SAML Conformance Program Specification

This version:

File : sstc-draft-conformance-spec-006.doc
Date : November 2, 2001

Authors

- Krishna Sankar [ksankar@cisco.com]
- Robert Griffin [Robert.Griffin@entrust.com]

Contributors

- Lynne Rosenthal
- Mark Skall
- Marc Chanliau
- Charles Norwood
- Tony Palmer
- Mark O'Neill
- Mike Myers
- Hal Lockhart

Abstract

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

Referenced Documents

1. http://www.itl.nist.gov/div897/ctg/conformProject.shtml
2. http://lists.oasis-open.org/archives/conformance/200104/msg00000.html
3. XML Protocol specification conformance issues

Notational Conventions

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

Status of this Document

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

Document Version History

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

Table of Contents

1 Scope of the Conformance Program

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

The deliverables of the SAML conformance effort include:

- Conformance clause in the SAML Specification, defining at a high-level what conformance means for the SAML standard
- Conformance Program specification (this document)
- Conformance Test Suite. This is a set of test programs, result files and report generation tools that can be used by vendors of SAML-compliant software, buyers interested in confirming SAML compliance of software, and testing labs running conformance tests on behalf of vendors or buyers.

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

2 Conformance Clause

Please refer to the SAML specification for the conformance clause.

3 Conformance Process

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

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

- Documentation describing test cases, linked to use cases and requirements

- Test suite, based on those test cases, that can be run against an implementation to demonstrate any of the several levels/profiles of conformance defined in the conformance clause of the SAML specification

- Documentation describing how to run the test suite, interpret the results, and resolve disputes regarding the results of the tests

The SAML Technical Committee is not, however, responsible for testing of particular implementations.

3.1 Conformance Testing, Validation and Certification

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

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

- **Validation** may be done without certification for such purposes as self-test. An implementor who has validated SAML conformance by means of self-test cannot legitimately use the term “certified for SAML conformance”. However, an implementor may claim to have “validated for SAML conformance” at a given conformance partition and level after having run successfully all tests required for that partition and level.

- **Certification** requires validation by a third-party rather than through self-test. A certifying authority identified by the SAML TC as responsible for issuing certification of SAML conformance.

Note that both validation and certification subsume conformance testing.

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

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

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

3.2 Implementation and Application Conformance

SAML Conformance is applicable to:

- Implementations of SAML assertions, protocols and bindings. These could be in the form of toolkits, products incorporating SAML components, or reference implementations that demonstrate the use of SAML components.

- Applications that consume SAML assertions or that execute on SAML implementations (for example, using a SAML toolkit to support multi-domain single-signon)

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

(1) The implementation shall support all the required interfaces defined within this standard for a given profile and level. These interfaces shall support the functional behavior described in the standard.

(2)An implementation may provide additional or enhanced features or functionality not required by the SAML Specification. These non-standard extensions shall not alter the specified behavior of interfaces or functionality defined in the specification

(3) The implementation may provide additional or enhanced facilities not required by this standard. These non-standard extensions shall not alter the specified behavior of interfaces defined in this standard. They may add additional behaviors. In these circumstances, the implementation shall provide a mechanism whereby a SAML conforming application shall be recognized as such, and be executed in an environment that supports the functional behavior defined in this standard.

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

(1) The application shall be able to execute on any conforming implementation.

(2) If an application requires a particular feature set that is not available on a specific implementation, then the application must act within the bounds of the SAML specification even though that means that the application may not perform any useful function. Specifically, the application shall do no harm, and shall correctly return resources and vacate memory upon discovery that a required element is not present.

4 Technical requirements for SAML Conformance

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

4.1 Conformance Partitions and Levels

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

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

Partitions provide a means to:

a) improve interoperability between implementations by inhibiting the proliferation of private subsets of SAML

b) provide a foundation for testing and promote uniformity of conformance tests;

c) enhance the availability of consistent implementations of profiles.

