

1
2
3
4



5
6
7

Access to Identity-Enabled Web Services in Cross-Border, Inter-Federation Scenarios

Version: 1.0

11
12

Abstract:

The following whitepaper describes the different potential options to access identity-based web services in Inter-federation (Inter-CoT¹) scenarios; i.e., when there is no business relationship between the service requestor and the service provider AND such relationship cannot be inherited from a commonly-trusted third party, such as in typical federation cases - Intra-CoT.

Even if there is such lack of direct business relationship, final interoperability is still possible by (indirect) inheritance of the trust relationship existing among the entities operating the different CoTs.

The solutions proposed in this whitepaper are especially interesting in certain scenarios, such as those associated to roaming situations in the telecommunications industry. They can also be applicable to other industries, such as the eHealth or eGovernment sectors.

Filename: access-to-identity-enabled-services-in-inter-cot-scenarios-v1.0.pdf

25

¹ CoT – Circle of Trust

26 **Editors:**

27 Carolina Canales-Valenzuela, Ericsson

28 Sampo Kellomäki, Symlabs

29

30 **Contributors:**

31 Fulup Ar Foll, SUN

32 Conor Cahill, Intel

33 Gaël Gourmelen, Orange

34 Mikko Laukkanen, Teliasonera

35 Rob Lockhart, IEEE-ISTO

36 Antonio Navarro, Symlabs

37 Pat Patterson, SUN

38 **Notice:**

39 This document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby
40 granted to use the document solely for the purpose of implementing the Specification. No rights
41 are granted to prepare derivative works of this Specification. Entities seeking permission to
42 reproduce portions of this document for other uses must contact the Liberty Alliance to determine
43 whether an appropriate license for such use is available.

44
45 Implementation of certain elements of this document may require licenses under third party
46 intellectual property rights, including without limitation, patent rights. The Sponsors of and any
47 other contributors to the Specification are not and shall not be held responsible in any manner for
48 identifying or failing to identify any or all such third party intellectual property rights. **This**
49 **Specification is provided "AS IS," and no participant in the Liberty Alliance makes any**
50 **warranty of any kind, express or implied, including any implied warranties of**
51 **merchantability, non-infringement of third party intellectual property rights, and fitness for**
52 **a particular purpose.** Implementers of this Specification are advised to review the Liberty
53 Alliance Project's website (<http://www.projectliberty.org/>) for information concerning any
54 Necessary Claims Disclosure Notices that have been received by the Liberty Alliance
55 Management Board.

56
57 Copyright © 2007 2FA Technology; Adobe Systems; Agencia Catalana De Certificacio; America
58 Online, Inc.; American Express Company; Amsoft Systems Pvt Ltd.; Avatier Corporation;
59 BIPAC; BMC Software, Inc.; Bank of America Corporation; Beta Systems Software AG; British
60 Telecommunications plc; Computer Associates International, Inc.; Credentica; DataPower
61 Technology, Inc.; Deutsche Telekom AG, T-Com; Diamelle Technologies, Inc.; Diversinet Corp.;
62 Drummond Group Inc.; Enosis Group LLC; Entrust, Inc.; Epok, Inc.; Ericsson; Falkin Systems
63 LLC; Fidelity Investments; Forum Systems, Inc.; France Télécom; French Government Agence
64 pour le développement de l'administration électronique (ADAE); Fugen Solutions, Inc; Fulvens
65 Ltd.; GSA Office of Governmentwide Policy; Gamefederation; Gemalto; General Motors;
66 GeoFederation; Giesecke & Devrient GmbH; Hewlett-Packard Company; Hochhauser & Co.,
67 LLC; IBM Corporation; Intel Corporation; Intuit Inc.; Kantega; Kayak Interactive; Livo
68 Technologies; Luminance Consulting Services; Mark Wahl; Mary Ruddy, MasterCard
69 International; MedCommons Inc.; Mobile Telephone Networks (Pty) Ltd; NanoIdent Biometrics
70 GmbH, NEC Corporation; NTT DoCoMo, Inc.; Netegrity, Inc.; Neustar, Inc.; New Zealand
71 Government State Services Commission; Nippon Telegraph and Telephone Corporation; Nokia
72 Corporation; Novell, Inc.; OpenNetwork; Oracle Corporation; Ping Identity Corporation; RSA
73 Security Inc.; Reactivity Inc.; Royal Mail Group plc; SanDisk Corporation, SAP AG; Senforce;
74 Sharp Laboratories of America; Sigaba; SmartTrust; Sony Corporation; Sun Microsystems, Inc.;
75 Supremacy Financial Corporation; Symlabs, Inc.; Telecom Italia S.p.A.; Telefónica Móviles,
76 S.A.; Telenor R&D; Thales e-Security; Trusted Network Technologies; UNINETT AS; UTI;
77 VeriSign, Inc.; Vodafone Group Plc.; Wave Systems Corp. All rights reserved.

