

# 1 SAML Conformance Program Specification

## 3 This version:

5 File : sstc-draft-conformance-spec-006.doc

6 Date : November 2, 2001

---

---

## 8 Authors

9 o Krishna Sankar [ksankar@cisco.com]

10 o Robert Griffin [Robert.Griffin@entrust.com]

---

---

## 11 Contributors

12 o Lynne Rosenthal

13 o Mark Skall

14 o Marc Chanliau

15 o Charles Norwood

16 o Tony Palmer

17 o Mark O'Neill

18 o Mike Myers

19 o Hal Lockhart

---

---

## 20 Abstract

21 This document describes the program and technical requirements for the SAML  
22 conformance system.

## 24 Referenced Documents

25  
26 1. <http://www.itl.nist.gov/div897/ctg/conformProject.shtml>

27 2. <http://lists.oasis-open.org/archives/conformance/200104/msg00000.html>

28 3. XML Protocol specification conformance issues

## 29 **Notational Conventions**

30 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",  
31 "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this  
32 document are to be interpreted as described in Key Words for Use in  
33 RFC's to Indicate Requirement Levels (RFC 2119).

## 34 **Status of this Document**

35 This document represents work in progress upon which no reliance should  
36 be made.

## 37 **Document Version History**

- 38 o Version 0.001: Initial version
- 39 o Version 0.002: Strawman profiles, test cases and process
- 40 o Version 0.003: Revisions from 1-June-2001 review; added example of  
41 test case
- 42 o Version 0.004: Revisions from 18-June-2001 review; modified to  
43 reflect conformance clause
- 44 o Version 0.005: Additions to test cases
- 45 o Version 0.006: Additions to test cases

46  
47

47 **Table of Contents**

48 1 Scope of the Conformance Program..... 4

49 2 Conformance Clause..... 4

50 3 Conformance Process..... 4

51 4 Technical requirements for SAML Conformance..... 7

52 4.1 Conformance Profiles and Levels..... 7

53 4.1.1 Profile 1: Interoperable Authentication Capability.... 7

54 4.1.2 Profile 2: Interoperable PEP/PDP**Error! Bookmark not defined.**

55 4.1.3 Profile 3: Interoperable PEP **Error! Bookmark not defined.**

56 4.1.4 Profile 4: Interoperable PDP **Error! Bookmark not defined.**

57 4.1.5 Profile 5: Interoperable Authorization Authoriy... **Error!**

58 **Bookmark not defined.**

59 4.2 Test Cases..... 11

60 4.2.1 Test Group 1 - Interoperable Authentication Capability Only

61 11

62 4.2.2 Test Group 2 - Interoperable PEP/PDP..... 20

63 4.3 Test Suite..... 20

64 4.3.1 Reference Architecture..... 21

65 4.3.2 Infrastructure..... 21

66 4.3.3 Using the Test Suite..... 21

67 4.3.4 Test result tabulation and reporting..... 21

68 4.4 Certification Process..... 21

69 4.4.1 Certification program considerations. **Error! Bookmark not**

70 **defined.**

71 4.4.2 21

72 5 Conformance services..... 21

73 5.1.1 Testing Service..... 21

74 6 To Do..... **Error! Bookmark not defined.**

75

76

77

77 **1 Scope of the Conformance Program**

78

79 SAML deals with a rich set of functionalities ranging from authentication  
80 assertions to session assertions to assertions for policy enforcement. Not  
81 all software might choose to implement all the SAML specifications. In  
82 order to achieve compatibility and interoperability, applications and  
83 software need to be certified for conformance in a uniform manner. The SAML  
84 conformance effort aims at fulfilling this opportunity.

85 The deliverables of the SAML conformance effort include:

86

87     ▪ Conformance clause in the SAML Specification, defining at a high-level  
88        what conformance means for the SAML standard

89     ▪ Conformance Program specification (this document)

90     ▪ Conformance Test Suite. This is a set of test programs, result files and  
91        report generation tools that can be used by vendors of SAML-compliant  
92        software, buyers interested in confirming SAML compliance of software,  
93        and testing labs running conformance tests on behalf of vendors or  
94        buyers.

95 Section 3 of this document deals with defining and specifying the process  
96 by which conformance to the SAML specification can be demonstrated and  
97 certified. Section 4 elaborates the actual technical requirements which  
98 constitute conformance; this includes both the levels of conformance that  
99 may be demonstrated, the requirements for each of those levels of  
100 conformance, the processes by which conformance can be established, and the  
101 policies and procedures relating to those processes. Section 5 defines the  
102 services which are available to assist in establishing conformance.

103 **2 Conformance Clause**

104 Please refer to the SAML specification for the conformance clause.

105

106 **3 Conformance Process**

107 The goal of the SAML effort is to obtain implementations of the standard  
108 that correctly perform the functionality specified in the standard.  
109 Conformance testing helps to achieve correct implementation. It provides a  
110 way to determine whether or not these implementations conform to the  
111 standard. It provides software developers and users assurance and  
112 confidence that the conforming product behaves as expected, performs  
113 functions in a known manner, or possesses a prescribed interface or format.

114 The SAML Technical Committee is responsible for generating the materials  
115 that allow vendors, customers, and third parties to evaluate software for  
116 SAML conformance. These materials include:

- 117           ▪ Documentation describing test cases, linked to use cases and  
118           requirements
  - 119           ▪ Test suite, based on those test cases, that can be run against an  
120           implementation to demonstrate any of the several levels/profiles of  
121           conformance defined in the conformance clause of the SAML  
122           specification
  - 123           ▪ Documentation describing how to run the test suite, interpret the  
124           results, and resolve disputes regarding the results of the tests
- 125       The SAML Technical Committee is not, however, responsible for testing of  
126       particular implementations.

