SAML 2.0 Security

Jona, 14. Januar 2016
Bern, 21. Januar 2016

antoine.neuenschwander@csnc.ch
roland.bischofberger@csnc.ch

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Hello

Antoine
Neuenschwander
IT Security Analyst

antoine.neuenschwander@csnc.ch
T: +41 55 214 41 68
F: +41 55 214 41 61

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

www.csnc.ch

Roland Bischofberger
IT Security Analyst

Compass Security Schweiz AG
Werkstrasse 20 | Postfach 2038 | CH-8645 Jona
T: +41 55 214 41 70 | F: +41 55 214 41 61

roland.bischofberger@compass-security.com

Agenda

- Introduction to SAML
- Use-Cases
- Protocol Details

- SAML Attacks
- Demo
- Remediation

Introduction: SAML

WEB

Security

Crossdomain

Assertion

Single Sign-On

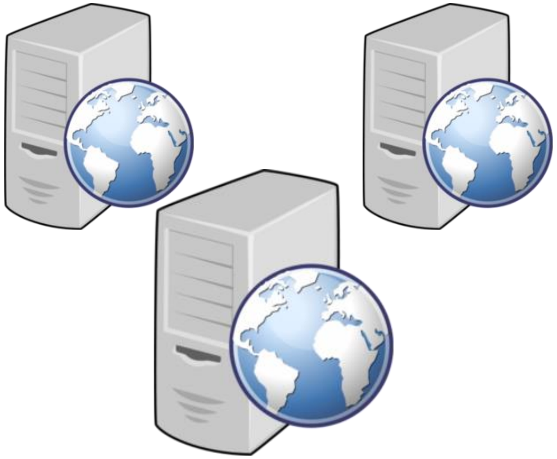
Markup

Such wow!

Language

Introduction: Components

Client / User
Entity that wants to assert a particular identity



Identity Provider (IdP)

- Checks the identity of subjects
- Issues SAML assertions
- Provides the result to SPs

Service Providers (SP)

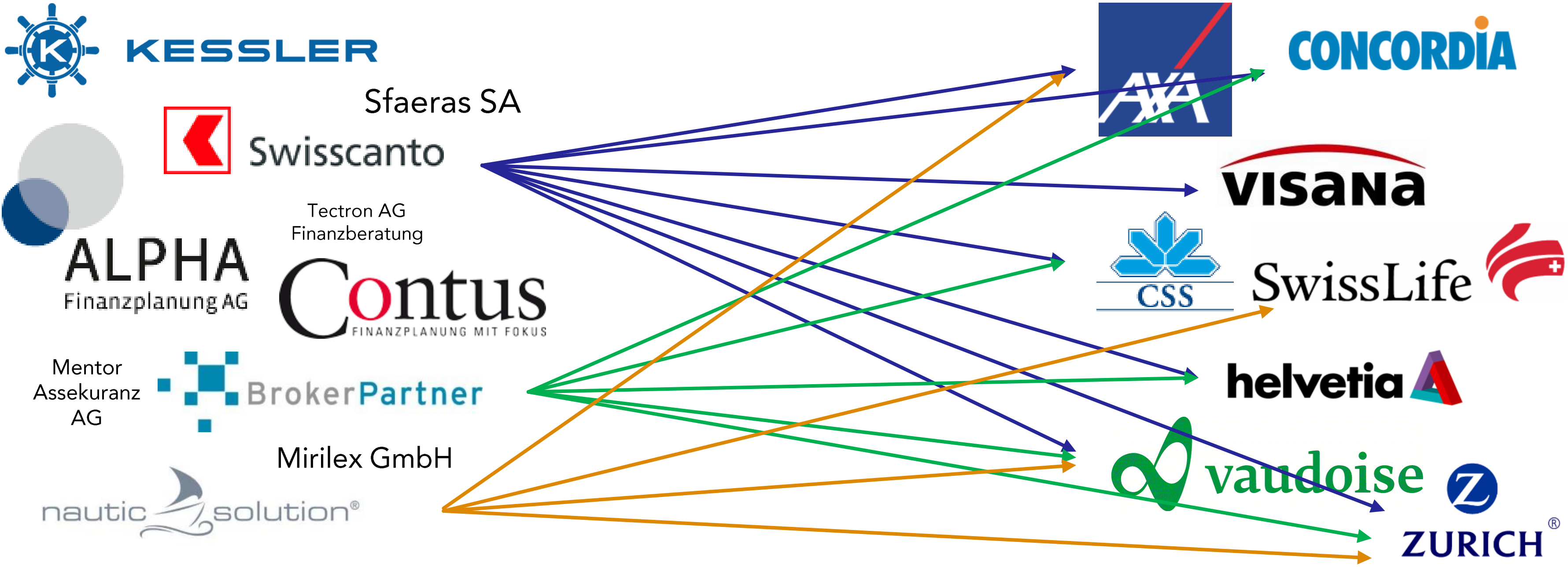
- Provides services to subjects
- Trusts the identification from the IdP based on the assertions it receives

