1099 18th
Street
Suite 2950
Denver, CO 80202

Adoption Services Application for SAML v1.1 OASIS Standard Conformance Testing Services

Submitted By: Frank Cardello, VP Business Development
Darren Platt, Solutions Architect
March 8, 2005

Table of Contents

1. Service Description 3
2. OASIS SAML v1.1 Security Services Technical Committee (SSTC) Member Advocates 3
3. Market Driver(s) For The Service 3
4. Market Size 4
4.1 Estimated Participating Companies 4
4.2 Timeframe for Service Availability 4
4.3 Service Pricing 4
5. Technical Service Requirements 4
5.1 Level of Participation Required of the OASIS SSTC 4
5.2 Service Availability (How is the Service Offered) 4
6. Service overview 5
6.1 Service Provider Name: 5
6.2 Service Overview 5
6.2.1 Toolset 5
6.2.2 Service Details 6
6.2.3 Methodology 6
6.2.4 Staffing 6
6.2.5 Related Service Provider Organizations 6
6.2.6 Planned Service Enhancements 6
6.3 Pricing Information 6
6.4 Certification Program 6
6.5 Proposed Revenue Share With OASIS 6
7. Required Documentation 6
7.1 Requirements for Conformance Testing Services 6
7.1.1 Test assertion summary document 6
7.1.2 Testing process overview 7
7.1.3 Process and Procedures 7
7.2 Requirements for Training/Personal Skill Certification: 9
7.2.1 Summary of Training or Test Information 9
7.2.2 Training or Testing Process Overview 9
7.3 Process and Procedures 9
7.3.1 Program Development 9
7.3.2 Problem/Issue Resolution (Clarifying OASIS Involvement) 9
Appendices 10

1. Service Description

PingDeploy SAML v1.1 Conformance & Security Testing is a managed service to enable remote testing for the SAML v1.1 OASIS Standard ("SAML v1.1") specification:
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#samlv11

PingDeploy allows organizations to test a baseline level of SAML v1.1 conformance. It is designed to help you ensure security and interoperability – reducing deployment time, cost and complexity.

As a mediated web application, PingDeploy is easy to use and implement. No software is required, and the service can be set up in minutes. Leveraging PingDeploy is accomplished through the use of the Conformance Engine and interaction with a Ping Identity conformance engineer.

2. OASIS SAML v1.1 Security Services Technical Committee (SSTC) Member Advocates

Member Advocates:

- ***Rob Philpott*** -- RSA – (781) 515-7115 – rphillpott@rsasecurity.com – SSTC
- ***Marc Chanliau*** – Computer Associates – (508) 847-8309 – marc.chanliau@ca.com – Security Services SSTC
- ***Robin Martherus*** – Oblix – (480) 814-0016 – rmartherus@oblix.com – Security Services SSTC
- ***Mark Joynes*** – Entrust – (613)270-3134 – mark.joynes@entrust.com – Security Services SSTC
- ***Prateek Mishra*** – Principal Identity -- (617) 872-7737 – pmishra@principalidentity.com – SSTC
- ***Kevin M. Anderson*** – DataPower -- (617) 453-5660 -- kevina@datapower.com – SSTC

See http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security for more information on the SSTC.

3. Market Driver(s) For The Service

As identity federation gains in popularity a growing number of vendor products are incorporating SAML v1.1 functionality to enable secure identity authentication, authorization and attribute exchange. Vendor interpretations of the SAML v1.1 protocol may vary – this results in a marketplace of products that often lack interoperability or require significant work and testing to validate.

The PingDeploy Conformance Testing Service enables vendor products that implement SAML v1.1 to validate that their SAML v1.1 implementation adheres to a consistent and industry tested interpretation of the SAML v1.1 protocol.

4. Market Size

4.1 Estimated Participating Companies

Ping estimates that today approximately 50 companies who implement SAML v1.1 will be interested in consuming the testing service. We expect that number to increase significantly with the ratification and subsequent vendor product support of SAML 2.0.