78 **Contents**
79
80 **1 Introduction 5**
81 **2 Description 6**
82 2.1 SSO Using IdP Proxying 6
83 2.2 Access to Identity-enabled Web Services..... 7
84 2.2.1 Web Services Invocation Using DS Proxying 7
85 2.2.2 Inter-Federation (Inter-CoT) Discovery 9
86 2.2.3 Direct Access 11
87 2.3 Metadata Distribution in Inter-CoT Scenarios..... 11
88 **3 Conclusion..... 13**
89 **4 References 14**
90
91

92 1 Introduction

93 The goal of the present paper is to describe the scenario where an application (Service
94 Provider B, SP-B, working as web service consumer WSC-B) wants to access an identity-
95 enabled service (Web Service Provider, WSP-A), and both of them belong to different
96 Circles of Trusts (CoT, as defined in [LibertyGlossary]) or federations. Due to this, it is
97 assumed that, although no direct business agreement exists between SP-B/WSC-B and
98 SP-A/WSC-A, some sort of business agreement exists between the entities operating the
99 IdPs/DSs of both CoTs.

100 This document explores different mechanisms to achieve this, in particular:

- 101 1. **Discovery Service Proxying:** There exists a trust relationship between the
102 entities operating the DSs of both CoTs, trust is established by proxying WSC-B's
103 discovery request through DS-B towards DS-A.
- 104 2. **Inter-Federation (Inter-CoT) Discovery:** In this case, it is assumed that WSC-B
105 obtains a direct reference to DS-A, trust is established between both entities by
106 leveraging the already existing trust (business) relationship between DS-A and
107 DS-B.
- 108 3. **Direct Access:** In this case, DS-B is able to directly provide a reference to WSP-
109 A, however, this effectively implies that WSP-A is registered in DS-B, and
110 therefore both entities factually belong to the same CoT (any sort of business
111 relationship between them is implied).

112 Note that in all of the three scenarios, apart from some sort of business relationship
113 between "distinguished" members of the different CoTs (e.g., the IdP-DSs), there is a
114 need to be able to establish a direct or derived trust relationship at the PKI level. See
115 [TrustModelsGuidelines] for further information about trust relationships.

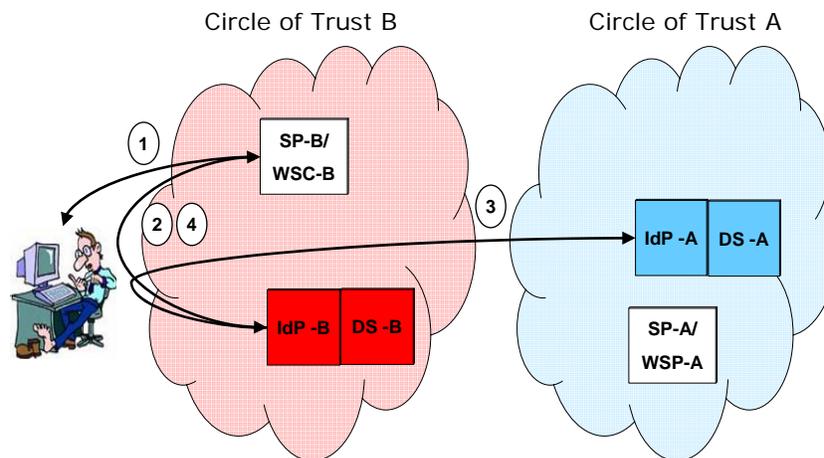
116 Regarding the scenario of a heavily firewalled environment, it seems to be a requirement
117 that each CoT manages its own SPs and firewalling rules. The other CoT's administrators
118 should not have to make any "per SP" configuration.