### 127    3.1 Conformance Testing, Validation and Certification

128       In describing the SAML Conformance Program, it is helpful to distinguish  
129       among conformance testing, validation and certification. **Conformance**  
130       **testing** is the running of (some or all) tests within the SAML Conformance  
131       Test Suite. Conformance testing performed by implementers early on in the  
132       development process can find and correct their errors before the software  
133       reaches the marketplace, without necessarily being part of either a  
134       validation or certification process. **Validation** is the process of testing  
135       implementations for conformance. The validation process consists of the  
136       steps necessary to perform the conformance testing by using an official  
137       test suite in a prescribed manner. **Certification** is the acknowledgment  
138       that a validation has been completed and the criteria established by the  
139       certifying organization for issuing a certificate, has been met. When  
140       validation is coupled with certification, successful completion of  
141       conformance testing results in the issuance of a certificate (or brand)  
142       indicating that the implementation conforms to the appropriate  
143       specification. It is important to note that certification cannot exist  
144       without validation, but validation can exist without certification.

145       The SAML Conformance Program provides for both validation alone and  
146       certification (with validation) as options in demonstrating conformance to  
147       the SAML standard:

148

- 149           ▪ **Validation** may be done without certification for such purposes as  
150           self-test. An implementor who has validated SAML conformance by means  
151           of self-test cannot legitimately use the term "certified for SAML  
152           conformance". However, an implementor may claim to have "validated  
153           for SAML conformance" at a given conformance partition and level  
154           after having run successfully all tests required for that partition  
155           and level.
- 156           ▪ **Certification** requires validation by a third-party rather than  
157           through self-test. A certifying authority identified by the SAML TC  
158           as responsible for issuing certification of SAML conformance.

159

160       Note that both validation and certification subsume conformance testing.

161 Validation (most likely, though not necessarily by self-test) is most  
162 important for implementors developing SAML-compliant software who want to  
163 ensure conformance to the standard prior to submitting software to testing  
164 by a third party. Validation may also be used by vendors or customers as a  
165 form of self-certification; the adequacy of self-certification will depend  
166 on the purpose for which the software is intended, the degree of  
167 interoperability that will be required (the larger the number of  
168 implementations that it must interoperate with, the greater the value of  
169 third-party testing) and the degree of formal certification required by  
170 customers of the software.

171

172 Certification differs from validation in the formal issuance of a  
173 certificate of conformity by a recognized authority. The validation  
174 performed prior to certification employs the same materials as self-test;  
175 however, the certification authority requires that the validation be  
176 performed by a testing lab which it has reviewed for adherence to the SAML  
177 conformance policies and procedures. (For description of the certification  
178 process, see "CertificationModel.doc".)

179 **NOTE:** For SAML V1.0, there is no requirement that a given implementation or  
180 application be certified as conforming to the SAML standard. In many cases,  
181 a statement that validation has been performed by the vendor will be  
182 sufficient for their customers. Until and if the certification process is  
183 in place, vendor declaration of validation will be the only means of  
184 demonstrating conformance.

## 185 3.2 Implementation and Application Conformance

186 SAML Conformance is applicable to:

- 187 - Implementations of SAML assertions, protocols and bindings. These  
188 could be in the form of toolkits, products incorporating SAML  
189 components, or reference implementations that demonstrate the use of  
190 SAML components.
- 191 - Applications that consume SAML assertions or that execute on SAML  
192 implementations (for example, using a SAML toolkit to support multi-  
193 domain single-signon)

194 A conforming **implementation** shall meet all the following criteria:

- 195 (1) The implementation shall support all the required interfaces defined  
196 within this standard for a given profile and level. These interfaces  
197 shall support the functional behavior described in the standard.
- 198 (2) An implementation may provide additional or enhanced features or  
199 functionality not required by the SAML Specification. These non-standard  
200 extensions shall not alter the specified behavior of interfaces or  
201 functionality defined in the specification
- 202 (3) The implementation may provide additional or enhanced facilities not  
203 required by this standard. These non-standard extensions shall not  
204 alter the specified behavior of interfaces defined in this standard.  
205 They may add additional behaviors. In these circumstances, the  
206 implementation shall provide a mechanism whereby a SAML conforming  
207 application shall be recognized as such, and be executed in an  
208 environment that supports the functional behavior defined in this  
209 standard.

210 A conforming **application** shall meet all the following criteria:

- 211 (1) The application shall be able to execute on any conforming  
212 implementation.
- 213 (2) If an application requires a particular feature set that is not  
214 available on a specific implementation, then the application must act  
215 within the bounds of the SAML specification even though that means that  
216 the application may not perform any useful function. Specifically, the  
217 application shall do no harm, and shall correctly return resources and  
218 vacate memory upon discovery that a required element is not present.  
219

## 220 4 Technical requirements for SAML Conformance

221 This section defines the criteria which apply to various partitions and levels  
222 of conformance.

### 223 4.1 Conformance Partitions and Levels

224 For both validation and certification, conformance may be achieved in terms of  
225 a single or multiple partitions. A **partition** defines a set of SAML  
226 capabilities, with a corresponding set of test cases, for which an  
227 implementation or application can declare conformance. Within a given  
228 partition, an implementation may achieve conformance at any of several levels.

229 Note that the term "profile" is used in a corresponding sense in other  
230 conformance programs, as well as in ISO/IEC 8632. We are using the term  
231 "partition" rather than profile to avoid confusion regarding the meaning of  
232 profile as it is used elsewhere in SAML.

