1

Liberty ID-WSF 2.0 Interoperability Testing Procedures

Version Draft 1.0-01

16 August 2006

Editors:

Eric Tiffany, Liberty Alliance Project

Contributors:

Greg Whitehead, Hewlett Packard
Emily Xu, Sun Microsystems
Roger Sullivan, Oracle
Stuart Jensen, Novell
Nick Ragouzis, Enosis
Sampo Kellomäki, Symlabs
Conor Cahill, Intel

Abstract:

The conformance program is designed to validate core functionality via interoperability testing so that purchasers of Liberty-based technology can focus on other details specific to their market and/or deployment. This document describes the process and procedures for conducting interoperability testing for the Liberty Interoperable certification program. The goal of this document, combined with the SCR and the Liberty Conformance Process and Administration document is to unambiguously define the process and procedures that will be followed at conformance interoperability testing events. The procedures in this document are intended to streamline testing events, shorten testing times, and minimize disputes that could result in requests for arbitration.

File: ID-WSF-2-0-TestProcedures-v1-01.odt

Change log (to be deleted when published publicly):

1.0-01   9/26/06   ET   Initial version

31 # Contents

1. Introduction

This document refers to ID-WSF 2.0 and the conformance profiles described in the ID-WSF 2.0 Static Conformance Requirements (SCR) [LibertyIDWSF20SCR].

The conformance program is designed to validate core functionality via interoperability testing so that purchasers of Liberty-based technology can focus on other details specific to their market and/or deployment. This document describes the process and procedures for conducting interoperability testing for conformance.

The goal of this document, combined with the SCR and the Liberty Conformance Process and Administration document is to unambiguously define the procedures that will be followed at conformance interoperability testing events. The procedures in this document are intended to streamline testing events, shorten testing times, and minimize disputes that could result in requests for arbitration.

The SCR describes a total of nine conformance profiles and the specific features that are required or optional for each profile. The tables below summarizes the features that comprise the profiles. A vendor can participate in conformance interoperability testing in the role of any one or more of these conformance profiles.

Feature	SAML SP WSC	LUAD WSC	SAML SP WSP	LUAD WSP	SAML IdP	ID-WSF IdP	DS	PS	IS
WSC Common	MUST	MUST							
WSP Common			MUST	MUST			MUST	MUST	MUST
SAML SP WSC SOAP Binding	MUST								
SAML SP WSC Security Security Mechanisms	MUST								
LUAD		MUST		MUST			OPT	OPT	OPT
SAML DS Bootstrap	MUST				MUST				
Authentication Service		MUST				MUST			
SSO Service	OPT	OPT				MUST			
Identity Mapping Service						MUST			
Service Registration			OPT	OPT			MUST		OPT
Service Discovery	MUST	MUST					MUST		
Service Invocation	MUST	MUST							
Group & User Management	OPT	OPT						MUST	
Invitations	OPT	OPT						OPT	
Interaction Service			OPT	OPT			OPT		MUST

Table 1 ID-WSF 2.0 SCR Profiles Matrix

This document is maintained by the Technology Expert Group (TEG). Testing events are organized and managed by Liberty staff under the direction of the Liberty Conformance Review Team (LCRT). The LCRT is a sub-team of the Liberty Alliance management board and will arbitrate any claims arising from testing events and shall act as an official observer of testing events.

59 ## 2. Overview of Conformance Process

60 See [LibConfProc]

3. Test Procedures

Testing will follow a simple scenario based approach with multiple passes that test required features, and optional features when support if indicated by the vendor in the registration form. The basic scenario is intended to simulate the use of the full range of range of features available in the ID-WSF framework :

1. Authenticate

2. Invoke Discovery Service

3. Contact Service via WSC and WSP.

4. Optionally interact with user.

5. Return service results

It will be necessary to repeat this scenario through several passes in order test each of the profiles specified in the SCR and the test process is designed avoid repeating unnecessary steps to the extent possible.

Note that these testing procedures integrate the testing of several profiles concurrently in a single test sequence. Typically, one testing sequence will benefit all testing partners as they each try to achieve interoperability with the required number of testing partners.

