



SAML signature validation

Stakeholder workshop

GN5-1 Trust & Identity Incubator

GÉANT Project Symposium, Montpellier, France
12 December 2023

Public (PU)

GN5-1

Agenda

- 11:45 Activity description and previous results
- 12:00 Feedback & discussion
- 12:25 Wrap-up and next steps

Activity description

The goal of the activity is to deliver a (software or service) solution that assists federation operators of NREN federations in testing at scale of several core security aspects of Service Providers SAML deployments within their federation.

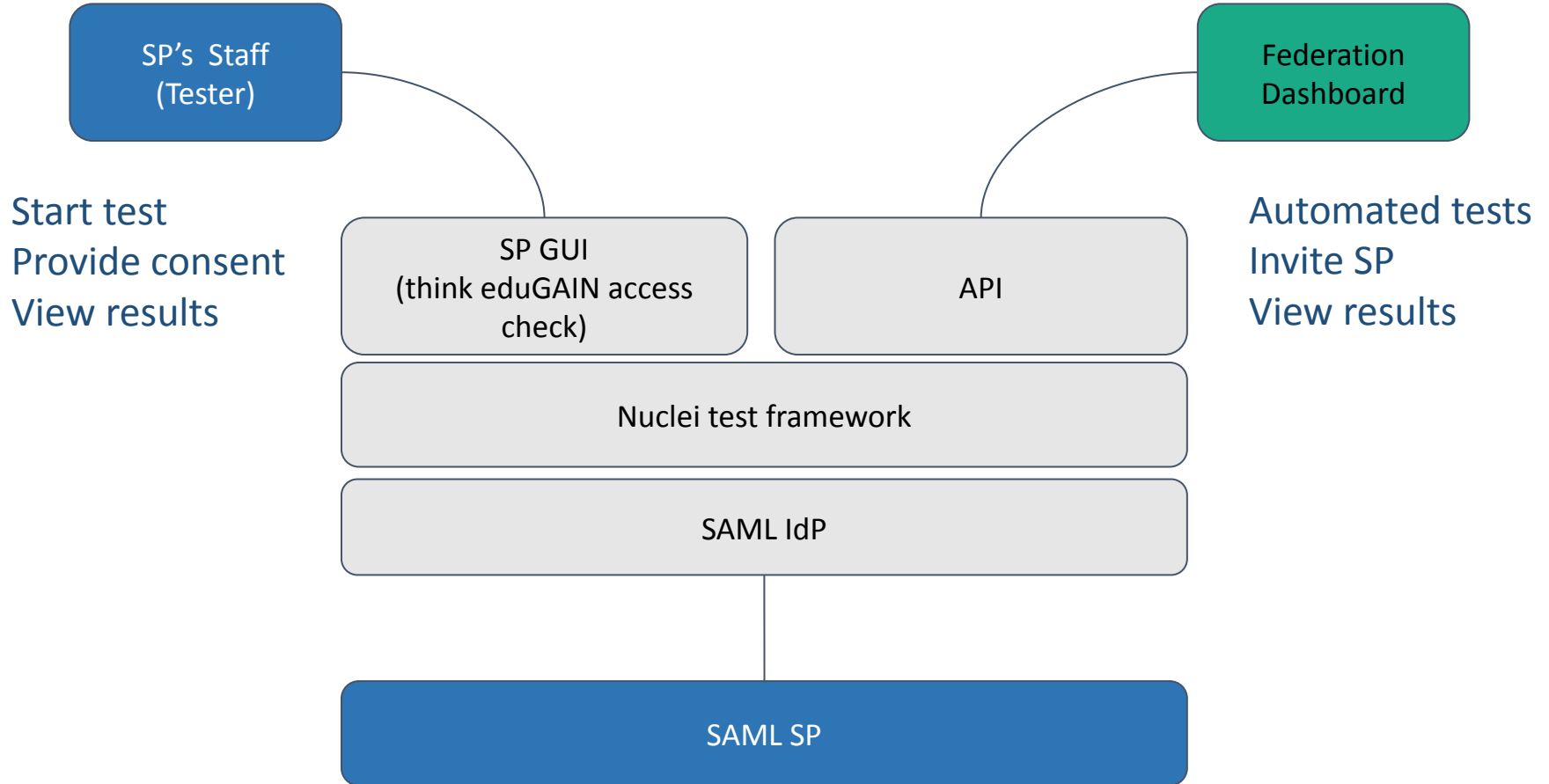
Deployment scenarios, to be confirmed with stakeholders, might include:

- Self-testing by an SP as part of the route towards becoming a production deployment
- (Automated) Testing the SP deployment as part of the initial onboarding into the federation by FedOps
- (Automated) Testing the SP deployment as part of periodic review by FedOps
- Institution initiated testing of SP as part of compliance review, e.g. wrt GDPR compliance, for a service they have a contract with

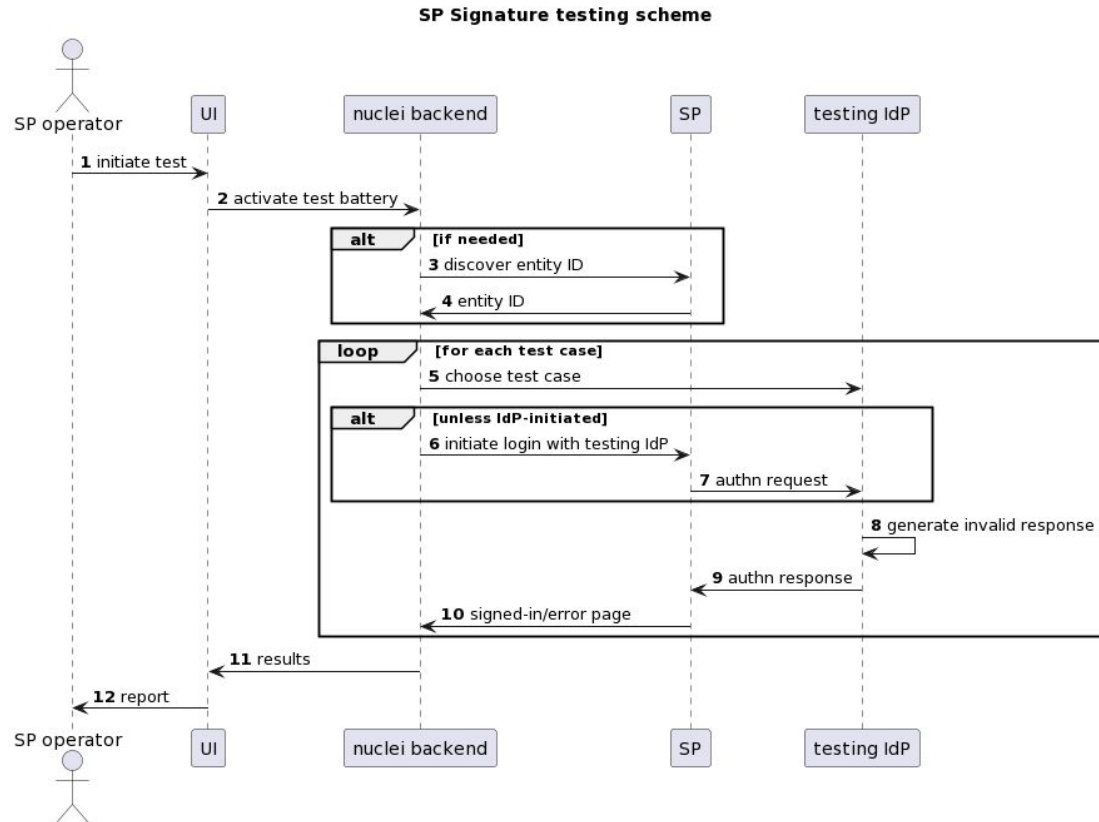
This topic should include the technical implementation of the use cases we would like to test against. In addition it needs to discuss and if need be develop a means to support FedOps to deploy the testsuite both technically and operationally.

Next to technical and operational requirements we need to understand as well as potential legal aspects, so we can include all of these in the design of the test suite.