233 Partitions provide a means to:

- 234 a) improve interoperability between implementations by inhibiting the proliferation of private  
235 subsets of SAML
- 236 b) provide a foundation for testing and promote uniformity of conformance tests;
- 237 c) enhance the availability of consistent implementations of profiles.

238 A partition defines the options, elements, and parameters necessary to  
239 accomplish a particular function and maximize the probability of interchange  
240 between systems implementing the partition and the SAML standard as a whole.

241 The SAML partitions are:

- 242     ▪ **Authentication Authority.** This partition contains all SAML  
243     functionality related to creation, propagation and consumption of  
244     authentication assertions and authentication assertion artefacts.
- 245     ▪ **Attribute Authority.** This partition includes all SAML functionality  
246     related to the creation, propagation and consumption of attribute  
247     assertions and attribute assertion artefacts.
- 248     ▪ **Authorization Authority.** This partition includes all SAML functionality  
249     related to the creation, propagation and consumption of authorization  
250     decision assertions and authorization decision artefacts.
- 251     ▪ **Policy Decision Authority.** This partition is a subset of the  
252     Authorization Authority partition, supporting the producer role for  
253     authorization decision assertions.

254       ▪ **Policy Enforcement Authority.** This partition is a subset of the  
255       Authorization Authority partition, supporting the consumer role for  
256       authorization decision assertions.

#### 257   **4.1.1 Authentication Authority Partition**

258   This partition includes all SAML functionality related to the creation and  
259   propagation of authentication assertions and authentication assertion  
260   references. It is appropriate to authentication systems that produce and  
261   consume authentication assertions, such as to achieve single-signon across  
262   internet domains, application servers, and other environments. An  
263   implementation conforming only to this partition would not need to implement  
264   any assertion other than authentication assertions.

265   Conformance to this partition can be claimed at several levels:

266   (1) Any implementation claiming conformance to this partition must implement  
267   both the producer and the consumer roles for the HTTP authentication query and  
268   response protocol binding. Such a claim shall be expressed as follows:  
269   "[implementation or application] conforms to required functionality for the  
270   authentication authority partition".

271   (2) Authentication authority conformance may also be claimed for other  
272   bindings and profiles supported in SAML V1.0.

273       ▪ Conformance to the SOAP protocol binding shall be expressed as  
274       "[implementation or application] conforms to the SAML V1.0 SOAP protocol  
275       binding for the authentication authority partition"

276       ▪ Conformance to the web browser profile shall be expressed as  
277       "[implementation or application] conforms to the SAML V1.0 SOAP protocol  
278       binding for the authentication authority partition"

279   Conformance to this partition requires both kinds of roles (producer and  
280   consumer) in order to allow for nesting of assertions.

281   Test cases for this partition relate to validity of assertions produced and  
282   consumed, and to validity of request/response messages.

283   (**Issue:** Should we also allow for the partition to implement only returning an  
284   authentication assertion in an HTTP response, while binding a request/response  
285   for an authentication assertion on SOAP is a different level?)

#### 286   **4.1.2 Attribute Authority Partition**

287   This partition includes all SAML functionality related to the creation and  
288   propagation of attribute assertions and their corresponding references.  
289   Conformance to just this partition is appropriate to an authorization  
290   subsystem that provides privilege information for consumption by other  
291   implementations or applications.

292   Conformance to this partition can be claimed at several levels:

293   (1) Any implementation claiming conformance to this partition must implement  
294   both the producer and the consumer roles for the HTTP attribute assertion  
295   query and response protocol binding. Such a claim shall be expressed as  
296   follows: "[implementation or application] conforms to required functionality  
297   for the attribute authority partition".

298   (2) Authorization authority conformance may also be claimed for other bindings  
299   and profiles supported in SAML V1.0.



300       ▪ Conformance to the SOAP protocol binding shall be expressed as  
301        "[implementation or application] conforms to the SAML V1.0 SOAP protocol  
302        binding for the attribute authority partition"  
  
303       ▪ Conformance to the web browser profile shall be expressed as  
304        "[implementation or application] conforms to the SAML V1.0 SOAP protocol  
305        binding for the attribute authority partition"  
  
306       Conformance to this partition must include both consumer and producer roles to  
307       allow for nesting of assertions.  
  
308       Test cases for this partition relate to validity of assertions produced and  
309       consumed, and to validity of request/response messages.

#### 310       **4.1.3 Authorization Authority Partition**

311       This partition includes all SAML functionality related to the creation and  
312       propagation of authorization assertions and authorization decision assertions  
313       and their corresponding references. Conformance to just this partition is  
314       appropriate to an authorization subsystem that provide privilege information  
315       for consumption by other implementations or applications.

316       Conformance to this partition can be claimed at several levels:

- 317       (1) Any implementation claiming conformance to this partition must implement  
318       both the producer and the consumer roles for the HTTP authorization decision  
319       query and response protocol binding. Such a claim shall be expressed as  
320       follows: "[implementation or application] conforms to required functionality  
321       for the authorization authority partition".  
  
322       (2) Authorization authority conformance may also be claimed for other bindings  
323       and profiles supported in SAML V1.0.

- 324       ▪ Conformance to the SOAP protocol binding shall be expressed as  
325        "[implementation or application] conforms to the SAML V1.0 SOAP protocol  
326        binding for the authorization authority partition"  
  
327       ▪ Conformance to the web browser profile shall be expressed as  
328        "[implementation or application] conforms to the SAML V1.0 SOAP protocol  
329        binding for the authorization authority partition"

330       Conformance to this partition must include both consumer and producer roles  
331       for authorization decision assertions (to allow for nesting of assertions).