3.1. Common Test Features

This section describes test features or procedures that are common across some or all of the profiles defined in subsequent sections.

3.1.1. Asymmetry of Testing Requirements

One of the fundamental aspects of interoperability testing is that two or more participants must work together in complementary roles to achieve a testing result. In several cases, one role (e.g. WSC) is required to support a feature that is optional for the complementary role (e.g. WSP). In these cases, the WSC (e.g.) is dependent on the fact that enough partners will implement the optional features so that interoperability can be demonstrated.

Typically, a test participant will implement both roles (e.g., a WSC and WSP) and they have a vested interest in making mutual interoperability possible. In this case, the sensible strategy is to build the optional features (i.e., observe the Golden Rule).

3.1.2. Security Mechanisms

The initial portion of each test sequence requires that the implementation demonstrate correct functioning of each of the required security mechanisms for the profile under test. This is accomplished by repeating a sequence of test steps, changing the security mechanism prior to each repetition.

Once all of the required security mechanisms are tested, the remainder of the testing is performed using a security mechanism agreed to by all testing partners.

The table below lists the ID-WSF 2.0 security mechanisms that are required for the different profiles under test. Note that the WSP, DS and IS profiles have three alternative subsets (ALT1, ALT2, ALT3) of the security mechanisms, at least one of which must be demonstrated.[1]

Test Step	Security Mechanism	SAML SP WSC	LUAD WSC	WSP, DS, PS, IS
SEC-NN	**urn:liberty:security:2003-08:null:null**	**MUST**	**MUST**	**ALT1**
SEC-TN	**urn:liberty:security:2003-08:TLS:null**	**MUST**	**MUST**	**ALT1**
SEC-NB	**urn:liberty:security:2005-02:null:Bearer**	**MUST**	**MUST**	**ALT2**
SEC-TB	**urn:liberty:security:2005-02:TLS:Bearer**	**MUST**	**MUST**	**ALT2**
SEC-N2	**urn:liberty:security:2006-08:null:SAMLV2**	**MUST**		**ALT3**
SEC-T2	**urn:liberty:security:2006-08:TLS:SAMLV2**	**MUST**		**ALT3**
SEC-CP	**urn:liberty:security:2006-08:ClientTLS:peerSAMLV2**	**MUST**		**ALT3**

Table 2: ID-WSF 2.0 Security Mechanisms

---

[1]This table reflects a pending correction to the ID-WSF 2.0 SCR. The original SCR indicated that the SAML SP WSC was required to perform ClientTLS:SAMLV2, whereas the intent was that it be ClientTLS:peerSAMLV2 as depicted.

79 3.1.3. Service Invocation

80 Essentially every test sequence for WSC and WSP include a service invocation step. The ID-WSF 2.0
81 specifications do not normatively specify the nature of such services, and these testing procedure do not explicitly
82 define a service interface to be invoked. The requirements only state that conforming WSC and WSP
83 implementations must support the invocation of a discovered service.

84 However, many test participants have found it useful to agree upon a common service for demonstrating
85 interoperability. The Liberty ID Hello World Protocol [LibIDHello] is ideally suited for this purpose, and test
86 participants are encouraged to implement support for this service.

87 3.1.4. Test Pairings

88 Test partners are assigned randomly and dynamically from amongst all participants with complementary
89 implementations who are ready to test at a particular time. As noted above, the test procedures are designed so
90 that all testing partners in a particular test benefit from participating[2] ((i.e., the test "counts" for all participants). The
91 test pairings shown in the table below are typical:

	WSC	WSP	DS/IDP
	A	A	B
	A	B	A
Test 1	B	B	A
	B	A	B

	WSC	WSP	DS/IDP
	A	A	C
	A	C	A
Test 2	C	C	A
	C	A	C

93 After these tests, Team A has tested with 2 partners in all roles, and is "done" for WSC, WSP, and DS. If Teams B
94 and C test together (e.g. substituting C for A in Test 1) then B and C will also be done for all three profiles[3].