Use-Case: IG B2B BrokerGate

IGB2B for Insurers +Brokers®

941 Brokers,
4146 Users

22 Insurers (13 online)
Broker portal as
Service Providers



Sfaeras SA

Tectron AG
Finanzberatung

Mentor
Assekuranz
AG

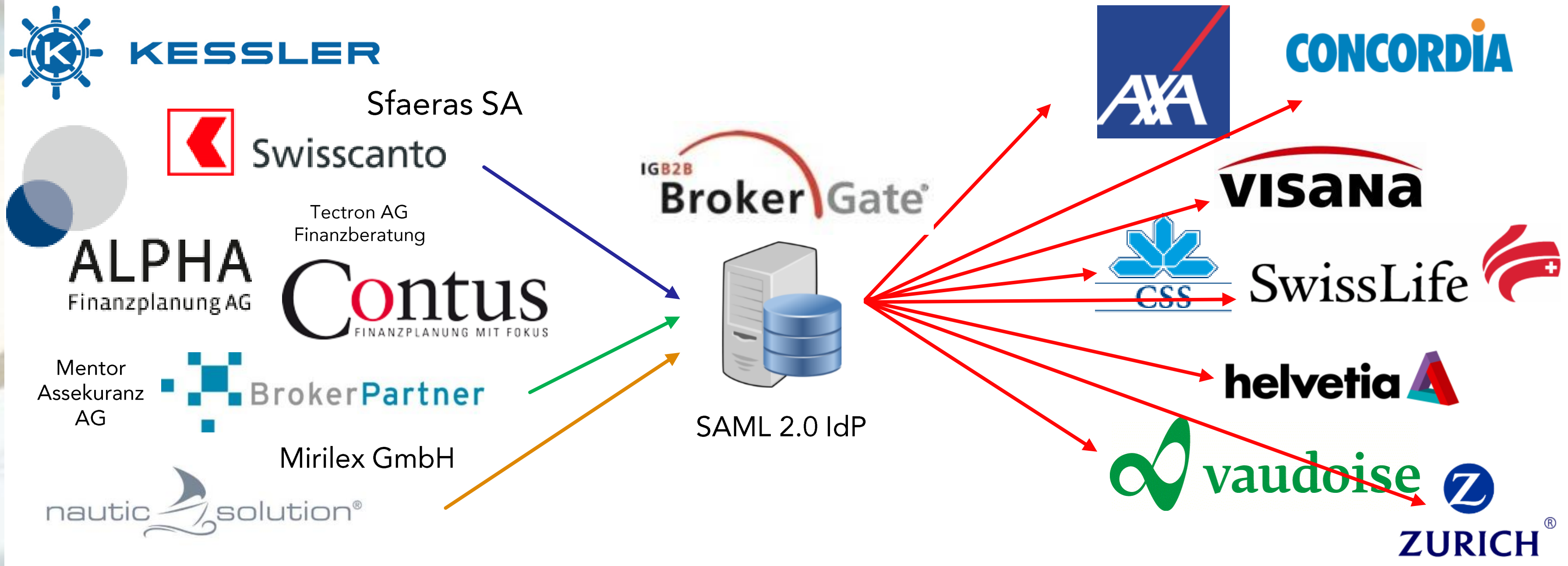
Mirilex GmbH

Use-Case: IG B2B BrokerGate

941 Brokers,
4146 Users

IGB2B for Insurers + Brokers®

22 Insurers (13 online)
Broker portal as
Service Providers



Sfaeras SA