332       In addition, the conformance claim for an implementation or application must  
333       state whether consumption of authentication assertions and attribute  
334       assertions are supported by the authorization authority:

- 335       ▪ Support for consumption of authentication assertions shall be expressed  
336        as "[implementation or application] authorization authority conforms to the  
337        SAML V1.0 authentication assertion schema."  
  
338       ▪ Support for consumption of attribute assertions shall be expressed as  
339        "[implementation or application] authorization authority conforms to the  
340        SAML V1.0 attribute assertion schema."

341       Test cases for this partition relate to validity of assertions produced and  
342       consumed, and to validity of request/response messages.

343 **4.1.4 Policy Decision Authority Partition**

344 This partition is a subset of the authorization authority partition,  
345 supporting only the producer role for the authorization authority. Includes  
346 all SAML functionality related to the Policy Decision Point in a SAML  
347 implementation or application.

348 Conformance to this partition can be claimed at several levels:

349 (1) Any implementation or application claiming conformance to this partition  
350 must implement the producer role for the HTTP authorization decision query and  
351 response protocol binding for the authorization decision assertion. Such a  
352 claim shall be expressed as follows: "[implementation or application] conforms  
353 to required functionality for the policy decision authority partition".

354 (2) Authorization authority conformance may also be claimed for other bindings  
355 and profiles supported in SAML V1.0.

356     ▪ Conformance to the SOAP protocol binding shall be expressed as  
357       "[implementation or application] conforms to the SAML V1.0 SOAP protocol  
358       binding for the policy decision authority partition"

359     ▪ Conformance to the web browser profile shall be expressed as  
360       "[implementation or application] conforms to the SAML V1.0 SOAP protocol  
361       binding for the policy decision authority partition"

362 Conformance to this partition includes only the producer role for  
363 authorization decision assertions; nesting of assertions is not included in  
364 this partition.

365 In addition, the conformance claim for an implementation or application must  
366 state whether consumption of authentication assertions and attribute  
367 assertions are supported by the policy decision authority:

368     ▪ Support for consumption of authentication assertions shall be expressed  
369       as "[implementation or application] policy decision authority conforms  
370       to the SAML V1.0 authentication assertion schema."

371     ▪ Support for consumption of attribute assertions shall be expressed as  
372       "[implementation or application] policy decision authority conforms to  
373       the SAML V1.0 attribute assertion schema."

374 Test cases for relate to validity of assertions produced and consumed, and to  
375 validity of request/response messages.

376 **4.1.5 Policy Enforcement Authority Partition**

377 This partition is a subset of the authorization authority partition,  
378 supporting only the consumer role for the authorization authority. It includes  
379 all SAML functionality related to the Policy Enforcement Point in a SAML  
380 implementation or application.

381 Conformance to this partition can be claimed at several levels:

382 (1) Any implementation or application claiming conformance to this partition  
383 must implement the consumer role for the HTTP authorization decision query and  
384 response protocol binding for the authorization decision assertion. Such a  
385 claim shall be expressed as follows: "[implementation or application] conforms  
386 to required functionality for the policy enforcement authority partition".

387 (2) Authorization authority conformance may also be claimed for other bindings  
388 and profiles supported in SAML V1.0.

389     ▪ Conformance to the SOAP protocol binding shall be expressed as  
390       "[implementation or application] conforms to the SAML V1.0 SOAP protocol  
391       binding for the policy enforcement authority partition"

392       ▪ Conformance to the web browser profile shall be expressed as  
393        "[implementation or application] conforms to the SAML V1.0 SOAP protocol  
394        binding for the policy enforcement authority partition"

395 Conformance to this partition includes only the consumer role for  
396 authorization decision assertions.

397 In addition, the conformance claim for an implementation or application must  
398 state whether consumption of authentication assertions and attribute  
399 assertions are supported by the policy enforcement authority:

400       ▪ Support for consumption of authentication assertions shall be expressed  
401        as "[implementation or application] policy enforcement authority  
402        conforms to the SAML V1.0 authentication assertion schema."

403       ▪ Support for consumption of attribute assertions shall be expressed as  
404        "[implementation or application] policy enforcement authority conforms  
405        to the SAML V1.0 attribute assertion schema."

406 Test cases for relate to validity of assertions consumed, and to validity of  
407 request/response messages.

408

## 409   **4.2 Test Cases for SAML V1.0**

410 A test suite, which is the combination of test cases and test documentation,  
411 is used to check whether an implementation or application satisfies the  
412 requirements in the standard. The test cases, implemented by a test tool or a  
413 set of files (i.e., data, programs, scripts, or instructions for manual  
414 action) checks each requirement in the specification to determine whether the  
415 results produced by the implementation or application match the expected  
416 results, as defined by the specification.

417 Each test case includes:

418       ▪ A description of the test purpose (i.e., what is being tested - the  
419        conditions, requirements, or capabilities which are to be addressed by a  
420        particular test

421       ▪ The pass/fail criteria,

422       ▪ A reference to the requirement or section in the standard from which the  
423        test case is derived (i.e., traceability back to the specification.

424 The test documentation describes how the testing is to be done and the  
425 directions for the tester to follow. Additionally, the documentation should  
426 be detailed enough so that testing of a given implementation can be repeated  
427 with no change in test results.

428 Conformance testing is black box testing to test the functionality of an  
429 implementation. This means that the internal structure or the source code of  
430 a candidate implementation is not available to the tester. However, content  
431 and format of received or returned messages can be inspected as part of the  
432 determination of conformance.