95 3.2. Testing Steps

96 The following sections list the the testing steps for the various profiles noted in Table 1and whether they are
97 required ("MUST"), optional ("OPT"), or alternates (ALT; see discussion of security mechanisms above). Each list
98 is an expansion of the requirements in [LibertyIDWSF20SCR] derived from the referenced specifications.

99 3.2.1. SAML SP WSC/P, SAML IDP, DS Test Procedures

100 The test steps for the SAML-based profiles are listed in Table 3. Note the following preconditions:

101   1. A principal (user) must be created and federated between the IDP and the SP-WSC.

102   2. The initial sequence assumes that a service has been registered at the DS. The manner by which this is
103   accomplished is not specified, but typically it could be done by the WSP registering the service with the
104   DS. As that operation is optional for the WSP, however, some other method for registering the service at
105   the DS may need to be used.

106 The optional Single Signon (SSO) Service invocation will require the participation of a suitable AS (ID-WSF IDP).
107 The optional PAOS test sequence at the end of the procedure will (typically) need to be performed in conjunction
108 with a LUAD WSP that supports PAOS.

---

[2]After a participant has met the minimum requirements, their participation no longer is strictly necessary and thus they don't benefit directly.
However, it is sensible to test with as many partners as possible.
[3]This procedure thus requires twelve separate tests to complete testing of three teams against three profiles. The same could be
accomplished theoretically by six tests where each test involved all three teams, each in a different role. However, coordinating a three-way
test has proven extremely difficult and time-consuming.

No.	Test Step	Feature	SAML SP WSC	SAML SP WSP	SAML IdP	DS
1	SEC-TN	TLS:null (modify for each iteration)	MUST	ALT1		ALT1
2	ID-Login	Principal SSO via Artifact Profile (already Federated)			MUST	
3	ID-DSBA	SAML Assertion with DiscoveryEPR attribute			MUST	
4	ID-DSBP	Process Bootstrap to locate Disco	MUST			
5	DS-WSCQ1	WSC Query Plain	MUST			MUST
6	DS-QR	DS QueryResponse	MUST			MUST
7	WS-SI	Service Invocation	MUST	MUST		
8	Repeat	Repeat 1-7 above for each secmec				
9	DS-MODE	DS Modify InsertEntry		OPT		MUST
10	DS-QRE	DS QueryResponse	MUST			MUST
11	WS-SI	Service Invocation	MUST	MUST		
12	DS-WSCQ2	WSC Query with Options				
13	DS-QR	DS QueryResponse	MUST			MUST
14	WS-SI	Service Invocation	MUST	MUST		
15	DS-WSCQ1	WSC Query Plain	MUST			MUST
16	DS-QR	DS QueryResponse	MUST			MUST
17	IR-1	1 - WSC sends Request with redirect=true	MUST			
18	INT-PH	Process Interaction Header		MUST		MUST
19	IR-2	2 - WSP sends SOAP Fault with Redirect		OPT		OPT
20	IR-3	3 - WSC HTTP 302 to RedirectURL at WSP	MUST			
21	IR-4	4 - WSP Validate URLs		OPT		OPT
22	IR-CD	c,d - WSP Draw inquiry page, enter		OPT		OPT
23	IR-E	e - WSP Process GET/POST answers		OPT		OPT
24	IR-5	5,6 - WSP HTTP 302 to ReturnToURL		OPT		OPT
25	IR-7	7 - WSC Resend	MUST			
26	IR-8	8 - WSP Response		OPT		OPT
27	IR-V	Validate Result	MUST	OPT		OPT
28	AS-SSOS	Single Signon Service (SAML Token)	OPT			
29	SIU Setup	Setup for EndpointUpdate (partial) Credential Change				
30	ID-Login	Principal SSO via Artifact Profile (already Federated)				
31	ID-DSBA	SAML Assertion with DiscoveryEPR attribute			MUST	
32	ID-DSBP	Process Bootstrap to locate Disco	MUST			
33	DS-WSCQ1	WSC Query Plain	MUST			MUST
34	DS-QR	DS QueryResponse	MUST			MUST
35	WS-SI	Service Invocation	MUST	MUST		
36	COM-SIUC	EndpointUpdate Credential change	MUST			
37	WS-SI	Service Invocation	MUST	MUST		
38	SIU Setup	Setup for EndpointUpdatee (complete)				
39	ID-Login	Principal SSO via Artifact Profile (already Federated)				
40	ID-DSBA	SAML Assertion with DiscoveryEPR attribute			MUST	
41	ID-DSBP	Process Bootstrap to locate Disco	MUST			
42	DS-WSCQ1	WSC Query Plain	MUST			MUST
43	DS-QR	DS QueryResponse	MUST			MUST
44	WS-SI	Service Invocation	MUST	MUST		
45	COM-SIUE	EndpointUpdateFault retry	MUST			
46	WS-SI	Service Invocation	MUST	MUST		
47	PAOS-RR	PAOS Request-Response pattern	OPT			OPT
48	PAOS-R	PAOS Response pattern	OPT			OPT