119 2 Description

120 2.1 SSO Using IdP Proxying

121 The figure below depicts this scenario.

122



123

124

Figure 1: SSO in Inter-CoT (Inter-federation) scenario

125

126 In brief, and according to the IdP Proxying functionality as described in [SAMLCore2]:

- 127 1. Albert, a user with an account at IdP-A, accesses a page on SP-B which is in the
128 CoT of IdP-B.
- 129 2. The SP-B logically contacts IdP-B. Given that SP-B is in the CoT of IdP-B, the
130 access control is natural. This requires a firewall hole between Albert and IdP-B.
- 131 3. IdP B proxies the authentication of the user, Albert, to IdP-A by using HTTP
132 redirect. The firewall has to have a hole from Albert to IdP-A. (This seems to be
133 the usual case inside a given CoT.)
- 134 4. IdP-B trusts IdP-A to authenticate the user and consumes the assertion from IdP-A
135 and then issues a new assertion to SP-B (including Albert's federation handle as
136 understood by SP-B), i.e., the SP-B only needs to trust the leader of its own CoT,
137 the IdP-B.

138

139 The assertion from IdP-B towards SP-B has discovery bootstrap information pointing to
140 DS-B. Such information can be used to discover services in CoT-B and to perform
141 Discovery Proxying to find services in CoT-A. See Section 2.2.1 "Web Services
142 Invocation Using DS Proxying."

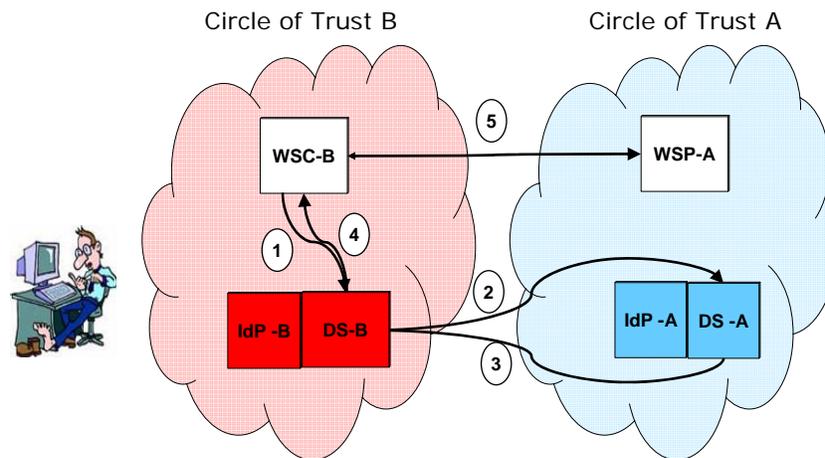
143 In the Inter-CoT Discovery approach in Section 2.2.2, IdP-B would include a reference to
144 Albert's DS (DS-A) in the assertion returned to SP-B. Such DS-A EPR is extracted from
145 the SAML token provided by IdP-A.

146 2.2 Access to Identity-enabled Web Services

147 Once SP-B has obtained a valid SSO token for Albert (containing references to, at least,
148 DS-B, but maybe also to DS-A), SP-B tries to discover and access some web services
149 exposing resources belonging to Albert (e.g., profile information for service
150 personalization). These web service providers are located in Albert's CoT (CoT-A,
151 exclusively, not in CoT-B).