433 The test suite should be platform independent, non-biased, objective tests.  
434 Generally a conformance test suite is a collection of combinations of legal  
435 and illegal inputs to the implementation being tested, together with a  
436 corresponding collection of expected results. Only the requirements specified  
437 in the standard are testable. A test suite should not check any  
438 implementation properties that are not described by the standard or set of  
439 standards. A test suite cannot require features that are optional in a  
440 standard, but if such features are present, a test suite could include tests  
441 for those features. A test suite does not assess the performance of an  
442 implementation unless performance requirements are specified in the  
443 specification, although implementation dependencies or machine dependencies  
444 may be demonstrated through the execution of the test cases.

445 The results of conformance testing apply only to the implementation and  
446 environment for which the tests are run. Test suites may be provided as a  
447 web-based system executed on a remote server, downloadable files for local  
448 execution, or a combination of remote and local access and execution. The  
449 method for providing and delivering the test suite depends on what is being  
450 tested as well as the objective for test suite use - that is, providing self-  
451 test capability or formal certification testing.

#### 452 **4.2.1 Test Group 1 - Authentication Authority Partition**

453 The test cases in this test group check for conformance to the Authentication  
454 Authority partition at both required and optional levels. The test cases  
455 derive from the following use cases:

- 456     ▪ Use Case 1 "Single Sign-on", addressing requirements **R-AUTHN**, **R-**  
457       **MULTIDOMAIN** and **R-REFERENCE**.
- 458     ▪ Scenario 1-1 "Single sign-on, pull model"
- 459     ▪ Scenario 1-3 "Single sign-on, third-party security service" (exclusive  
460       of authorization-related functionality).

461 An implementation or application claiming conformance must successfully  
462 complete the following tests, related to support for the required HTTP  
463 request/response protocol binding:

- 464     ▪ Test 1-1
- 465     ▪ Test 1-2
- 466     ▪ Test 1-3

467 An implementation or application claiming conformance to the SOAP protocol  
468 binding must successfully completed these tests in addition to the required  
469 tests.

- 470     ▪ Test 1-4
- 471     ▪ Test 1-5
- 472     ▪ Test 1-6

473 An implementation or application claiming conformance to the Web Browser  
474 Profile must successfully completed these tests in addition to the required  
475 tests.

- 476     ▪ Test 1-7
- 477     ▪ Test 1-8
- 478     ▪ Test 1-9
- 479     ▪ Test 1-10

480 Note that the use of a valid authentication assertion request/response as part  
481 of a request for authorization is included in Test Groups 3, 4 and 5 (Sections  
482 4.2.3, 4.2.4 and 4.2.5).

483 **Test Case 1-1: HTTP Protocol Binding: Valid Authentication Assertion Produced**  
484 **in Response to Valid Authentication Query. REQUIRED**

485 *Description:* This test case submits an HTTP message to an authentication  
486 authority containing authentication credentials and checks that the  
487 authentication authority return a valid authentication assertion.

488 *Pass/Fail Criteria:* Authentication assertion returned by implementation or  
489 application must contain all required information in the right sequence and  
490 format. Any optional information included (including conditions) must not  
491 compromise the validity of the required information.

492 *Reference:* **R-AUTHN**, and **R-MULTIDOMAIN**

493 *Implementation notes:* Test program implementing this test case establishes  
494 successful execution of the test case by inspection of the format of the  
495 returned assertion.

496

497 **Test Case 1-2: HTTP Protocol Binding: Valid Authentication Assertion Artefact**  
498 **Produced in Response to Valid Authentication Query. REQUIRED**

499 *Description:* This test case submits an HTTP message to an authentication  
500 authority containing authentication credentials and checks that the  
501 authentication authority returns a valid authentication assertion artefact.

502 *Pass/Fail Criteria:* Authentication assertion artefact returned by  
503 implementation or application must be contain all required information in the  
504 right sequence and format. Any optional information included (including  
505 conditions) must not compromise the validity of the required information.

506 *Reference:* **R-AUTHN**, and **R-MULTIDOMAIN**

507 *Implementation notes:* Test program implementing this test case establishes  
508 successful execution of the test case by inspection of the format of the  
509 returned assertion artefact.

510

511 **Test Case 1-3: HTTP Protocol Binding: Valid Authentication Assertion Artefact**  
512 **from Same Authority Consumed. REQUIRED**

513 *Description:* This test case submits a valid HTTP authentication artefact,  
514 generated as a result of an HTTP request/response protocol binding, to an  
515 authentication authority and confirms that the authentication assertion  
516 artefact has been properly consumed by inspecting the authentication assertion  
517 returned.

518 *Pass/Fail Criteria:* Authentication assertion returned by implementation or  
519 application must be contain all required information in the right sequence and  
520 format. Any optional information included (including conditions) must not  
521 compromise the validity of the required information.

522 *Reference:* **R-AUTHN**, and **R-MULTIDOMAIN**

523 *Implementation notes:* Test program implementing this test case establishes  
524 successful execution of the test case by inspection of the format of the  
525 returned assertion artefact.

526

527 **Test Case 1-4: SOAP Protocol Binding: Valid Authentication Assertion Produced**  
528 **in Response to Valid Authentication Query.**

529 *Description:* This test case submits a SOAP message to an authentication  
530 authority containing authentication credentials and checks that the  
531 authentication authority return a valid authentication assertion.

532 *Pass/Fail Criteria:* Authentication assertion returned by implementation or  
533 application must contain all required information in the right sequence and  
534 format. Any optional information included (including conditions) must not  
535 compromise the validity of the required information.