Table 3: SAML SP WSC/P, SAML IDP, DS Test Procedures

109 **3.2.2. LUAD WSC/P, ID-WSF IDP, DS, IS Test Procedures**

110 The LUAD WSC/P test steps are listed in Table 4. Note: the interaction sequence (test steps in yellow) are
111 optional, except for interaction service (IS) profile testing. Also, the PAOS sequence will require the participation of
112 a PAOS-capable SP/WSP implementation.

No.	Test Steps	Feature	LUAD WSC	LUAD WSP	ID-WSF IdP	DS	IS
1	SEC-TN	TLS:null	MUST	ALT1		ALT1	ALT1
2	AS-WSCI	WSC Authn Invocation	MUST				
3	AS-WSPR	WSP SASLResponse			MUST		
4	AS-WSPPA	WSC SASL Request PLAIN or ANONYMOUS	MUST				
5	DS-WSCQ1	WSC Query Plain	MUST			MUST	
6	DS-QR	DS QueryResponse	MUST			MUST	
7	WS-SI	Service Invocation	MUST	MUST			
8	Repeat	Repeat above for each secmec					
9	SEC-ANY	Set secmec for rest of tests					
10	AS-WSCI	WSC Authn Invocation	MUST				
11	AS-WSPR	WSP SASLResponse			MUST		
12	AS-WSPMD5	WSC SASL Request CRAM-MD5	MUST				
13	COM-SCH	Send Correlation Header	MUST	MUST		MUST	MUST
14	COM-PCH	Process Correlation Header	MUST	MUST		MUST	MUST
15	AS-PWT	Truncation	MUST				
16	AS-WSPPA	WSC SASL Request PLAIN or ANONYMOUS	MUST				
17	AS-PWL	Lowercase	MUST				
18	AS-WSPPA	WSC SASL Request PLAIN or ANONYMOUS	MUST				
19	AS-PWU	Uppercase	MUST				
20	AS-WSPPA	WSC SASL Request PLAIN or ANONYMOUS	MUST				
21	AS-PWS	Select	MUST				
22	AS-WSPPA	WSC SASL Request PLAIN or ANONYMOUS	MUST				
23	DS-MOD	DS Modify InsertEntry		OPT		MUST	OPT
24	DS-QRE	DS QueryResponse	MUST			MUST	
25	WS-SI	Service Invocation	MUST	MUST			
26	DS-WSCQ2	WSC Query with Options					
27	DS-QR	DS QueryResponse	MUST			MUST	
28	WS-SI	Service Invocation	MUST	MUST			
29	AS-SSOS	SSO Service Invocation (SAML Token)	OPT		MUST		
30	AS-SSOE	SSO Service Invocation (ECP)	OPT		MUST		
31	DS-WSCQ1	WSC Query Plain	MUST			MUST	
32	DS-QR	DS QueryResponse	MUST			MUST	
33	IS-WSC1	WSC sends UserInteraction redirect=false	OPT				
34	INT-PH	Process Interaction Header		MUST		MUST	MUST
35	IS-WSP1	WSP sends InteractionRequest to IS (or LUAD WSC)		OPT		OPT	
36	IS-ISQ	IS Queries Principal					MUST
37	IS-ISR	IS Sends InteractionResponse to WSP					MUST
38	IS-WSP2	WSP responds to WSC		OPT		OPT	
39	IS-WSC2	WSC processes response					
40	SIU Setup	Setup for EndpointUpdate CredentialChange					
41	Authenticate	Authenticate with ID-WSF IdP (AS) any profile					
42	DS-WSCQ1	WSC Query Plain	MUST			MUST	
43	DS-QR	DS QueryResponse	MUST			MUST	
44	WS-SI	Service Invocation	MUST	MUST			
45	COM-SIUC	EndpointUpdate (Partial) Credential change	MUST				
46	SIU Setup	Setup for EndpointUpdate EndpointMoved					
47	Authenticate	Authenticate with ID-WSF IdP (AS) any profile					
48	DS-WSCQ1	WSC Query Plain	MUST			MUST	
49	DS-QR	DS QueryResponse	MUST			MUST	
50	WS-SI	Service Invocation	MUST	MUST			
51	COM-SIUE	EndpointUpdate SOAP Fault Process	MUST				
52	PAOS-RR	PAOS Request-Response pattern		OPT		OPT	OPT
53	PAOS-R	PAOS Response pattern		OPT		OPT	OPT