152 2.2.1 Web Services Invocation Using DS Proxying

153 The figure below depicts this scenario.



154

155 **Figure 2: Inter-CoT (Inter-federation) Access to Id-based web services via DS**
156 **Proxying**

157

- 158 1 SP-B, acting as WSC-B, wants to invoke an identity service of Albert (ultimately
159 provided by WSP-A, but SP-B doesn't know about this, yet). It starts by sending
160 a discovery request to DS-B (the CoT agreements establish that this bootstrapping
161 information is always present in the SSO token). Since DS-B is the natural
162 member of CoT of SP-B, a firewall hole will exist.
163
- 164 2 DS-B detects that Albert does not belong to its CoT, but to another CoT, and
165 proxies the discovery request to DS-A.
- 166 DS-B adds a new field to the discovery request indicating that this is a proxied
167 request from WSC-B. DS-A can then make the appropriate credential/access
168 decisions based upon that info.
- 169 Note that this indication is not standard and would require to be specified as an
170 extension of the DS Query operation (a new element inside the Query element,
171 part of the RequestedService element).
- 172 How does DS-B know that it is supposed to use DS-A, and how it is to access DS-
173 A? Several possibilities exist here. The first one corresponds to the "official"
174 recommendation of the standard. The rest represent a non-exhaustive enumeration
175 of possible examples, and are provided for informational purposes, only:
- 176 a Due to previous business agreements, DS-B is aware of the information
177 necessary to query the DS of the users of CoT-A (DS-A's EPR preconfigured
178 upon set up).
 - 179 b IdP-B, when it consumed the assertion from IdP-A, stashed the DS-A
180 bootstrap from IdP-A somewhere where DS-B can find it. This, however,
181 requires that DS-B caches such information for each of the users of CoT-A
182 accessing services of CoT-B.
 - 183 c DS-A reference (EPR) was included in the SSO token provided to SP-B as
184 part of DS-B bootstrap info (e.g., in an AttributeStatement of the SAML token
185 to be presented to DS-B). SP-B includes such a token in its request to DS-B,
186 and DS-B is able to extract such DS-A information from the token. This
187 alternative has the advantage that it does not require DS-B to cache DS-A
188 information for each of the users of CoT-A.
- 189 3 DS-A issues WSP-A EPR which includes necessary security token(s) for access to
190 WSP-A by WSC-B, and returns that to DS-B. Note that the SubjectConfirmation
191 element of such tokens (assuming SAML tokens) should be set to WSC-B/SP-B,
192 rather than DS-B, as would normally be the case.
- 193 A firewall hole is needed between DS-B and DS-A. This is feasible because there
194 is only one DS in CoT-B, and often DS-B and IdP-B are the same machine so the
195 hole may already exist to facilitate IdP proxying. There is no need to open a hole
196 between WSC-B/SP-B and DS-A.
- 197 4 DS-B response to WSC-B/SP-B.
- 198 5 WSC-B/SP-B calls WSP-A presenting the token provided by DS-B.

199 WSP-A validates the token (assuming SAML token) according to the processing
200 guidelines in [[SAMLCore2](#)], i.e., validation of SubjectConfirmation element,
201 validation of signature in the token as signed by DS-A (who is a natural CoT
202 partner of WSP-A), etc.

203 Regarding validation of the SubjectConfirmation element, this is an
204 implementation-specific detail which can be materialized by means of multiple
205 mechanisms, but, in general, all of them are based on ensuring that WSC-B's
206 certificates matches the presenter of the token, for instance by:

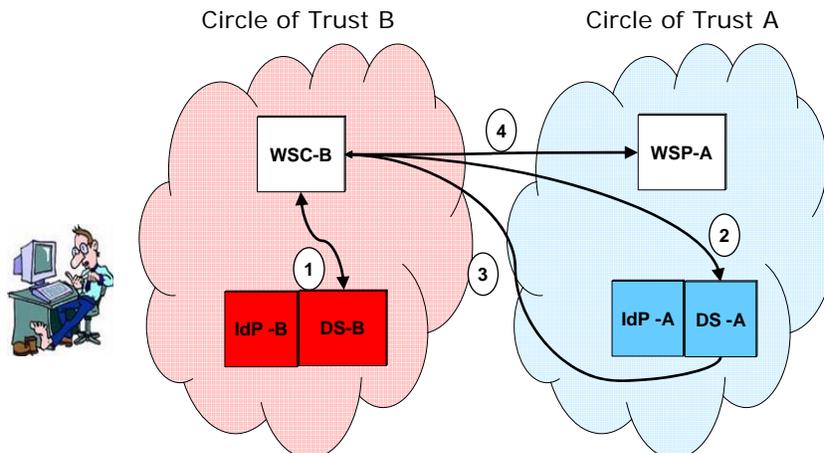
- 207 a Verifying that the CommonName in the WSC-B/SP-B's TLS certificate is the
208 proper prefix of WSC-B/SP-B's Provider ID, as reflected in the intended
209 SubjectConfirmation field of the SAML token.
- 210 b Verifying that the CommonName in the WSC-B/SP-B's signing certificate
211 (assuming the request was signed) is proper prefix of WSC-B/SP-B's
212 ProviderID, as reflected in the intended SubjectConfirmation field of the
213 SAML token.

214 For the signature and certificate checks in (a) and (b) to work, the certificates have
215 to be issued by some CA which WSP-A is willing to trust. (Presumably, this CA
216 can be trusted to enforce required policies.)

217 **2.2.2 Inter-Federation (Inter-CoT) Discovery**

218 In this case, WSC-B obtains a direct reference to DS-A, and is therefore able to directly
219 query such entity. DS-B works as a trust broker, in this case, by generating a token that
220 will be used to bridge trust between WSC-B and DS-A. Note that such token could be
221 issued with different possible subject confirmation mechanisms (e.g., it could be a bearer
222 token, a HoK token, etc). This depends on the deployment scenario, and the degree of
223 trust being required by the different entities. In a “degenerated” model, WSC-B could not
224 need to present any security token in order to access DS-A (being trust-established by
225 some other mechanisms, such as by extending the “Authentication” trust level, as
226 reflected in [TrustModelGuidelines]: WSC-B simply proves to be the owner of a
227 certificate issued by a Certification Authority that DS-A is willing to trust, directly or
228 indirectly, together with providing Albert’s handle in DS-A.

229 The following diagram reflects the associated message flow:



230

231 **Figure 3: Inter-CoT Access to Id-Based Web Services via Inter-CoT Discovery**
232

- 233 1 SP-B, acting as a WSC, queries DS-B asking for Albert's identity service. As a
234 result of this DS query, it obtains all the information and associated
235 credentials/tokens (EPR) to contact, directly, DS-A with IDP-B/DS-B acting as a
236 Trusted Third Party helping to authenticate SP-B/WSC-B towards DS-A: See the
237 description on different models, above. As reflected in the descriptive text of this
238 section, such credential could be:
- 239 a a SAML HoK token,
 - 240 b a bearer token (SAML or otherwise),
 - 241 c no security credential but rather an identity token conveying Albert's handle
242 in DS-A ("degenerated" model), in case the trust between DS-A and WSC-B
243 could be established in some other way, as mentioned above.

244

245 Note that the DS-A EPR information could also be obtained as a result of the SSO
246 operation (directly returned by IdP-B/DS-B, according to CoT-B bylaws applying
247 to users belonging to CoT-A), and therefore this step would not be needed.

- 248 2 SP-B/WSC-B will directly contact DS-A, and authenticate itself through any of
249 the authentication mechanisms defined in the Liberty ID-WSF specifications.
250 This will also depend on the type of token generated by DS-B; for instance, by
251 proving possession of the key reflected in the SAML HoK assertion signed by
252 IDP-B/DS-B, in case (1.a) above.