4.2 Timeframe for Service Availability

The testing service is currently available to the market.

4.3 Service Pricing

Costs for certification average between 12,000 – 20,000 USD depending upon the number of days required to complete the certification testing.

5. Technical Service Requirements

5.1 Level of Participation Required of the OASIS SSTC

The OASIS SSTC will not be directly involved in the operations of the PingDeploy conformance service. However, members of the Technical Committee (through their corporations) participate in the SAML Conformance Working Group (**"SCWG"**) that is responsible for determining the approved interpretation of the specification. The SCWG consists of member companies that collaborate under a Ping partner program under a governance process that results in a collaborative agreed upon interpretation of SAML v1.1 for the purposes of operating the Ping Deploy Conformance Testing Service. The SCWG and the OASIS SSTC are NOT affiliated entities.

5.2 Service Availability (How is the Service Offered)

The Ping Identity Conformance Service is available today and offered as a mediated web-based testing service to organizations wishing to test their implementations for conformance to the SAML v1.1 federation standard. The Conformance Service is implemented by 2 main 'actors' – Ping Identity's Conformance Engine, and a Ping Identity conformance engineer. Execution of the service also requires the participation of a representative from the client organization.

The Conformance Engine tests implementations for conformance to the SAML v1.1 specification by acting as the other parties in SAML v1.1 transactions. For example, in order to test that an implementation can correctly perform in the role of the 'producer' in a single sign-on interaction, the Conformance Engine acts as both the 'consumer' and the web browser.

A Ping Identity conformance engineer facilitates the testing process at each stage. First, the conformance engineer configures the Conformance Engine and works with a representative from the organization with the implementation to be tested to ensure that their implementation has been configured properly. The Ping conformance engineer then coordinates the test execution with the organization's representative, working to diagnose and resolve any issues that are identified. After the testing is complete, the Ping conformance engineer will analyze the results of the test and create a report containing the findings.

6. Service overview

6.1 Service Provider Name:

Ping Identity Corporation

6.2 Service Overview

6.2.1 Toolset

There are two key components in the delivery of the conformance testing service:

Web Interface

The conformance service provides a web interface for scheduling and configuring conformance testing events. Once an organization has entered into an agreement with Ping Identity to do conformance testing, they are provided an account they can use to access this interface. The web interface provides:

- A calendar for viewing their organization's scheduled testing events.
- A web form allowing the customer to choose the conformance profiles they would like to test. They may also choose a custom script pack that they had previously created in conjunction with Ping Identity's professional services team.
- A web form where customers will input their configuration for testing purposes.
- Functionality for generating certificates to be used in the testing.
- An interface that will display the configuration settings for the conformance engine that the implementation under test will need.

Conformance Engine

The Conformance Engine is a general-purpose protocol testing framework that is adapted to test specific federation protocols by using specific script packs. Script packs are groups of scripts that direct the Conformance Engine to perform standard protocol interactions with the system being tested. In order to thoroughly test implementations of standard federation protocols, the Conformance Engine acts in the roles of the 'other' systems of a federation – interacting with the system under test to validate its behavior. The Conformance Engine provides a large degree of configurability and extensibility; enabling a wide range of tests including basic course, boundary conditions, and failure scenarios. The Conformance Engine can be easily extended to test additional functionality, including configuration-specific and non-standard behavior.

6.2.2 Service Details

Please see above.

6.2.3 Methodology

The conformance testing service employs several testing methodologies:

- Black Box Testing
- Failure Scenario / Negative Testing
- Internet-Based Remote Testing

6.2.4 Staffing

The service is mediated by conformance engineers, who are staffed by the PingDeploy organization within Ping Identity Corporation.

The hardware infrastructure is provided by Ping Identity Corporation.

6.2.5 Related Service Provider Organizations

Not Applicable to the Ping Conformance Service.

