SAML Profile Test Framework

Author: Rainer Hörbe (City of Vienna)
Date: 20-Dec-2012
Document Status: Initial draft

Scope and Purpose

Assure compliance of federation-facing interfaces of SAML actors

The SAML Profile Test Framework (referred here „Framework“) shall provide (prospective) participants of federations to assess their products and services for interoperability and compliance with a specific SAML profile that confines the SAML WebSSO use case to the specifications and requirements of a specific deployment. A list of deployment profiles related to the Kantara SAML 2.0 eGov Interoperability Profiles can be found at the Kantara FI-WG Wiki[1] .

The focus in the first phase is to provide test services to SPs. The rationale is for portalverbund.at[2] that there is a significantly lager number of SPs than IdPs, and IdPs usually have more experience with IAM than SPs.

Stakeholders

Stakeholders addressed by this effort are:

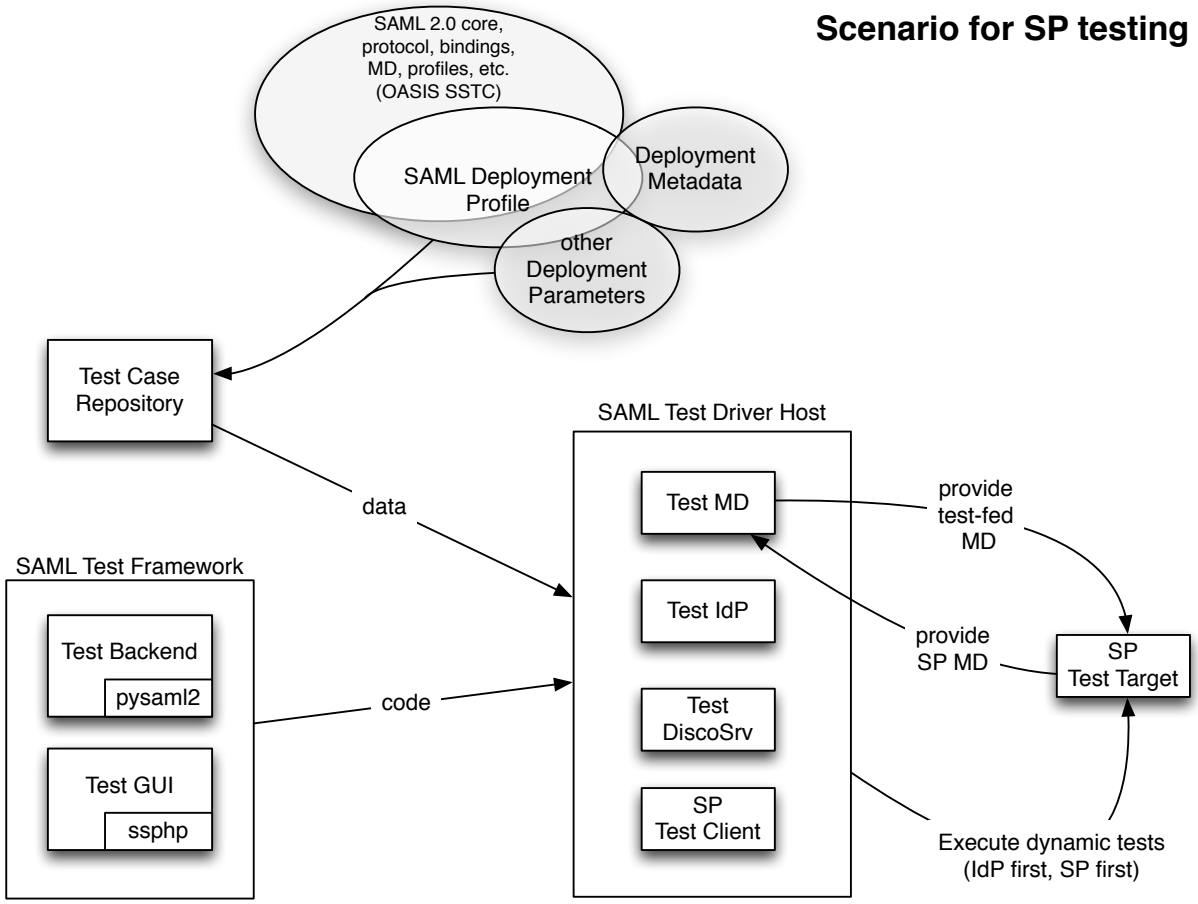
Stakeholder	*Concern*
SAML Profile Owner	Ensure that profile is adhered to; collect feedback from testers to improve profile.
Federation Authority/Operator	Require entities to be profile compliant before new or updates software is deployed.
Product vendor, OSS supporter/contributor	Ensure product compliance with deployment requirements; Reduce support requests by using test suite to spot configuration errors.
IdP Operator	Reduce integration effort with SPs
SP Operator	Reduce integration efforts when connecting to federations

The drivers of this effort are Kantara Initiative, Géant, and the AG-IZ (Austrian government’s eGov federation WG).

The first SAML profile to be implemented will be PVP2-S-Profile V2.1 (www.portalverbund.at)

[1] http://kantarainitiative.org/confluence/display/fiwg/SAML+Interoperability+and+Deployment+Profiles
[2] Austrian G2G Federation

Components



There are multiple sources that feed into test case repository:

- SAML standards (from OASIS SSTC);
- SAML Deployment Profile (restricts and extends the SAML standards);
- Deployment metadata (provides specific values about the SAML actors);
- Other deployment parameters: data and decisions that are neither in the profile nor in MD, but are needed to provide complete configurations; e.g. attribute sets.
- Unit test cases that prove certain behavior and structures.

The test framework shall be a common resource for many deployments. Test cases should be shared and improved in a community effort, but SAML profiles, test cases, test federations and test execution may differ for specific deployments. To support such a model, a service-type test case repository is being proposed.

Ideally, the repository should contain a superset of all test cases for all deployments to be tested providing reasonable test coverage. Test cases can be grouped and parameterized to address certain test scenarios. An extension and inheritance schema could be used to organize multiple scenarios.

Test execution would be the task of deployment-specific infrastructure. The tester would have to install the framework on the test driver host, check out the test data from the repository into a format suitable for the framework, and execute the tests.

Test Categories

SAML actors to be tested are SP and IdP.

Metadata Correctness & Completeness
- Schema valid XML?
- Check on elements in unknown namespaces
- Warn on recommended but missing elements
- Certificate validity
- Endpoint availability

Protocol flow
- Support for different bindings
- Request formats
- Response contents

Crypto properties
- Cipher support
- Signatures & TLS where required by profile
- trust anchors
- error handling on invalid, expired signatures and TLS-certs

Subject Attribute test (primär ein IDP fest)
- Nameid
- Attribute

Other rules
- retain relay state between request/response
- execute access decision based on authContextClassRef (exact match)
- Metadata freshness rules obeyed?

Vulnerability Scan
- Signature und TLS cert validation
- XML-Signature Wrapping (is SAML Pummel still relevant?)
- IMHO it does make sense to include the OWASP 10 vulnerability tests