536 *Reference:* **R-AUTHN**, and **R-MULTIDOMAIN**

537 *Implementation notes:* Test program implementing this test case establishes  
538 successful execution of the test case by inspection of the format of the  
539 returned assertion.

540 **Test Case 1-5: SOAP Protocol Binding: Valid Authentication Assertion Artefact**  
541 **Produced in Response to Valid Authentication Query.**

542 *Description:* This test case submits a SOAP message to an authentication  
543 authority containing authentication credentials and checks that the  
544 authentication authority returns a valid authentication assertion artefact.

545 *Pass/Fail Criteria:* Authentication assertion artefact returned by  
546 implementation or application must be contain all required information in the  
547 right sequence and format. Any optional information included (including  
548 conditions) must not compromise the validity of the required information.

549 *Reference:* **R-AUTHN**, and **R-MULTIDOMAIN**

550 *Implementation notes:* Test program implementing this test case establishes  
551 successful execution of the test case by inspection of the format of the  
552 returned assertion artefact.

553

554 **Test Case 1-6: SOAP Protocol Binding: Valid Authentication Assertion Artefact**  
555 **from Same Authority Consumed.**

556 *Description:* This test case submits a valid SOAP authentication artefact,  
557 generated as a result of an SOAP request/response protocol binding, to an  
558 authentication authority and confirms that the authentication assertion  
559 artefact has been properly consumed by inspecting the authentication assertion  
560 returned.

561 *Pass/Fail Criteria:* Authentication assertion returned by implementation or  
562 application must be contain all required information in the right sequence and  
563 format. Any optional information included (including conditions) must not  
564 compromise the validity of the required information.

565 *Reference:* **R-AUTHN**, and **R-MULTIDOMAIN**

566 *Implementation notes:* Test program implementing this test case establishes  
567 successful execution of the test case by inspection of the format of the  
568 returned assertion.

569

570 **Test Case 1-7: SHTTP Web Browser Profile: Valid Authentication Assertion**  
571 **Produced in Response to Valid Authentication Query.**

572 *Description:* This test case submits an HTTP message to an authentication  
573 authority containing authentication credentials and checks that the  
574 authentication authority return a valid authentication assertion.

575 *Pass/Fail Criteria:* Authentication assertion returned by implementation or  
576 application must contain all required information in the right sequence and  
577 format. Any optional information included (including conditions) must not  
578 compromise the validity of the required information.

579 *Reference:* **R-AUTHN**, and **R-MULTIDOMAIN**

580 *Implementation notes:* Test program implementing this test case establishes  
581 successful execution of the test case by inspection of the format of the  
582 returned assertion.

583 **Test Case 1-8: HTTP Web Browser Profile: Valid Authentication Assertion**  
584 **Artefact Produced in Response to Valid Authentication Query.**

585 *Description:* This test case submits an HTTP message to an authentication  
586 authority containing authentication credentials and checks that the  
587 authentication authority returns a valid authentication assertion artefact.

588 *Pass/Fail Criteria:* Authentication assertion artefact returned by  
589 implementation or application must be contain all required information in the  
590 right sequence and format. Any optional information included (including  
591 conditions) must not compromise the validity of the required information.

592 *Reference:* **R-AUTHN**, and **R-MULTIDOMAIN**

593 *Implementation notes:* Test program implementing this test case establishes  
594 successful execution of the test case by inspection of the format of the  
595 returned assertion artefact.

596

597 **Test Case 1-9: HTTP Web Browser Profile: Valid Authentication Assertion**  
598 **Artefact from Same Authority Consumed.**

599 *Description:* This test case submits a valid authentication artefact, generated  
600 as a result of an HTTP message, to an authentication authority and confirms  
601 that the authentication assertion artefact has been properly consumed by  
602 inspecting the authentication assertion returned.

603 *Pass/Fail Criteria:* Authentication assertion returned by implementation or  
604 application must be contain all required information in the right sequence and  
605 format. Any optional information included (including conditions) must not  
606 compromise the validity of the required information.

607 *Reference:* **R-AUTHN**, and **R-MULTIDOMAIN**

608 *Implementation notes:* Test program implementing this test case establishes  
609 successful execution of the test case by inspection of the format of the  
610 returned assertion.

611

612 **Test Case 1-10: HTTP Web Browser Profile: Valid Authentication Assertion**  
613 **Artefact from Different Authority Consumed.**

614 *Description:* This test case submits a valid HTTP authentication artefact  
615 generated by a different authority to the authentication authority being  
616 tested for conformance. It confirms that the authentication assertion  
617 artefact has been properly consumed by checking that access has been granted  
618 to a resource in the environment protected by the authentication authority for  
619 which conformance is being tested.

620 *Pass/Fail Criteria:* The environment in which the testec authentication  
621 authority operates must deny access to a resource prior to the  
622 receipt of an authentication assertion reference and must allow access to a  
623 resource in that environment after receipt of the authentication assertion  
624 reference.

625 *Reference:* **R-AUTHN**, and **R-MULTIDOMAIN**

626 *Implementation notes:* test program implementing this test case establishes  
627 successful execution of the test case by receiving access to a protected  
628 resource.

629 **Test Case 1-15: HTTP Web Browser Profile: Authentication Assertion with**  
630 **unrecognized condition rejected.**

631 *Description:* This test case submits a valid HTTP authentication artefact  
632 generated by a different authority to the authentication authority being  
633 tested for conformance. The corresponding authentication assertion, however,  
634 contains a condition unrecognized by the tested authentication authority. The  
635 test case confirms that the authentication assertion artefact has been  
636 properly consumed by checking that the authentication request is rejected by  
637 the authentication authority for which conformance is being tested.