6.2.6 Planned Service Enhancements

The future directions of enhancement of the service include:

- Greater Automation – less reliance on a conformance engineer to facilitate testing services.
- Full Remote Testing

6.3 Pricing Information

See Section 4.3 above.

6.4 Certification Program

Ping will license the Certification Mark (called PASS Certification) to Third Parties for use in connection with their respective products after successful completion of the Certification Services pursuant to the terms set forth in Ping's standard agreement for Certification Services.

6.5 Proposed Revenue Share With OASIS

Ping will provide10% of all top line revenue generated from the service during the term of the referral agreement with OASIS. Top line revenue is defined as gross invoiced dollars for each company tested (net of any travel related expenses, if applicable).

7. Required Documentation

7.1 Requirements for Conformance Testing Services

7.1.1 Test assertion summary document

See the attached Excel document called SAML v1.1 Testing Matrix. This represents the tests that are provided and required for each conformance profile. Conformance profiles are pre-defined subsets of the SAML v1.1 specification.

7.1.2 Testing process overview

Certification Process Flow

1. An organization signs up for the Ping Identity Conformance Service, and is issued a userID and password for accessing the Conformance Service Web Interface.
2. The organization interfaces with PingDeploy Conformance Engineer to coordinate testing dates.
3. The representative from the organization uses the web interface to choose the profiles they would like to test.
4. The representative from the organization uses the web interface to upload information about the configuration of the implementation they would like to test.
5. The representative from the organization downloads configuration information required to connect to the conformance service.
6. The representative from the organization downloads certificates to be used in the testing.
7. The representative configures their implementation to connect to the conformance service.
8. The representative from the organization contacts and the Ping conformance engineer contact each other via telephone or IM to coordinate the test execution.
9. The Ping conformance engineer directs the conformance engine to begin the applicable tests (depending on the conformance profile chosen).
10. The Ping conformance engineer and the organization's representative work together to troubleshoot any issues that are identified.
11. The Ping conformance engineer re-runs the tests to attempt to certify the organization's implementation.
12. The Ping conformance engineer evaluates the results of the test and creates a report that is sent to the organization's representative.
13. Steps 2 - 12 are repeated until the organization's implementation passes the test suite.
14. The organization either comes to Ping's testing lab, or hosts an PingDeploy conformance engineer at their site for certification testing.
15. Assuming successful onsite verification, the testing organization is deemed certified.

7.1.3 Process and Procedures

Test case development

The implementation of the test cases are developed by Ping Identity. The requirements for these implementations are driven by the SCWG (note: please see paragraph 5.3.1 for the definition and role of the SCWG) as they vote as to the specific correctness of the service implementation. The SCWG used several sources and techniques for developing the list of test cases. The conformance specification provided by the SAML v1.1 SSTC (please see http://www.oasis-open.org/committees/download.php/3402/oasis-sstc-saml-conform-1.1.pdf) was a starting point. The SCWG then analyzed each of the specifications' mentions of the normative word "MUST" in order to develop test cases that validate an implementations proper handling of the protocol in positive and negative scenarios.

Collection, Documentation, and Reporting of Client Issues
See below.

Problem/Issue Resolution (Particularly Clarifying OASIS Involvement)
In order for Ping to perform conformance testing, an initial interpretation of the specification was decided upon for a starting point. It is understood that this initial interpretation will be refined as additional organizations test against the initial interpretation - as embodied by the conformance engine and script pack. It is also understood that different organizations may at times disagree as to what the correct interpretation is. In order to resolve these disagreements and make these refinements, Ping has defined the following issue resolution process.

During the course of testing an implementation for conformance, the organization that is testing their implementation of SAML v1.1 will interact with the Ping Conformance Engineer to execute all of the appropriate test cases. As the tests progress, the Conformance Engineer will make the organization's testing representative (tester) aware of the results of each test as it is completed. After the testing is complete, Ping will provide the testing organization a report that details the tests that were performed, the ones that failed, why they failed, as well as the conformance engine log files.