253 DS-A validates the received <wsse:Security> header that authenticates SP-
254 B/WSC-B as it trusts IDP-B/DS-B, based on the Inter-CoT trust relationship that
255 exists between IDP-B/DS-B and IDP-A/DS-A.

256 Note that in the “degenerated” model, the validation of the identity token
257 conveying Albert’s handle in DS-A might not directly help to build trust between
258 WSC-B and WSP-A. Trust will instead be directly from already existing trust on
259 the PKI infrastructure.

260 3 DS-A, in turn, returns WSP-A’s EPR with associated credential to enable SP-
261 B/WSC-B to query WSP-A (no security token in “degenerated” model, simply
262 WSP-A contact information including Albert’s identity token for WSP-A).

263 4 SP-B/WSC-B directly contacts WSP-A, and can authenticate itself according to
264 the mechanism specified in WSP-A’s EPR, as provided by DS-A (for instance,
265 relying on the SAML HoK assertion signed by DS-A). A full description of this
266 peer-authentication functionality is provided in [[LibertySecMech20](#)].

267 WSP-A validates the received <wsse:Security> header that authenticates SP-
268 B/WSC as it trusts DS-A (both entities belonging to the same CoT).

269

270 **2.2.3 Direct Access**

271 As stated in previous sections, in this scenario, WSC-B would query DS-B, and would be
272 able to obtain a direct reference (together with the appropriate credentials) to access
273 WSP-A. This would be equivalent to saying that WSP-A is directly registered in DS-B,
274 which is therefore factually-equivalent to belonging to CoT-A (business relationship
275 between DS-B and WSP-A, DS-B works as trust broker between WSC-B and WSP-A).

276 This scenario is, in practical terms, equivalent to the Intra-CoT scenario. Therefore, no
277 further description seems to be needed.

278 **2.3 Metadata Distribution in Inter-CoT Scenarios**

279 Interoperability in federated scenarios typically requires agreements between system
280 entities regarding identifiers, binding support and endpoints, certificates and keys, and so
281 forth. In these types of scenarios, this information is usually described as metadata
282 information, and it becomes even more relevant in Inter-CoT environments. Even if the
283 different network entities will have commonly shared this sort of information with the
284 members of its own CoT, for interoperability purposes, however, it seems necessary that
285 all or at least some part of such metadata information is also made available to partners of
286 another CoT with whom there is no *a priori* business relationship, but one could be
287 established *on the fly*. In practice, there are several potential ways of distributing such
288 information, let’s name a few for informational purposes:

289 a **Push from Central Authority:** A central authority (perhaps the DS/IdP
290 operator) pushes the authorized metadata to the members of its own CoT.

- 291 This could be by means of LDAP replication, synchronizing flat files³ with
292 the metadata in XML format (as standardized by the OASIS SSTC), or some
293 other types of enterprise synchronization procedures.
- 294 b **Pull from central authority:** This is very similar to the previously described
295 mechanisms (Push) and much of the database backend standardization
296 discussion applies.
- 297 c **Well-Known-Location** (WKL, as defined in [[SAMLMeta2](#)], Section 4.1
298 "Publication and Resolution via Well-Known Location") **plus PKI:**
299 Ubiquitous use of a Well-Known-Location to get metadata and then use PKI
300 to trust it.
- 301 d **Well-Known-Location plus central authority distribution of trusted**
302 **ProviderIDs:** Ubiquitous use of a well-known-location to get metadata and
303 then use central authority to distribute list of trusted ProviderIDs (push or
304 pull).
- 305 The main advantage of this approach is that the trust list is very simple so
306 even junior system administrators are likely to get it right. Ideally, the format
307 of this list should be standardized (one proposal would be: first line:
308 "issuerprovid:issuenum:expiry:futexp," followed by ProviderIDs of
309 members of the CoT, one per line, separated by Unix newline (0x0a)).
310 However, given the simplicity of this approach, even a non-standard format is
311 unlikely to cause any problems.
- 312 The main disadvantage of this approach is that the well-known-location
313 approach is not supported by many vendors (or, at least, as part of the default
314 product configuration).
- 315 e **Well-Known-Location for metadata, OCSP for trust:** Ubiquitous use of
316 WKL to get metadata and then use OCSP [[RFC2560](#)] to check trust from
317 central authority.