638 *Pass/Fail Criteria:* The environment in which the tested authentication  
639 authority operates must deny access to the environment for an  
640 assertion which is identical to an accepted assertion except for having an  
641 unrecognized condition.

642 *Reference:* **R-AUTHN**, and **R-MULTIDOMAIN**

643 *Implementation notes:* test program implementing this test case establishes  
644 successful execution of the test case by being denied access to the  
645 environment.

646 **4.2.2 Test Group 2: Attribute Authority Test Group**

647 The test cases in this test group check for conformance to the Attribute  
648 Authority partition at both required and optional levels. The test cases  
649 derive from the following use cases:

- 650     ▪ Scenario 1-3 "Single sign-on, third-party security service"  
651       (authorization-related functionality).
- 652     ▪ [tbd]

653 An implementation or application claiming conformance must successfully  
654 complete the following tests, related to support for the required HTTP  
655 request/response protocol binding:

- 656     ▪ Test 2-1
- 657     ▪ Test 2-2
- 658     ▪ Test 2-3



659 An implementation or application claiming conformance to the SOAP protocol  
660 binding must successfully completed these tests in addition to the required  
661 tests.

662     ▪ Test 2-4

663     ▪ Test 2-5

664     ▪ Test 2-6

665 An implementation or application claiming conformance to the Web Browser  
666 Profile must successfully completed these tests in addition to the required  
667 tests.

668     ▪ Test 2-7

669     ▪ Test 2-8

670     ▪ Test 2-9

671     ▪ Test 2-10

672 Note that the use of a valid attribute assertion request/response as part of a  
673 request for authorization is included in Test Groups 3, 4 and 5 (Sections  
674 4.2.3, 4.2.4 amd 4.2.5).

675 **Test Case 2-1: HTTP Protocol Binding: Valid Attribute Assertion Produced in**  
676 **Response to Valid Attribute Query. REQUIRED**

677 *Description:* This test case submits an HTTP message to an attribute authority  
678 and checks that the attribute authority return a valid attribute assertion.

679 *Pass/Fail Criteria:* Attribute assertion returned by implementation or  
680 application must contain all required information in the right sequence and  
681 format. Any optional information included (including conditions) must not  
682 compromise the validity of the required information.

683 *Reference:* [tbd]

684 *Implementation notes:* Test program implementing this test case establishes  
685 successful execution of the test case by inspection of the format of the  
686 returned assertion.

687

688 **Test Case 2-2: HTTP Protocol Binding: Valid Attribute Assertion Artefact**  
689 **Produced in Response to Valid Attribute Query. REQUIRED**

690 *Description:* This test case submits an HTTP message to an attribute authority  
691 and checks that the attribute authority returns a valid attribute assertion  
692 artefact.

693 *Pass/Fail Criteria:* Authentication assertion artefact returned by  
694 implementation or application must be contain all required information in the  
695 right sequence and format. Any optional information included (including  
696 conditions) must not compromise the validity of the required information.

697 *Reference:* [tdb]

698 *Implementation notes:* Test program implementing this test case establishes  
699 successful execution of the test case by inspection of the format of the  
700 returned assertion artefact.

701

702 **Test Case 2-3: HTTP Protocol Binding: Valid Attribute Assertion Artefact from**  
703 **Same Authority Consumed. REQUIRED**

704 *Description:* This test case submits a valid HTTP attribute artefact, generated  
705 as a result of an HTTP request/response protocol binding, to an attribute  
706 authority and confirms that the attribute assertion artefact has been properly  
707 consumed by inspecting the attribute assertion returned.

708 *Pass/Fail Criteria:* Attribute assertion returned by implementation or  
709 application must be contain all required information in the right sequence and  
710 format. Any optional information included (including conditions) must not  
711 compromise the validity of the required information.

712 *Reference:* [tbd]

713 *Implementation notes:* Test program implementing this test case establishes  
714 successful execution of the test case by inspection of the format of the  
715 returned assertion artefact.

716

717 **Test Case 2-4: SOAP Protocol Binding: Valid Attribute Assertion Produced in**  
718 **Response to Valid Attribute Query.**

719 *Description:* This test case submits a SOAP message to an attribute authority  
720 containing authentication credentials and checks that the attribute authority  
721 return a valid attribute assertion.

722 *Pass/Fail Criteria:* Attribute assertion returned by implementation or  
723 application must contain all required information in the right sequence and  
724 format. Any optional information included (including conditions) must not  
725 compromise the validity of the required information.

726 *Reference:* [TBD]

727 *Implementation notes:* Test program implementing this test case establishes  
728 successful execution of the test case by inspection of the format of the  
729 returned assertion.

730 **Test Case 2-5: SOAP Protocol Binding: Valid Attribute Assertion Artefact**  
731 **Produced in Response to Valid Attribute Query.**

732 *Description:* This test case submits a SOAP message to an attribute authority  
733 containing attribute credentials and checks that the attribute authority  
734 returns a valid attribute assertion artefact.

735 *Pass/Fail Criteria:* Assertion artefact returned by implementation or  
736 application must be contain all required information in the right sequence and  
737 format. Any optional information included (including conditions) must not  
738 compromise the validity of the required information.

739 *Reference:* [tbd]

740 *Implementation notes:* Test program implementing this test case establishes  
741 successful execution of the test case by inspection of the format of the  
742 returned assertion artefact.

743

744 **Test Case 2-6: SOAP Protocol Binding: Valid Attribute Assertion Artefact from**  
745 **Same Authority Consumed.**

746 *Description:* This test case submits a valid SOAP attribute artefact, generated  
747 as a result of an SOAP request/response protocol binding, to an attribute  
748 authority and confirms that the attribute assertion artefact has been properly  
749 consumed by inspecting the attribute assertion returned.