Upon reviewing the findings, a testing organization may choose to dispute some of the results. In this case, the first step the testing organization would take would be to schedule a conference call with the Ping Conformance Engineer to review the specific issues. Ping will work with the representative of the organization to review the relevant areas of the specification set, and explain the justification for the test as it exists. If the testing organization still believes that their interpretation is correct (and the test isn't), then the dispute must be decided by the SCWG. This is due to the fact that any changes that are made to the conformance engine and script pack must first be approved by the SCWG.

In the case that the testing organization would like to have the SCWG resolve a dispute, the Conformance Engineer will represent the testing organization's concerns to the SCWG in order to protect the testing organization's confidentiality. The Conformance Engineer will document the position of the testing organization and share the document with the testing organization for their approval and refinement.

Once the testing organization's arguments have been well understood and documented, the issue is put to the SCWG for voting via a mailing list. Discussion will be had on the list, and then there will be a vote within two weeks (with some flexibility to accommodate for holidays, etc.) Each member of this working group has one vote, and simple majority wins. If the testing organization is determined to be correct, the conformance engine and script pack will be updated to reflect the new interpretation. If the testing organization is determined to be incorrect, then the conformance engine and script pack will remain unchanged (WRT this issue) and the testing organization will be required to modify their implementation if they choose to continue to pursue conformance.

Process for handling bug fixes for service
As issues are identified with the conformance engine and/or script packs, they will be resolved by PingDeploy conformance engineers.

Proposals for how the Service Provider will handle OASIS Specification changes and versioning.
The SCWG will develop versions of the script pack, and in some cases new script packs, for current specifications as resources permit.

7.2 Requirements for Training/Personal Skill Certification:

7.2.1 Summary of Training or Test Information

No training is necessary to consume the service as Ping Identity's trained conformance engineers mediate the delivery of the testing services.

7.2.2 Training or Testing Process Overview

Please see 7.1.2 above and Appendix B: PingDeploy SAML v1.1 Conformance and Security Testing Datasheet.

7.3 Process and Procedures

7.3.1 Program Development

The Certification Program was developed in partnership with leading vendors in the Identity Management Industry including: RSA, Netegrity/CA and Oblix. Please see the following link for additional information regarding group formation and goals of the initiative:

http://www.pingidentity.com/news/showPressRelease.action?id=25

A copy of the press release may also be found in Appendix E. Interested members are invited to join the SCWG. Members are added to the group via a governance structure that requires a majority vote of approval by the existing members. Once approved, SCWG applicants are required to sign the SAML Conformance Working Group (SCWG) Participation Agreement (See Appendix C) prior to formal participation in the governance process.

7.3.2 Problem/Issue Resolution (Clarifying OASIS Involvement)

Please see 7.1.3 above. It is not anticipated that OASIS will be involved in problem resolution at this time. Problem resolution is currently handled by a governance process within the SCWG. In addition, as stated in 7.3.1 above, the SCWG welcomes additional members who desire to participate in the script pack vetting process (participation is NOT mandatory to consume the conformance service).

7.3.3 OASIS Specification Changes and Versioning

Please see 7.1.3.

Appendices

Appendix A

SAML v1.1 Testing Matrix

Please see excel spreadsheet include as an email attachment to this application.

Appendix B

PingDeploy SAML v1.1 Conformance and Security Testing Datasheet

Please see PDF provided as an email attachment to this application.

Appendix C

SAML Conformance Working Group Participation Agreement
(For Companies Interested in Joining the SCWG)

Please see the agreement provided as an email attachment to this application.

Appendix D

Ping Certification Services Agreement
(For Companies Interested in Purchasing the Service – Note the Service is provided by Ping Identity Corporation)

Please see the agreement provided as an email attachment to this application.

Appendix E

Press Release: Ping Identity Delivers Federated Identity Conformance Service for SAML v1.1 in Collaboration with Industry's Leading Identity Management Vendors.

Please see the Press Release provided as an email attachment to this application.