Table 4: LUAD WSC/P, ID-WSF IDP, DS, IS Test Procedures

113 ### 3.2.3. Core People Service (PS) Testing Steps

114 The People Service (PS) testing steps are divided into two sections: the "core" People Service features, and the
115 optional "invitation" features (covered in the next section). The core test steps are listed in Table 5.

Step	Function	WSC	PS	IDP/DS	Comment	Context
1	SecMech TLS:null	MUST	ALT1	ALT1		
2	Authenticate	MUST		MUST		
3	Discover PS EPR	MUST		MUST		
4	Invoke PS service (AddEntity)	MUST	MUST			
5	Repeat 1-4 with remaining SecMechs					
6	Add Entity ("A") Subscription	MUST	MUST			A
7	Add Known Entity ("B") Subscription includeData="no"	MUST	MUST			A, B
8	Add Collection ("Top" with "A" and "B") w/Subscription	MUST	MUST			T = {A, B}
9	Add Entity ("C")	MUST	MUST			T, A, B, C
10	Add collection Sub with "C"	MUST	MUST			Sub = {C}
11	AddtoCollection Top entity Sub	MUST	MUST		Expect notification of Top change	Top = {A, B, SUB}
12	ListMembersRequest of Top	MUST	MUST			
13	- Structure unspecified	MUST	MUST		Result = {A, B}	
14	- Structure="children" w/Subscription	MUST	MUST		Result = {A, B}	
15	- Structure="tree"	MUST	MUST		Result = {A, B, Sub{C}}	
16	- Structure="Entities"	MUST	MUST		Result = {A, B,C}	
17	Set Object Info "C" to "C1"	MUST	MUST		DO NOT Expect notification of List change	T={A, B, S{C1}}
18	Get Object Info for "C1"	MUST	MUST			T={A, B, S{C1}}
19	Set Object info for "Sub" to "Sub1"	MUST	MUST		Expect notification of ListMembers change	T={A, B, S1{C1}}
20	Get Object Info for "Sub1"	MUST	MUST			T={A, B, S1{C1}}
21	Set Object Info for "B" to "B1"	MUST	MUST		Expect notification of ListMembers change	T={A, B1, S1{C1}}
22	Test Membership of C1 in TOP w/Subscription	MUST	MUST		Result = true	T={A, B1, S1{C1}}
23	Query for nodeType = "collection" within TOP w/Subscription	MUST	MUST		Result = {S1}	T={A, B1, S1{C1}}
24	Remove Collection Sub1	MUST	MUST		Expect notification of ListMembers change AND TESTMember change AND Query Change	T={A, B1}, C1
25	Remove From Collection B1 from TOP	MUST	MUST		Expect notification of ListMembers change	T={A}, B1, C1
26	Remove Entity B1	MUST	MUST		DO NOT Expect notification of List change	T={A}, C1
27	Resolve Identifier for "A"	MUST	MUST			

Table 5: Core People Service Testing Steps

116 The core PS functions involve

117 • creating and manipulating entities and groups of entities,

118 • listing and querying this data, and

119 • subscription to, and notification of, changes in this data

120 In addition, since the PS is required to behave as a WSP, the initial sequence of test steps include a repetition of
121 steps to exercise the required security mechanisms.