Proposed setup



Technical solution



Technical solution

Nuclei

- A vulnerability scanner designed to identify exploitable weaknesses on the attack surface with a vast library of templates for various known vulnerabilities
- Built for automatic detection
- Two relevant scanning modes
 - raw HTTP (more efficient)
 - headless (with screenshots)
- Built-in basic modifications (base64, gzip, urlencode, ...)
 - Cannot construct signed XML documents
- Requires an IdP (library) for signature generation

Technical solution (nuclei template example)

```
id: incubatorsamltestheadless
info:
  name: Incubator SAML test headless
  severity: low
  tags: headless, extractor
variables:
  filename: '{{replace(BaseURL,"/","_')}}"
  dir: "screenshots"
  testCase: 'invalidSignature'
headless:
  - steps:
    - action: navigate
      args:
        url: "https://conformance-idp.maiv1.incubator.geant.org/module.php/conformance/test/setup
?testId={{url_encode(testCase)}}&spEntityId={{url_encode(BaseURL)}}"
    - action: waitload
    - action: navigate
      args:
        url: "https://conformance-idp.maiv1.incubator.geant.org/saml2/idp/SSOService.php?spentityid={{url_encode(BaseURL)}}"
    - action: waitload
    - action: screenshot
      args:
        fullpage: "true"
        mkdir: "true"
        to: "{{dir}}/{{filename}}"
  matchers:
    - part: resp
      type: word
      words:
        - "Welcome"
        - "REMOTE_USER = test"
        - "Authenticated"
  extractors:
    - type: kval
      part: extract
      kval:
        - extract
```

Technical solution (nuclei report example)

```
[
  {
    "template-id": "incubatorsamltestheadless",
    "template-path": "/home/brousek/Dokumenty/Incubator/nuclei-templates/saml-headless.yaml",
    "template-encoded": "aWQ6IGluY3ViYXRvcnNhbWx0ZXN0aGVhZGxlc3MKaW5mbzoKICBuYW11OiBJbmn1YmF0b3Igu0FNTC...",
    "info": {
      "name": "Incubator SAML test headless",
      "author": [
        "pavel brousek"
      ],
      "tags": [
        "headless",
        "extractor"
      ],
      "severity": "low"
    },
    "type": "headless",
    "host": "aai-playground.ics.muni.cz",
    "port": "443",
    "scheme": "https",
    "url": "https://aai-playground.ics.muni.cz/simplesaml/module.php/saml/sp/metadata.php/default-sp",
    "path": "/simplesaml/module.php/saml/sp/metadata.php/default-sp",
    "matched-at": "https://conformance-idp.maiv1.incubator.geant.org/saml2/idp/SSOService.php?spentityid=...",
    "response": "<html xmlns=\"http://www.w3.org/1999/xhtml\"><head>\n...",
    "timestamp": "2023-12-11T00:56:04.298944088+01:00",
    "matcher-status": true
  }
]
```


Technical solution

Test IdP

- SimpleSAMLphp v2.1 instance with a configured IdP and a custom 'conformance' module (authentication processing filter) that can modify SAML responses sent to trusted SPs
- Static authentication source (automatic authentication with a sample user)
- It exposes endpoints for manual or programmatic:
 - Defining the next test for the SP (valid response, response without signature, response with an invalid signature, etc.)
 - Provisioning of SP metadata trusted by the Test IdP

