SAML Test Harness Specification

as of April 4, 2013

Rainer Hörbe

Project Parameters

Building on Federation Lab:

(From http://de.slideshare.net/erlang/federation-lab-and-openid-connect)

- Identity toolkit for testing, validation and debugging of Identity Software.
- Automated testing tool for increasing interoperability between providers and consumers with SAML and OpenID Connect.
- A GÉANT project (GN3JRA3T2) in collaboration with Kantara Initiative and the OpenID community.
- Nordic collaboration (UNINETT and umu.se)

Enhanced by AT government contribution

- Help project to become a SAMl community effort with more and better test cases
- Test Harness for AT SAML eGov profile should be available end of Q2/2013

Key Concepts

Community Effort

- Use deployment experience to improve testing
- Manage test cases with web-2.0 style service

Self-service Testing

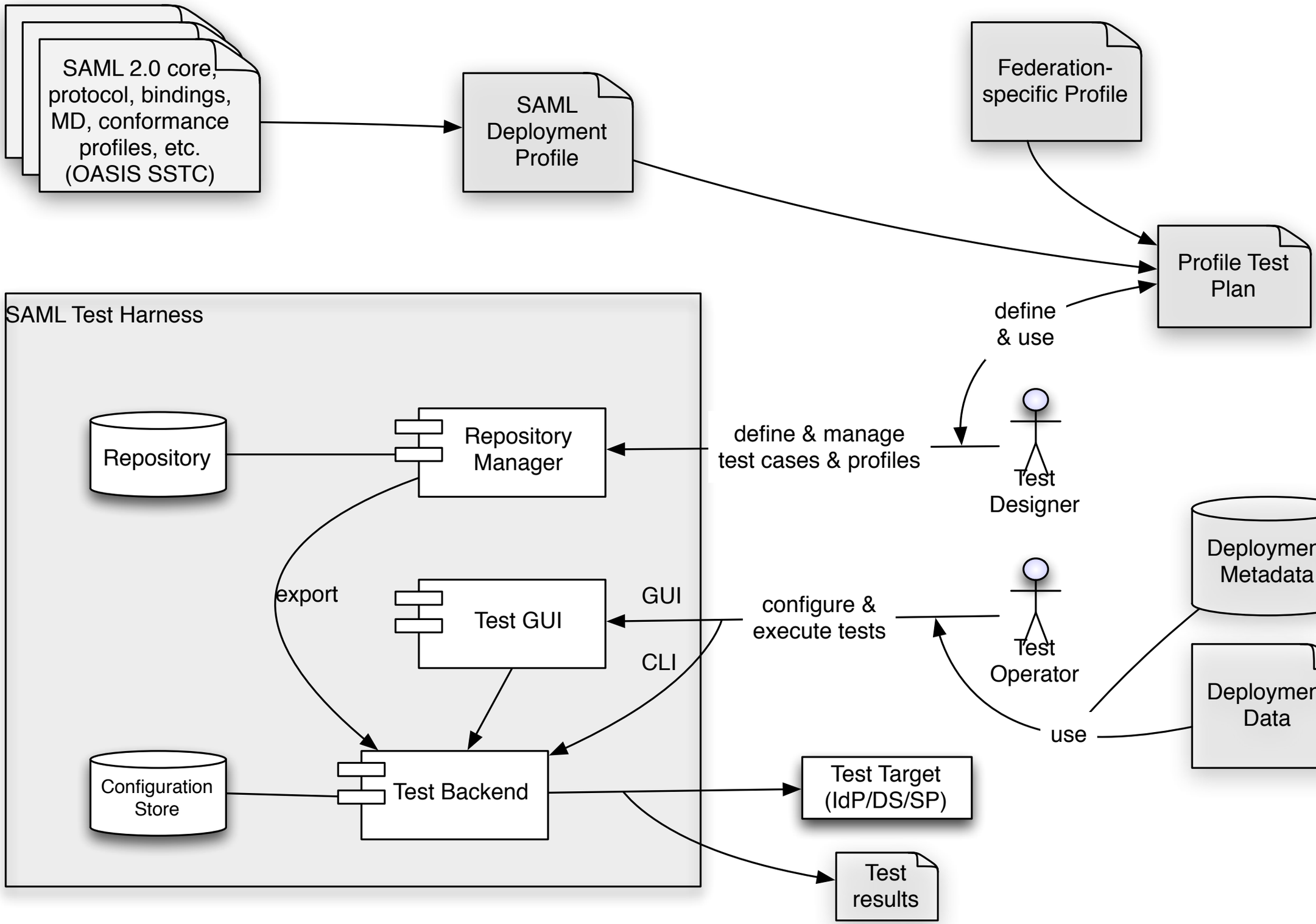
- Test Harness provides Test Plans consisting of Test Cases
- Test Plans can be executed when combined with deployment-specific Test Configuration

Organization of Test Repository

- Analogy to Linux Distro and Packages: Test Plans and Cases
- Version Management, System Configuration

SAML
Test Harness

Overview



Rough Test Categories

Metadata Correctness & Completeness

SAML Protocol flow

- (Bindings, request formats, response contents,

Attributes

- Attribute sets, values and rules involving multiple attributes
- LoA including timeout compliance