3.2.4. PS Invitation testing steps

123 The PS invitation steps are listed in Table 6. Note that the invitation scenario involves two separate users, A and
124 B, and there are separate ID-WSF roles required for each user. The inviting user is A, and the invited user is B.
125 Certain steps involving interactions with A and B to facilitate the interaction protocol are out of scope, but are
126 described in [LibPS].

127 In order to fairly test the interoperability of two vendors X and Y, the roles are assigned as follows so that the
128 "interesting" interactions occur between different vendor implementations:

129   Vendor X: SPa, IDPa, DSa, IDPb, DSb

130   Vendor Y: PSa

131 The preconditions for the test include the creation of users A and B, and the registration of the PSa EPR at DSa.
132 Any supported security mechanism may be employed for these tests.

Step	Feature	SPa	IDPa	DSa	PSa	IDPb	DSb
1	Authenticate User A		MUST				
2	Collect info for Invited User B						
3	Query For User B						
4	Discover PSa EPR			OPT			
5	AddedEntity B	OPT			MUST		
6	Send invitation to user B						
7	B accesses invitation						
8	B consents						
9	Authenticate User B at IDPb					MUST	
10	Discover Auth Service for B				MUST		MUST
11	Invoke IdentityMapingService for B	OPT			OPT	MUST	
12	Notify about IdentityToken for B	OPT			MUST		
13	Discover Service for B	MUST					MUST

Table 6: PS Invitation Steps

134 # 4. Testing Checklist

135 This form must be completed for each complete test run. Both parties to the test must agree to the indication of
136 pass/fail for each feature tested and sign each copy of the form. A copy of the form will go to each testing party
137 and the original will be kept on record by LCRT/ISTO.

138 The product name is simply an identifier; it does not have to be the public name of the product.

IDP Tester	
Product Name	
Version (major.minor)	
Implementation Type(s)	IDP IDP Extended
Company	
Contact Name	
Contact Phone	
Contact Email	
Signature (after testing)	

139

SP Tester	
Product Name	
Version (major.minor)	
Implementation Type(s)	SP Basic SP Complete SP Extended
Company	
Contact Name	
Contact Phone	
Contact Email	
Signature (after testing)	

140

LECP Tester	
Product Name	
Version (major.minor)	
Company	
Contact Name	
Contact Phone	
Contact Email	
Signature (after testing)	

141

LCRT Representative	
Contact Name	
Signature (after testing)	

142

5. References

143 [LibConfProc] Smith, Jeff. "Liberty Conformance Process and Administration," Version 1.0-05, Liberty Alliance
144 Project (April 2004), *http://www.projectliberty.org/conformance/*
145

147 [LibertyIDWSF20SCR] Whitehead, Greg. "Liberty ID-WSF 2.0 Static Conformance Requirements," Version 1.0,
148 Liberty Alliance Project (September 2006). *http://www.projectliberty/specs*
149

150 [LibPS] Yuzo Koga and Paul Madsen, "Liberty ID-WSF People Service Specification," Version 1.0, Liberty Alliance
151 Project (September 2006), http://www.projectliberty.org/specs
152

153 [LibIDHello] Kellomäki, Sampo, "Liberty ID Hello World Protocol," Version 1.0, Liberty Alliance Project (2006),
154 http://www.projectliberty.org/specs
155

156 [LibOSSTest] Conor Cahill, "Liberty Client Toolkit," Version 0.8.5, http://www.cahillfamily.com/OpenSource/

157 ## A. Test Harness

158 An open source implementation of the ID-WSF 2.0 protocols [LibOSSTest] is used to conduct the negative test
159 steps for the ID-WSF IDP (aka Authentication Service, or AS) and DS profiles. The test steps are listed below;
160 additional tests may be available in later versions of the software.