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

The SAML partitions are:

- **Authentication Authority**. This partition contains all SAML functionality related to creation, propagation and consumption of authentication assertions and authentication assertion artefacts.
- **Attribute Authority**. This partition includes all SAML functionality related to the creation, propagation and consumption of attribute assertions and attribute assertion artefacts.
- **Authorization Authority**. This partition includes all SAML functionality related to the creation, propagation and consumption of authorization decision assertions and authorization decision artefacts.
- **Policy Decision Authority**. This partition is a subset of the Authorization Authority partition, supporting the producer role for authorization decision assertions.

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

4.1.1 Authentication Authority Partition

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

Conformance to this partition can be claimed at several levels:

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

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

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

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

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

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

4.1.2 Attribute Authority Partition

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

Conformance to this partition can be claimed at several levels:

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

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

- Conformance to the SOAP protocol binding shall be expressed as "[implementation or application] conforms to the SAML V1.0 SOAP protocol binding for the attribute authority partition"

- Conformance to the web browser profile shall be expressed as "[implementation or application] conforms to the SAML V1.0 SOAP protocol binding for the attribute authority partition"

Conformance to this partition must include both consumer and producer roles to allow for nesting of assertions.

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

4.1.3 Authorization Authority Partition

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

Conformance to this partition can be claimed at several levels:

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

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

- Conformance to the SOAP protocol binding shall be expressed as "[implementation or application] conforms to the SAML V1.0 SOAP protocol binding for the authorization authority partition"

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

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

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

- Support for consumption of authentication assertions shall be expressed as "[implementation or application] authorization authority conforms to the SAML V1.0 authentication assertion schema."

- Support for consumption of attribute assertions shall be expressed as "[implementation or application] authorization authority conforms to the SAML V1.0 attribute assertion schema."

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

4.1.4 Policy Decision Authority Partition

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

Conformance to this partition can be claimed at several levels:

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

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

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

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

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

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

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

4.1.5 Policy Enforcment Authority Partition

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

Conformance to this partition can be claimed at several levels:

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

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

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

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

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

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

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

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

4.2 Test Cases for SAML V1.0

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

Each test case includes:

- A description of the test purpose (i.e., what is being tested – the conditions, requirements, or capabilities which are to be addressed by a particular test
- The pass/fail criteria,
- A reference to the requirement or section in the standard from which the test case is derived (i.e., traceability back to the specification.

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

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

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

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

4.2.1 Test Group 1 – Authentication Authority Partition

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

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

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

- Test 1-1
- Test 1-2
- Test 1-3

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

- Test 1-4
- Test 1-5
- Test 1-6

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

- Test 1-7
- Test 1-8
- Test 1-9
- Test 1-10

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.2.2 Test Group 2: Attribute Authority Test Group

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

- Scenario 1-3 “Single sign-on, third-party security service” (authorization-related functionality).
- [tbd]

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

- Test 2-1
- Test 2-2
- Test 2-3

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

- Test 2-4
- Test 2-5
- Test 2-6

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

- Test 2-7
- Test 2-8
- Test 2-9
- Test 2-10

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

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

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

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

Reference: **[tbd]**

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

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

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

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

Reference: **[tdb]**

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

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

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

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

Reference: **[tbd]**

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

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

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

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

Reference: **[TBD]**

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

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

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

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

Reference: **[tdb]**

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

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

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

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

Reference: **[tbd]**

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

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

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

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

Reference: **[TBD]**

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

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

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

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

Reference: **[tdb]**

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

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

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

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

Reference: **[tbd]**

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

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

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

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

Reference: [TBD]

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

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

4.2.3 Test Group 3: Authorization Authority Test Group

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

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

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

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

4.2.4 Test Group 4: Policy Decision Authority Test Group

4.2.5 Test Group 5: Policy Enforcement Authority Test Group

4.3 Test Suite

- Prescribe a test methodology
- How test suite will be delivered/used (e.g., web based, downloadable)
- Who will ‘own’ the testing program
- Policy and procedures
- Testing laboratory
- Control board
- Test suite maintenance

4.3.1 Reference Architecture

4.3.2 Infrastructure

4.3.3 Using the Test Suite

4.3.4 Test result tabulation and reporting

4.4 Certification Process

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

5 Conformance services

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

5.1.1 Testing Service

Guidelines for establishing a test service