

## **SAML 2.0 Interoperability Test**

**First Quarter 2011 (1Q11)**

**Due Diligence Report for Kantara IRB**

**June 6, 2011**

Prepared by:

DRUMMOND GROUP INC.

[www.drummondgroup.com](http://www.drummondgroup.com)

**Table of Contents**

Scope of Document ..... 3  
Overview of Test Event Execution ..... 4  
DGI Perspective..... 6  
    A Whole Lotta New ..... 6  
    Five Is Not Enough ..... 6  
Looking Forward ..... 7  
    Healthcare and eGov 2.0 ..... 7  
    Make Process for Situation Where Only One Participant Registers for a  
    Mode or Profile..... 7  
    Expand Test Tool for More IdP Error Test Cases ..... 7  
    IRB Review of Test Plan? ..... 8  
About Drummond Group Inc. .... 9

## 1 **Scope of Document**

2 The Due Diligence Report is designed to be both a look back at the past test  
3 event and a look ahead for future testing activities. By examining the previous  
4 test event, noting lessons learned and identifying areas which can be improved,  
5 the test process and future test events can be enhanced to provide greater value  
6 for all involved.

7 This report begins with an overview section re-examining the test administration  
8 and test process for the SAML 2.0 1Q11 interoperability test event. After that is a  
9 Drummond Group (DGI) Perspective section sharing observations about the test  
10 event and a final section on Looking Forward which points out ideas which need  
11 to be implemented or questions addressed before the next test round.

## 12 **Overview of Test Event Execution**

13 The SAML 2.0 1Q11 interoperability test event began on January 10<sup>th</sup> and  
14 completed slightly over 7 weeks later on March 1<sup>st</sup>, a few days past the original  
15 targeted end date of February 25<sup>th</sup>. There were some delays at the beginning of  
16 the test event with a number of participants slow to get their systems configured  
17 and prepared to send/receive Test Cases, resulting in the Test Event dropping a  
18 few days behind schedule. But, with a week of make-up days built into the 7  
19 week schedule, there was time to make the time up as the Debug Phase  
20 proceeded.

21 However, throughout the debug period of testing, there were several significant  
22 issues that delayed the progress of the test event. One issue involved an  
23 SSL/TLS handshaking problem between CA and UNINETT that eventually was  
24 resolved by CA deploying a 2<sup>nd</sup> and separate testing environment. This involved  
25 several days of extra activity for that vendor before they could continue testing  
26 some of the test cases with UNINETT.

27 Additionally, a debate between CA, SAP and IBM regarding encryption for SLO  
28 over HTTP Redirect Binding caused further delays in the testing schedule, as the  
29 SAML specification, the Kantara Test Plan, and the historical List of Consensus  
30 Items from prior test events were reviewed and discussed. CA, who did not test  
31 during 3Q09 Interop Test Event, initially was not in agreement with the 3Q09  
32 consensus agreement on this issue. Eventually, changes were made and  
33 interoperability was demonstrated, but not before further delays to the testing  
34 schedule.

35 A number of other interoperability issues also occurred as the Debug Phase  
36 progressed, resulting in the schedule slipping further. The execution of Test  
37 Case K is the only test case that is not performed in a full-matrix fashion,  
38 required three vendor products to test together . one in the role of IdP and two  
39 others in the role as SP<sub>a</sub> and SP<sub>b</sub>. Scheduling the Test Case K rotations during  
40 the Debug Phase was initially somewhat confusing and caused some minor  
41 delay in testing, but the PartialLogout in Step 13 caused additional confusion and  
42 delay while we sorted out an issue involving the acceptable response(s). The  
43 Test Plan had been tagged to be edited following a 3Q09 consensus item, but  
44 the Test Plan had remained unchanged and this resulted in some confusion over  
45 the acceptable test results.

46 Furthermore, CA discovered two interoperability issues, one regarding the  
47 AttributeStatement for Test Case S and another involving Test Case K that  
48 required code changes and some regression testing.

49 The Debug Phase was originally scheduled to complete by February 4<sup>th</sup>, but as a  
50 result of the accumulation of these issues and delays, actually did not complete  
51 until February 14<sup>th</sup>.

52 The Dry Run testing that began on February 15<sup>th</sup> completed almost without error.  
53 However, for the Dry Run, the rotation for Test Case K was modified from the  
54 Debug Phase in an effort to attempt to have all products handle different logout  
55 responses. In past test events, the Test Case K rotation was structured to  
56 expose products to different logout responses returned by different products to  
57 ensure interoperability across all acceptable responses. The DGI Test Lead  
58 changed the TC K rotation structure for the Dry Run for this purpose, and it  
59 resulted in IBM exhibiting a possible interoperability failure. Discussions between  
60 vendor actually decided that the issue observed was not actually a  
61 conformance/interoperability issue, but IBM decided to make a minor code  
62 change anyway.

63 The Certification Run began on February 24<sup>th</sup> and completed without error for all  
64 participants on March 1<sup>st</sup>.