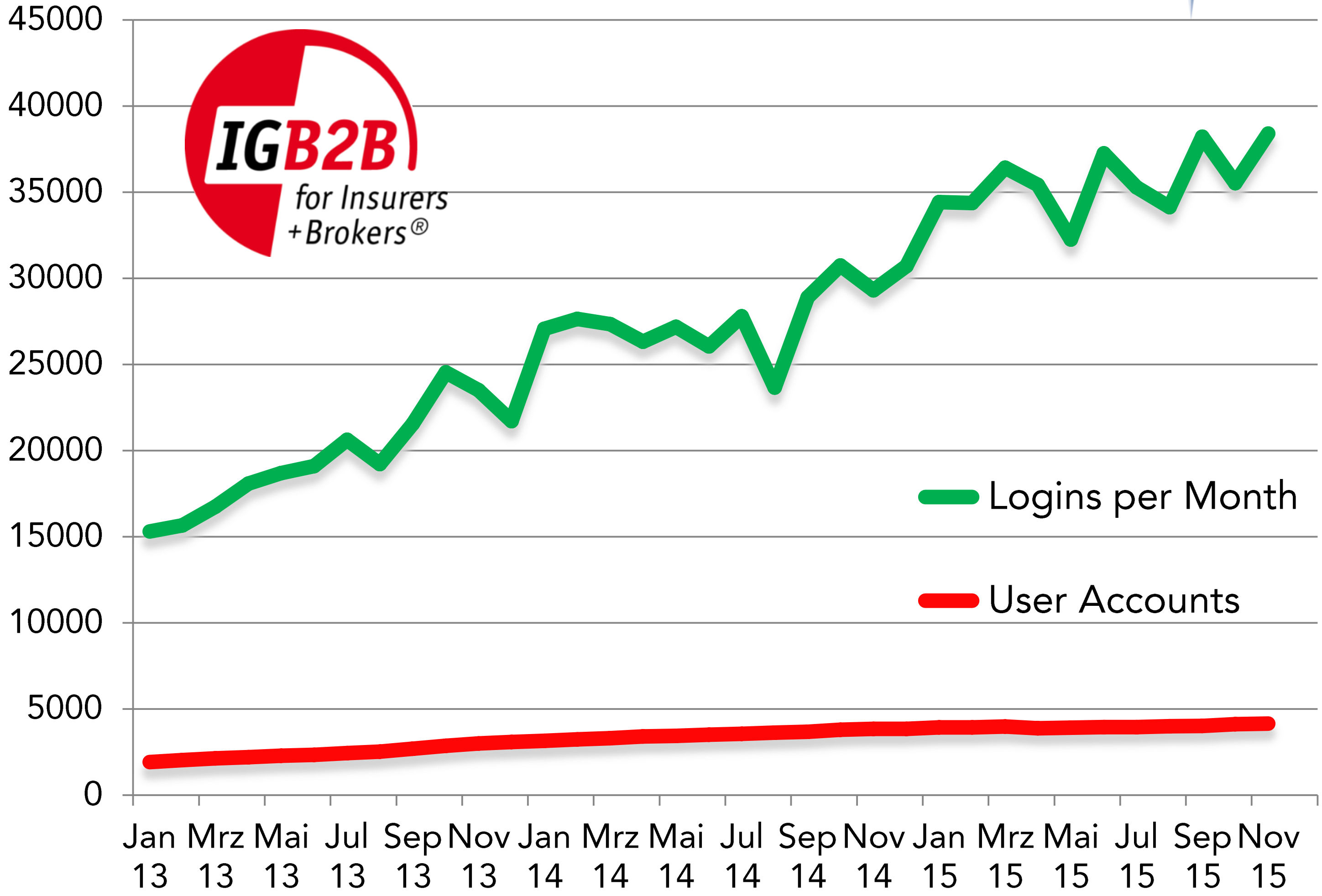
Tectron AG
Finanzberatung

Mentor
Assekuranz
AG

Mirilex GmbH

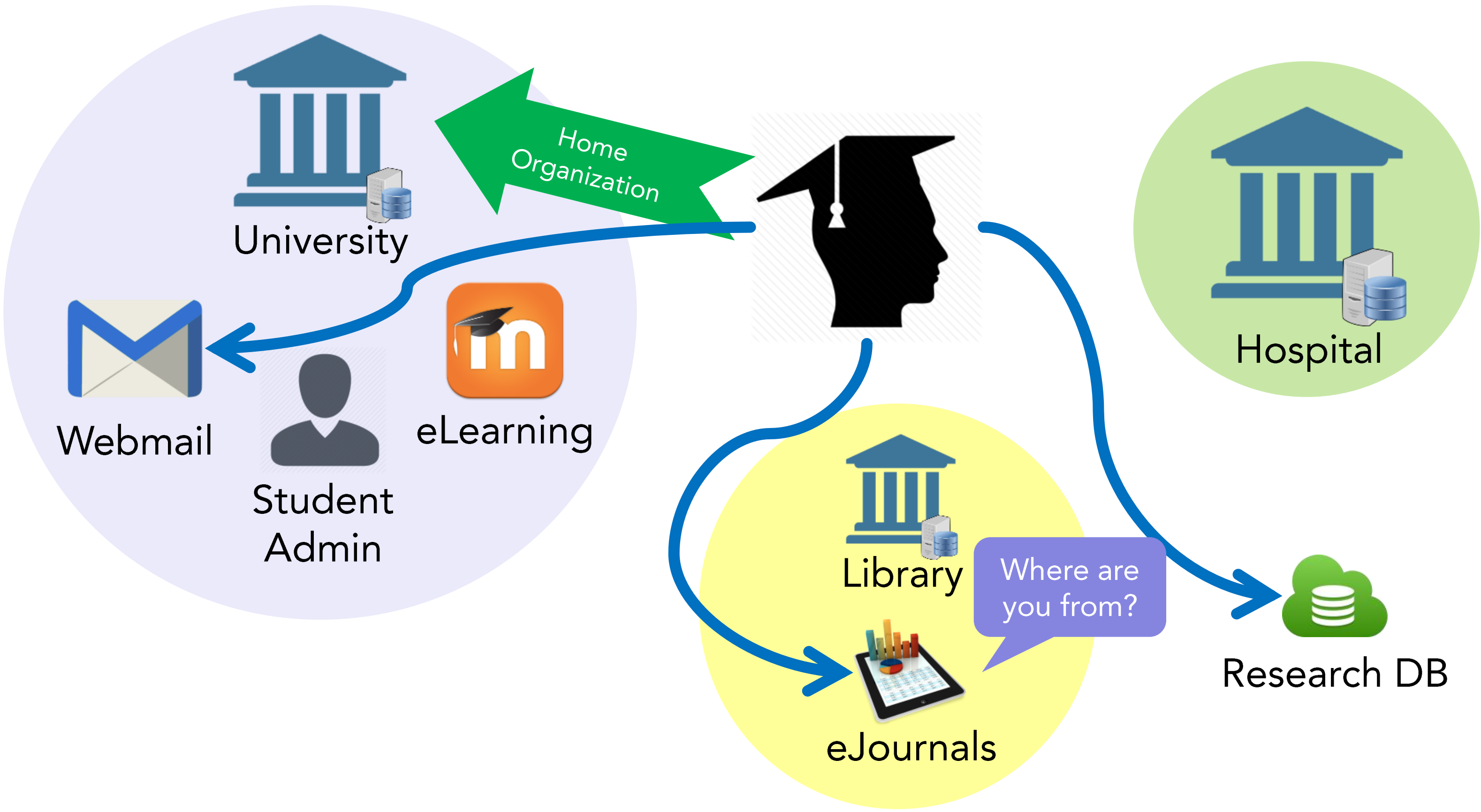
SAML 2.0 IdP

Use-Case: IG B2B BrokerGate



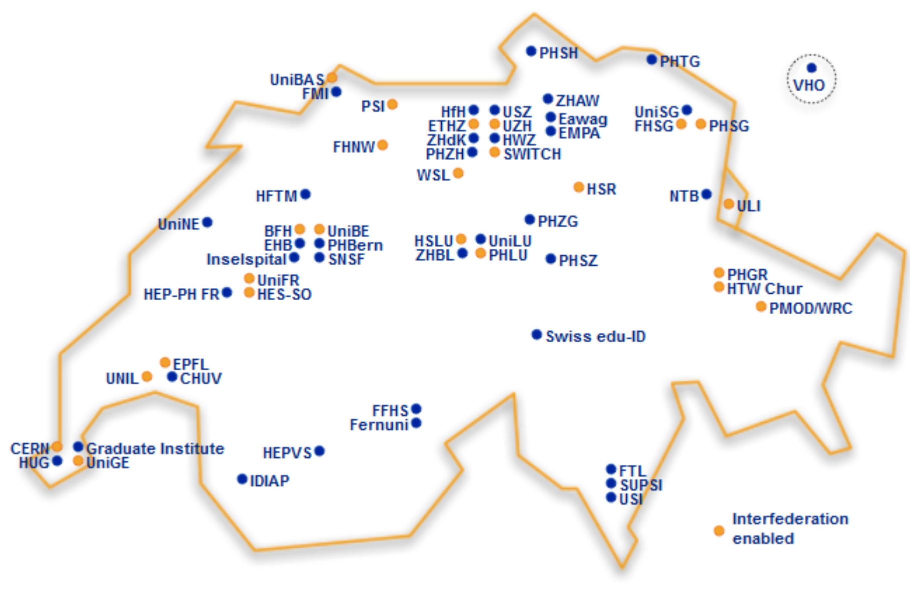