² For instance, by making use of tools such as "rsync," see <http://rsync.samba.org/>

318 **3 Conclusion**

319 In summary, access to identity-based web services in scenarios where there is no direct
320 business relationship between the service requestor and the service provider can be
321 achieved by leveraging a previously-existing business relationship established between
322 some “distinguished” members of the CoT (for instance, the entities operating the IdP-
323 DS).

324 As an example, this seems to be of special applicability in roaming scenarios typical of
325 the telecommunication industry, by leveraging (and possibly extending) the already-
326 existing agreements among the different operators. It can also be of applicability to other
327 industries, such as the eHealth or eGovernment sectors.

328 To conclude, all the scenarios described in this paper are fully interoperable and can be
329 achieved by direct applicability of the Liberty Alliance’s specification set, with the
330 following exception:

- 331 • Section 2.2.1(DS Proxying), extension of the RequestedService element inside the DS
332 Query operation is needed in order to signal to DS-A that the entity to be presenting
333 the DS-A-generated token (WSC-B) is different from the DS requestor (DS-B).

334

335 Some other enhancement proposals (although not explicitly required for interoperability):

- 336 • Inter-CoT Metadata distribution, define the format of the file containing the list of
337 trusted ProviderIds, to be distributed by the central authority of each CoT.

338

339 Even if these specific topics are not directly addressed by the standard, it seems rather
340 immediate to handle them as proprietary extensions in specific deployments.

341

342 4 References

343 [LibertyGlossary] Hodges, Jeff, eds. "Liberty Technical Glossary," Version v2.0, Liberty
344 Alliance Project (30 July, 2006).

345 [http://www.projectliberty.org/liberty/content/download/868/6180/file/liberty-glossary-
346 v2.0.pdf](http://www.projectliberty.org/liberty/content/download/868/6180/file/liberty-glossary-
346 v2.0.pdf)

347
348 [LibertySecMech20]. Hirsch, Frederick, eds. "Liberty ID-WSF Security Mechanisms
349 Core," Version 2.0 errata v1.0, Liberty Alliance Project (09 July, 2007).,

350 [http://www.projectliberty.org/liberty/content/download/893/6255/file/liberty-idwsf-
351 security-mechanisms-core-2.0-errata-v1.0.pdf](http://www.projectliberty.org/liberty/content/download/893/6255/file/liberty-idwsf-
351 security-mechanisms-core-2.0-errata-v1.0.pdf)

352
353 [TrustModelGuidelines] OASIS "Trust Models Guidelines," John Linn (RSA) et al,
354 [http://www.oasis-open.org/committees/download.php/6158/sstc-saml-trustmodels-2.0-
355 draft-01.pdf](http://www.oasis-open.org/committees/download.php/6158/sstc-saml-trustmodels-2.0-
355 draft-01.pdf)

356
357 [SAMLCore2] Cantor, Scott, Kemp, John, Philpott, Rob, Maler, Eve, eds. (15 March
358 2005). "Assertions and Protocol for the OASIS Security Assertion Markup Language
359 (SAML) V2.0," SAML V2.0, OASIS Standard, Organization for the Advancement of
360 Structured Information Standards,

361 <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

362
363 [RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C., eds. (June
364 1999). "X.509 Public Key Infrastructure: Online Certificate Status Protocol - OCSP,"
365 RFC 2560, The Internet Engineering Task Force, <http://tools.ietf.org/html/rfc2560>

366
367 [SAMLMeta2], Cantor, Scott, Moreh, Jahan, Philpott, Rob, Maler, Eve, eds. (15 March
368 2005). "Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0,"
369 SAML V2.0, OASIS Standard, Organization for the Advancement of Structured
370 Information Standards

371 <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>

372