65 While the test had its share of interoperability issues, the test event was  
66 performed at a high level and all the participants were very professional and  
67 worked extremely hard to meet the scheduling goals of the event and their own  
68 goals of demonstrating full-matrix interoperability. No alerts were issued nor were  
69 an emergency IRB call needed. Participants reported no difficulties in working  
70 with each other in resolving interoperability problems.

## 71 **DGI Perspective**

72 This section highlights some of the important observations from DGI team and  
73 the DGI Test Lead perspective from this test event.

## 74 **A Whole Lotta New**

75 There were a number of new things about the SAML 1Q11 test event, including  
76 Kantara's first run as sponsoring and leading the testing event. While Drummond  
77 Group returned to facilitate the testing event, a new DGI staff member was  
78 assigned as the responsible Test Lead. Undoubtedly, it was the first time for a  
79 number of folks at Kantara and Drummond Group in new positions and roles  
80 within this Interoperability Test Event, and that will be of benefit in future test  
81 events considering the experience gained in this event.

82 After being involved in the 2008 Test Event, CA did not participate in the 8-  
83 product 3Q09 interop event and ended up having to catch-up with a number of  
84 consensus items identified during that last event. Along with newcomer  
85 UNINETT testing the open-sourced simpleSAMLphp code base, both of these  
86 new vendors were involved in most of the interoperability and configuration  
87 issues discovered and resolved during this Test Event.

88 No doubt that consistency at each level of the participants of the Test Event has  
89 a direct effect on how smooth the event is executed. Since many of the 8  
90 products certified in the 3Q09 event did not return for the 1Q11 event, if the next  
91 event sees a number of returnees, the Test Event should plan for a rather bumpy  
92 Debug Phase to sort out interoperability issues arising from going too long  
93 between testing.

## 94 **Five Is Not Enough**

95 The test event that eventually became the 1Q11 event was originally slated to be  
96 executed in 4Q10, but a somewhat lack of interest in participation among  
97 vendors during the last half of 2010 resulted in the start of the Test Event being  
98 delayed until the beginning of 2011. It is recommended that future Test Events  
99 not be scheduled unless a minimum of six (6) participants will test.

100 Perhaps some participants are holding off returning to interoperability testing until  
101 the eGov 2.0 profile will be tested, but there wasn't enough interest from the  
102 vendor community in eGov 2.0 to facilitate any testing of that profile. There  
103 seems to be a sort of Catch-22 situation with eGov 2.0, and without the eGov 2.0  
104 profile being tested, there's a risk of stagnation being viewed by the vendor  
105 community with respect to interoperability. There is clearly a need for some  
106 marketplace drivers to motivate interoperability testing. More on this in the next  
107 section.

## 108 **Looking Forward**

109 Looking ahead to the next SAML 2.0 interoperability test event, here are some  
110 important issues to address or implement.

## 111 **Healthcare and eGov 2.0**

112 Focusing on industry profile areas, particularly in the areas of government and  
113 healthcare deployments, serve to keep the interoperability testing aspects from  
114 stagnating and suffering from lack of vendor participation. It is recommended  
115 that an emphasis be placed on eGov 2.0 and Healthcare XSPA profile modes for  
116 future testing events.

## 117 **Make Process for Situation Where Only One Participant Registers for 118 a Mode or Profile**

119 Similar to 3Q09, this year we had at least one product be the sole registrant for  
120 conformance modes which meant they were unable to test for those modes. We  
121 indicated to the participant that due to lack of participation that they would not be  
122 able to test the modes in question (and therefore not certified for those modes).  
123 There was some disappointment registered by IBM since they had been certified  
124 interoperable for those profile(s) in 3Q09 and some discussion precipitated with  
125 the IRB during the review of the Final Report. During previous test events  
126 sponsored by the Liberty Alliance, there were discussions about a process to  
127 handle this situation in the future.

128 One suggestion would be to require/offer a product which had test in a previous  
129 IOP event and tested the needed conformance mode to return and provide at  
130 least one testing partner. Of course, there are challenges with this approach such  
131 as feasibility of participation, if an updated certification seal granted and payment  
132 of test services.

133 This situation remains a topic for further discussion.

## 134 **Expand Test Tool for More IdP Error Test Cases**

135 This was an issue brought up during previous testing years, and its value is still  
136 apparent now. The error tool currently functions only as an IdP in sending %bad+  
137 assertions and responses to the SP-under test. However, we do have an IdP  
138 error test which has required us to seek a participant to volunteer to perform. It is  
139 not a good situation to ask participants to conduct the testing.

140 We need to expand the error test tool to have the IdP error test scenario. By  
141 doing so, it will also open the doors to expanding our error testing, such as  
142 testing other negative conditions within the SP communication, like the  
143 AuthnRequest.

144 **IRB Review of Test Plan?**

145 CA, one of the participants in the 1Q11 test event lodged several opinions with  
146 the DGI Test Lead during the Test Event that perhaps one or more of the Test  
147 Cases in the Kantara Test Plan may not accurately represent good tests of the  
148 SAML 2.0 specification or profile objectives. It might be worthwhile for the IRB to  
149 further investigate CA's claims and determine if any changes to the Test Plan are  
150 warranted ahead of future Test Events.

151 **About Drummond Group Inc.**

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