Use-Case: SWITCHaai

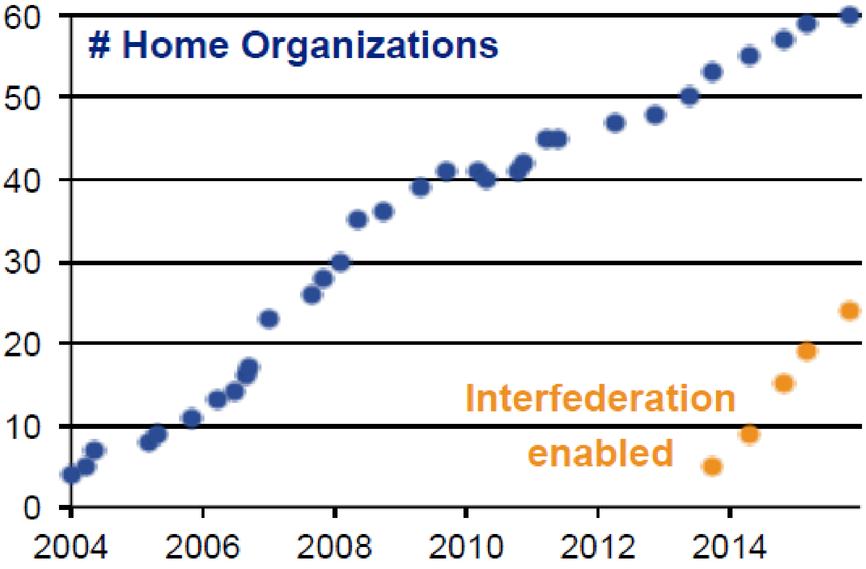
SWITCH



Use-Case: SWITCHaai

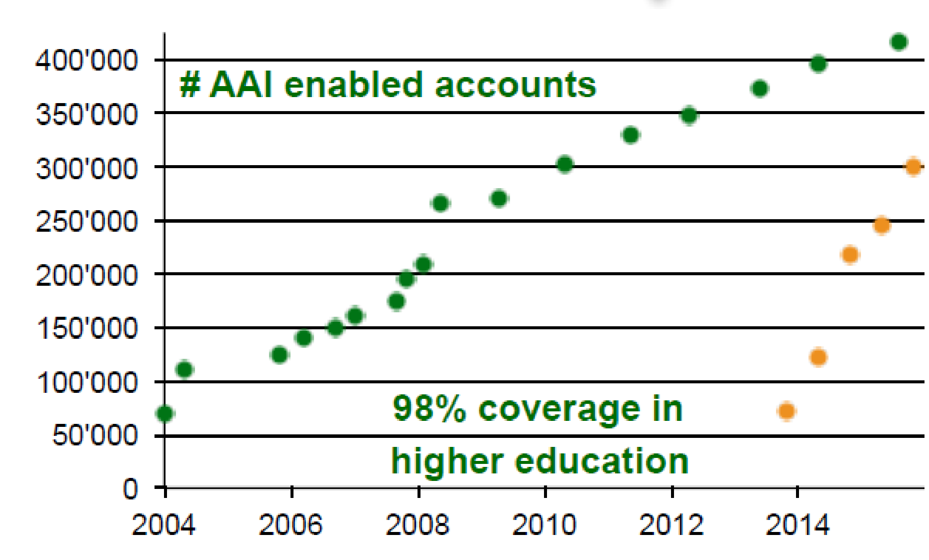
SWITCH

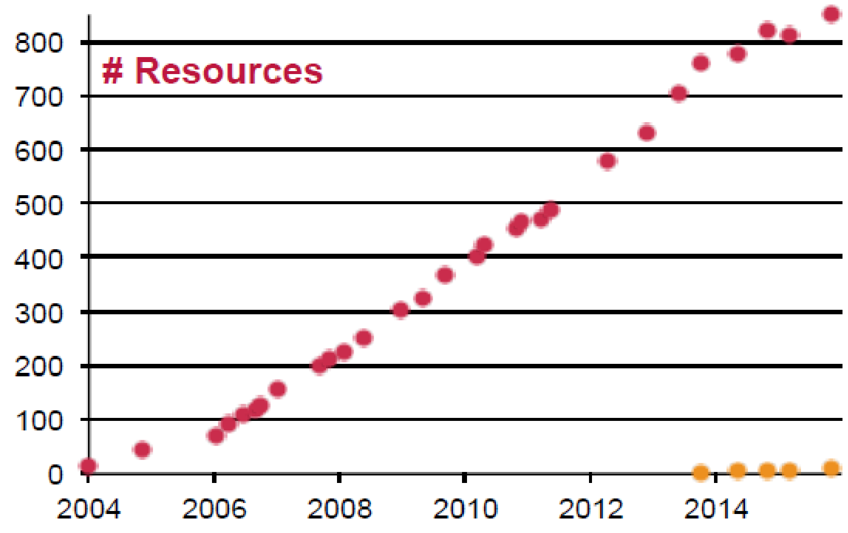




Use-Case: SWITCHaai