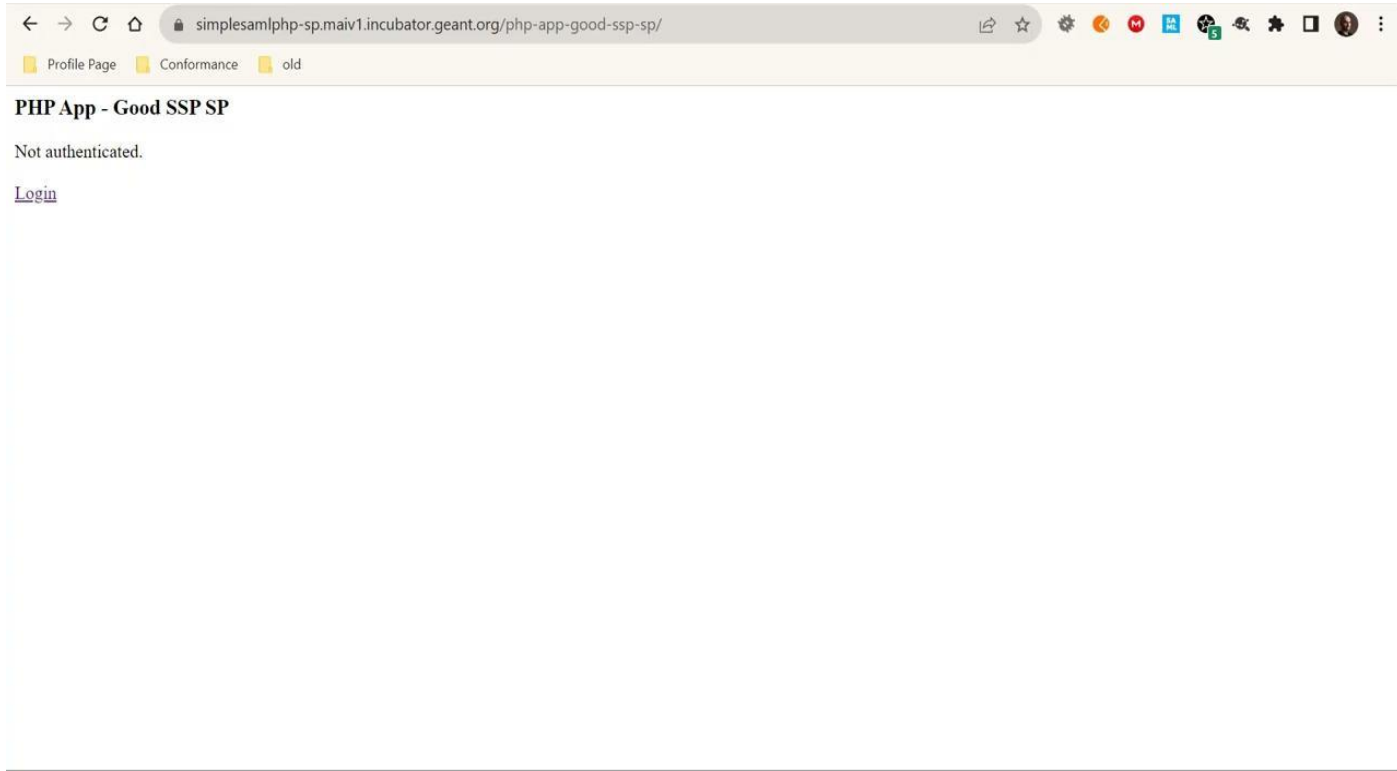
Technical solution

Tested SPs

- Good and bad SP deployments (SPs that validate and SPs that do not validate signatures)
- Two SimpleSAMLphp SPs
 - Bad SP has a hardcoded modification to skip signature checks
- Two Keycloak SPs
 - Bad SP has a configuration option set to not check for signatures
- Shibboleth (TODO)

Technical solution

Manual test of the good SP (validates signature) and bad SP (does not validate it)



The screenshot shows a web browser window with the address bar containing the URL `simplesam/php-sp.maiv1.incubator.geant.org/php-app-good-ssp-sp/`. The browser's address bar also shows navigation icons (back, forward, refresh, home) and a star icon for bookmarks. Below the address bar, there are three yellow tabs labeled "Profile Page", "Conformance", and "old". The main content area of the browser displays the text "PHP App - Good SSP SP" in bold, followed by "Not authenticated." and a blue underlined link labeled "Login".

Discussion

Feedback

What do you think about our solution?

Use cases

Please review and comment:
https://wiki.geant.org/x/_Q5uJw

Open issues - what do you think?

1. Deployment scenario: GÉANT service, NREN service or product?
2. Trust between IdP and services
3. Important and other potential test cases (including exotic ones)



Thank You

www.geant.org



Co-funded by
the European Union