 default its usage is disabled.

358 *ForceAuthn/IsPassive:*

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

362

363 **SAP NetWeaver Identity Management 7.2**

364 *Signature/Encryption:*

365 The default signature and encryption settings in SAP NetWeaver Identity
366 Management 7.2 match the requirements for all IdP/SP test cases except for test
367 case B. For SSO profile by default the AuthnRequest will be signed by the SP

368 and only the Assertion will be signed by the IdP (the Response is unsigned). The
369 encryption of Assertions and NameIDs has to be enabled explicitly. All signature
370 and encryption settings are maintained per trusted provider (partner).

371 *Bindings:*

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

378 *IdP Discovery:*

379 For IdP Discovery, the IdP and SP have to be configured to use external
380 Common Domain Cookie (CDC) write/read services. Such services come as part
381 of the product. By default their usage is disabled.

382 *ForceAuthn/IsPassive:*

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

386 *Authentication Context Comparison*

387 For authentication context comparisons (minimum, maximum, better), used in
388 test case Q (eGov 1.5), authentication context ranks have to be configured at the
389 IdP side.

390

391 **UNINETT**

392 To enable full logout support, we configured the installation with the 'sql' session
393 store.

394 Validation and signing of logout messages was enabled unconditionally.

395 We disabled the sending of client certificates when issuing requests over the
396 SOAP binding.

397 To enable Common Domain Cookie (CDC) support, we configured and enabled
398 the 'cdc' "authentication processing filter" in the IdP. Since CDC support is not
399 required by the SP lite, it is not directly supported by the built-in discovery Page.
400 To ease testing, we added a minimal proof-of-concept discovery page that read
401 the CDC cookie.

402 Browsers used were Opera 11.00 and Firefox 3.6.13.

403

403 **Browser Usage**

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

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

414 CA: IE 8.0.6001.18702

415 IBM: Firefox 3.0.13

416 SAP: IE 6, IE 8, Firefox 3.6

417 UNINETT: Opera 11.00 and Firefox 3.6.13

DavidMTemoshok 4/12/11 1:18 PM

Comment: Why can't Drummond/CA identify the browser(s) that CA used in the test?

418 **Testing Requirements**

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

421 **Federation Requirements**

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

431 **Metadata**

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

- 435 • Furnish correct metadata, and
- 436 • Process metadata furnished by other testing partners.

437 While metadata is not specified for SAML Attribute Requesters, interoperability
438 with SAML Authorities is very difficult without it, and for this certification event, it
439 is required that SAML Attribute Requesters provide metadata as described in the
440 draft metadata extension specification [SAMLMetaExt]. Participants were
441 responsible for creating their own certificates for testing.

442 **Technical Requirements**

443 **IdP Authentication**

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

- 449 1. HTTP Basic Auth.
- 450 2. HTTP Form Post
- 451 3. HTTP Get

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

454 **Trivial Processing**

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

461 **Authentication Contexts**

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

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

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

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

482 **Name Identifier Formats**

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

- 484 1. Unspecified
- 485 2. Email
- 486 3. X.509 Subject
- 487 4. Windows

488 5. Kerberos

489 6. Entity

490 7. Persistent

491 8. Transient

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

494 **XML Signatures**

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

498 1. Web SSO: The assertion element(s) in the <Response> MUST be signed
499 for the HTTP POST binding.

500 2. Single Logout: The <LogoutRequest> and <LogoutResponse> MUST be
501 signed for the HTTP redirect binding.

502 3. Name Identifier Management: The <ManageNameIDRequest> and
503 <ManageNameIDResponse> MUST be signed for the HTTP redirect
504 binding.

505 Note that when a test step refers to a “signed SAML Response message” this
506 implies the assertion element itself is signed per the requirements in
507 [SAMLProf].3

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

511 **XML Encryption**

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

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

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

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

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

534 **Attribute Profiles**

535 [SAMLConf] makes no normative statements about which Attribute Profiles in
536 [SAMLProf] are required to be supported by SAML Attribute Authority. This
537 document only describes testing procedures for the Basic profile, and does not
538 describe any testing procedures regarding other profiles.

539 **Overview of the DGI Interoperability**
540 **Compliance Process®**

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

546 **DGI Interoperability Test Round**

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

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

556 Products-with-version which demonstrate complete interoperability among the
557 passing members of the Product Test Group are given a Kantara Initiative
558 Interoperable™ seal and are listed with Interoperability Status on the
559 <http://www.kantarainitiative.org> website. Interoperability Test Rounds are
560 periodically repeated to verify that as product names, versions or releases
561 change, the products remain interoperable.

562 **References**

- 563 [SAMLAuthnCxt] J. Kemp et al, "Authentication Context for the OASIS
564 Security Assertion Markup Language (SAML) V2.0," OASIS
565 SSTC (March 2005), [http:// docs.oasis-](http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf)
566 [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).
- 567 [SAMLConf] Prateek Mishra et al, "Conformance Requirements for the
568 OASIS Security Assertion Markup Language (SAML) V2.0,"
569 OASIS SSTC (March 2005). [http://docs.oasis-](http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf)
570 [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).
- 571 [SAMLCore] S. Cantor et al, "Assertions and Protocols for the OASIS
572 Security Assertion Markup Language (SAML) V2.0," OASIS
573 SSTC (March 2005), [http://docs.oasis-](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)
574 [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).
- 575 [SAMLErrata] Eve Maler, et al, "Errata for the OASIS Security 2 Assertion
576 Markup Language (SAML) V2.0, Working Draft 28," OASIS
577 SSTC (August 14, 2007), [http://docs.oasis-](http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf)
578 [open.org/security/saml/v2.0/sstc-saml-approved-errata-](http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf)
579 [2.0.pdf](http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf).
- 580 [SAMLMeta] S. Cantor et al, "Metadata for the OASIS Security Assertion
581 Markup Language (SAML) V2.0," OASIS SSTC (March
582 2005), [http://docs.oasis-open.org/security/saml/v2.0/saml-](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)
583 [metadata-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf).
- 584 [SAMLMetaExt] Tom Scavo et al, "SAML Metadata Extension for Query
585 Requesters, Committee Draft 01", OASIS SSTC (March
586 2006), [http://www.oasis-](http://www.oasis-open.org/committees/download.php/18052/sstc-saml-metadata-ext-query-cd-01.pdf)
587 [open.org/committees/download.php/18052/sstc-saml-](http://www.oasis-open.org/committees/download.php/18052/sstc-saml-metadata-ext-query-cd-01.pdf)
588 [metadata-ext-query-cd-01.pdf](http://www.oasis-open.org/committees/download.php/18052/sstc-saml-metadata-ext-query-cd-01.pdf)
- 589 [SAMLProf] S. Cantor et al, "Profiles for the OASIS Security Assertion
590 Markup Language (SAML) V2.0," OASIS SSTC (March
591 2005), [http://docs.oasis-open.org/security/saml/v2.0/saml-](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)
592 [profiles-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf).

593 **About Drummond Group Inc.**

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