750 *Pass/Fail Criteria:* Assertion returned by implementation or application must  
751 be contain all required information in the right sequence and format. Any  
752 optional information included (including conditions) must not compromise the  
753 validity of the required information.

754 *Reference:* [tbd]

755 *Implementation notes:* Test program implementing this test case establishes  
756 successful execution of the test case by inspection of the format of the  
757 returned assertion.

758 **Test Case 2-7: SHTTP Web Browser Profile: Valid Attribute Assertion Produced**  
759 **in Response to Valid Attribute Query.**

760 *Description:* This test case submits an HTTP message to an attribute authority  
761 and checks that the attribute authority return a valid authentication  
762 assertion.

763 *Pass/Fail Criteria:* Assertion returned by implementation or application must  
764 contain all required information in the right sequence and format. Any  
765 optional information included (including conditions) must not compromise the  
766 validity of the required information.

767 *Reference:* [TBD]

768 *Implementation notes:* Test program implementing this test case establishes  
769 successful execution of the test case by inspection of the format of the  
770 returned assertion.

771 **Test Case 2-8: HTTP Web Browser Profile: Valid Attribute Assertion Artefact**  
772 **Produced in Response to Valid Attribute Query.**

773 *Description:* This test case submits an HTTP message to an attribute authority  
774 and checks that the attribute authority returns a valid attribute assertion  
775 artefact.

776 *Pass/Fail Criteria:* Authentication assertion artefact returned by  
777 implementation or application must be contain all required information in the  
778 right sequence and format. Any optional information included (including  
779 conditions) must not compromise the validity of the required information.

780 *Reference:* [tdb]

781 *Implementation notes:* Test program implementing this test case establishes  
782 successful execution of the test case by inspection of the format of the  
783 returned assertion artefact.

784

785 **Test Case 2-9: HTTP Web Browser Profile: Valid Attribute Assertion Artefact**  
786 **from Same Authority Consumed.**

787 *Description:* This test case submits a valid attribute artefact, generated as a  
788 result of an HTTP message, to an attribute authority and confirms that the  
789 attribute assertion artefact has been properly consumed by inspecting the  
790 attribute assertion returned.

791 *Pass/Fail Criteria:* Assertion returned by implementation or application must  
792 be contain all required information in the right sequence and format. Any  
793 optional information included (including conditions) must not compromise the  
794 validity of the required information.

795 *Reference:* [tbd]

796 *Implementation notes:* Test program implementing this test case establishes  
797 successful execution of the test case by inspection of the format of the  
798 returned assertion.

799

800 **Test Case 2-10: HTTP Web Browser Profile: Valid Attribute Assertion Artefact**  
801 **from Different Authority Consumed.**

802 *Description:* This test case submits a valid HTTP attribute artefact generated  
803 by a different authority to the attribute authority being tested for  
804 conformance. It confirms that the attribute assertion artefact has been  
805 properly consumed by checking that a proper request for the corresponding  
806 attribute assertion is received from the tested attribute authority.

807 *Pass/Fail Criteria:* The environment in which the testec authentication  
808 authority operates must generate a valid request for the attribute  
809 assertion associated with the artefact.

810 *Reference:* [TBD]

811 *Implementation notes:* test program implementing this test case establishes  
812 successful execution of the test case by generating a valid request for the  
813 attribute assertion.

814 *Implementation notes:* test program implementing this test case establishes  
815 successful execution of the test case by being denied access to the  
816 environment.

817 **4.2.3 Test Group 3: Authorization Authority Test Group**

818 **Test Case 3-11: HTTP Web Browser Profile: Attribute Assertion with**  
819 **unrecognized condition rejected.**

820 *Description:* This test case submits a valid HTTP authentication artefact to  
821 the authentication authority being tested for conformance. The corresponding  
822 authentication assertion, however, contains a condition unrecognized by the  
823 tested authentication authority. The test case confirms that the  
824 authentication assertion artefact has been properly consumed by checking that  
825 the authorization request with which the attribute assertion is associated is  
826 rejected by the authentication authority for which conformance is being  
827 tested.

828 *Pass/Fail Criteria:* The environment in which the tested authentication  
829 authority operates must deny access to the environment for an  
830 assertion which is identical to an accepted assertion except for having an  
831 unrecognized condition.

832 *Reference:* **R-AUTHN**, and **R-MULTIDOMAIN**

833 **4.2.4 Test Group 4: Policy Decision Authority Test Group**

834 **4.2.5 Test Group 5: Policy Enforcement Authority Test Group**

835 **4.3 Test Suite**

- 836 - Prescribe a test methodology
- 837 - How test suite will be delivered/used (e.g., web based, downloadable)
- 838 - Who will 'own' the testing program
- 839 - Policy and procedures
- 840 - Testing laboratory
- 841 - Control board
- 842 - Test suite maintenance

843

844

845 **4.3.1 Reference Architecture**

846 **4.3.2 Infrastructure**

847 **4.3.3 Using the Test Suite**

848 **4.3.4 Test result tabulation and reporting**

849 **4.4 Certification Process**

850 A certification process has not been defined for SAML V1.0. Conformance may  
851 be declared for an implementation or application on the basis of validation  
852 testing.

853 **5 Conformance services**

854

855 < This section describes the services, which the organization has to provide  
856 including software services, releases, self-test kit, actual computer  
857 systems, facilities, web based interfaces, availability,... >

858 **5.1.1 Testing Service**

859 Guidelines for establishing a test service