161 ### A.1. ID-WSF IDP Tests

162 These are the test steps from the `test-auth` test script:

163   1.   good credentials works

164   2.   using PLAIN works

165   3.   Immediate PLAIN (no negotiation) works

166   4.   bad password fails

167   5.   bad userid fails

168 ### A.2. Disco Tests

169 These are the test steps from the `test-disco` test script:

170   1.   We can find good svc

171   2.   Cleanup old test data

172   3.   Query by PID for Provider 1 works

173   4.   Query by PID w/o assn for Provider 1 works

174   5.   We can find 2nd good svc

175   6.   Cleanup 2nd provider old test data

176   7.   Query by PID for Provider 2 works

177   8.   Query w/no RS works

178   9.   Query w/RS but no ST/PID fails

179   10. Query by ProviderID & ST works

180   11. Query by ST w/RT=only-one works

181   12. Query by ST&PID w/RT=only-one works

182   13. Good svc, Bad resultsType arg faults

183   14. Query all Svc Metadata succeeds

184   15. Query non-existant Svc metadata by ID fails

185   16. Register one simple metadata works

186   17. Query that metadata works

187   18. Delete that metadata works

188   19. Delete that metadata again fails

189   20. Query that metadata now fails

190   21. Register one complex metadata works

191   22. Query that metadata works

192   23. Query that metadata with other IDs works

193   24. Replace that metadata works

194   25. Query the replaced metadata works

195   26. Delete that metadata works

196   27. Query that metadata now fails

197   28. Register several metadata works

198   29. Query those metadata works

199   30. Delete those metadata works

200   31. Query those metadata now fails

201   32. Register several metadata works (again)

202   33. Disco of cal svc by type before assoc fails

203   34. Associate cal with user works

204   35. Query cal MD Assoc works

205   36. Query MD Assocs shows cal

206   37. Disco of cal svc by type now works

207   38. Disco of cal w/RT=all gets just 1 EPR

208   39. Disco of cal w/RT=only-one gets just 1 EPR

209   40. Delete cal MD Assoc works

210   41. Query cal MD Assoc fails

211   42. Disco of cal svc by type now fails again

212   43. 2nd Delete cal MD Assoc fails

213   44. Delete of bogus MD Assoc fails

214   45. Associate cal with user again works

215   46. Disco of cal svc by type now works

216   47. Assoc Del of cal & bogus MD fails

217   48. Assoc Del of cal & unassoc (atm) MD fails

218   49. Disco of cal w/action matches null action

219   50. Disco of cal w/sech mech w/2 addrs works

220   51. Disco of all of cal works

221   52. Disco of only-one of all of cal gets 1st

222   53. Disco of old Cal instance works

223   54. Replace Cal metadata works

224   55. Disco of replaced secMech now fails

225   56. Disco of cal w/sech mech has only 1 addr now

226   57. Disco of all of cal shows only replaced data

227   58. Disco of old Cal instance fails now

228   59. Associate atm with user works

229   60. New assoc doesn't impact disco of Cal svc

230   61. Disco of atm shows actions

231   62. Disco of atm w/all shows redundant addrs

232   63. Disco of atm w/action shows that endpoint

233   64. Disco of atm w/2nd action shows that endpoint

234   65. Disco of atm w/2 actions shows same endpoint

235   66. ResultType best doesn't impact action match

236   67. Disco of atm w/acts across EPs gets both EPs

237   68. Disco of atm needs 2 EPs but RT=only-one fails

238   69. Disco of atm w/RT=only-one from 2nd EP works

239   70. Disco of atm w/no acts & RT=only-one fails

240   71. Disco of atm w/good option works

241   72. Disco of atm w/two good options works

242   73. Disco of atm w/last options works

243   74. Disco of atm w/all options works

244   75. Disco of atm w/bad option fails

245   76. Disco of atm w/1 good & 1 bad option fails

246   77. Assoc Del of cal & atm now works