Crypto properties

- Cipher support, Signatures & TLS, invalid/expired signatures and certificates

Vulnerability Scan

- XML-Signature Wrapping, HTTP-server

Key Domain Objects

SAML Profiles specify *Requirements* (grouped in *Features*)

- e.g.: SAML2Int requires EntityDescriptors, which is part of the „Metadata“ Feature

Test Cases verify the *Test Target*‘s conformance with a *Requirement*

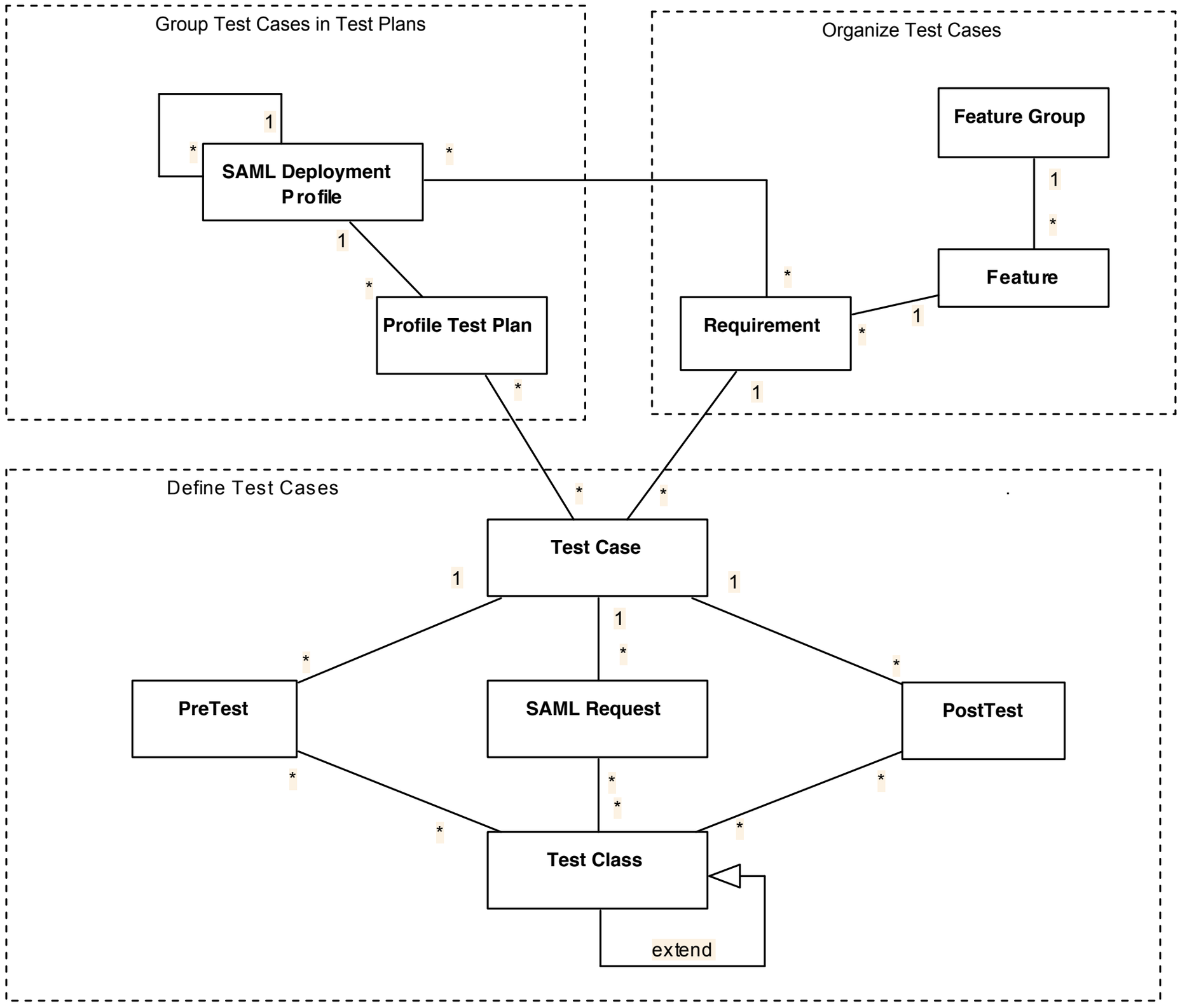
- e.g.: The IDP‘s metadata MUST include an<md:IDPSSODescriptor> element containing all necessary <md:KeyDescriptor> and<md:SingleSignOnService> elements

Test Plans select a set of *Test Cases* and define the relevance for each one (MUST/SHOULD/MAY comply and n/a)

A *Test Configuration* adds the deployment-specific data to execute a test plan, like metadata and the test target‘s EntityId

SAML
Test Harness

Repository Schema



How to deploy a Test Plan

a) Select Test Plan

- The Test GUI provides a list of available Profile Test Plans. The Test Operator needs to selected one to which this Test Configuration pertains.

b) Provide deployment configuration data to Test Harness

- Set MD Feed URL
- Provide any data and artifacts that are needed in addition to MD. E.g.:
  - MD certificate
  - User Interaction with the Test Target (AuthN, ..)
  - Test Results interface
  - Entity certificates if these are not provided with MD
  - Attribute release policy

c) Provide test target with Test Harness metadata

- Provide the selected subset of MD that is required to execute the Test Plan. The Test Operator may provide own certificates to the test harness.

d) Add Test Harness MD to Test target