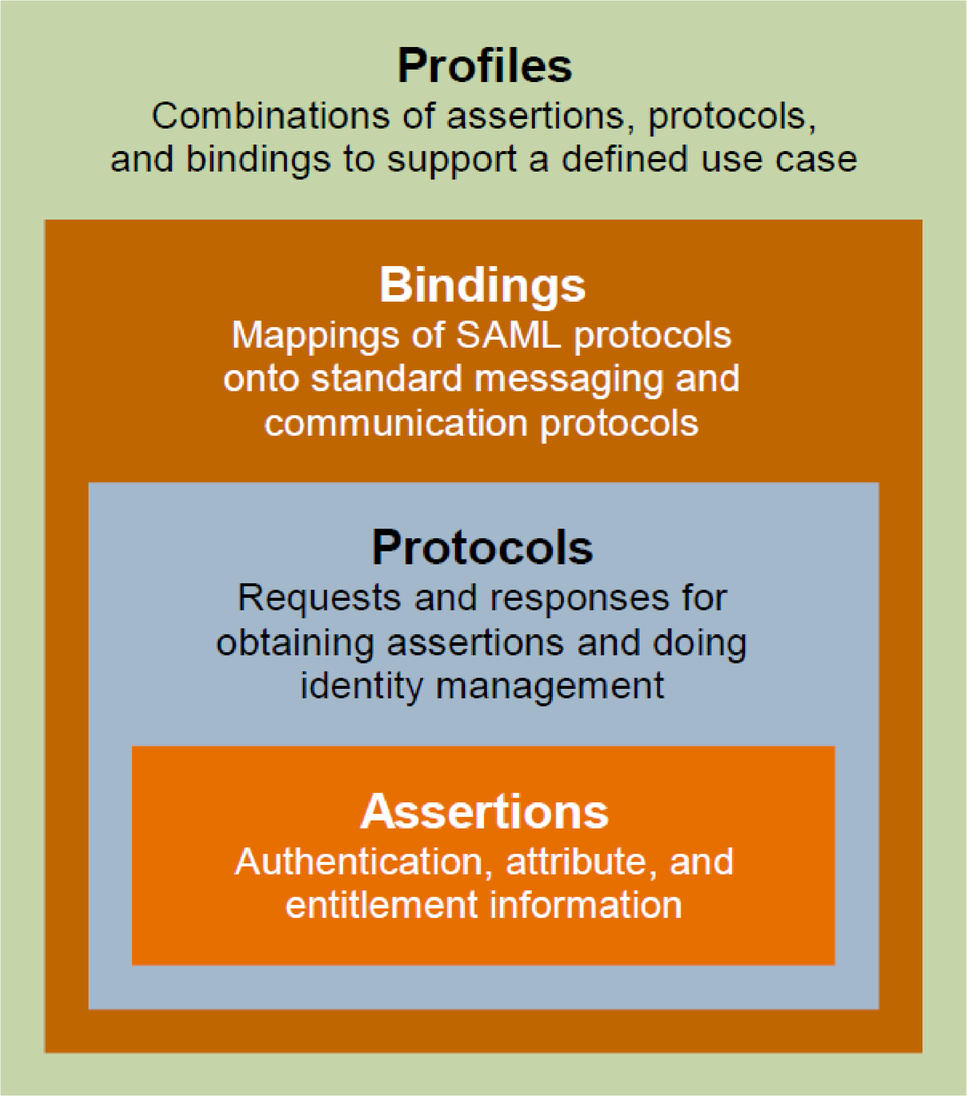
SWITCH





On Average: 50 SAML authentication requests per minute

SAML – The Overall Picture



Profiles
Combinations of assertions, protocols, and bindings to support a defined use case

Bindings
Mappings of SAML protocols onto standard messaging and communication protocols

Protocols
Requests and responses for obtaining assertions and doing identity management

Assertions
Authentication, attribute, and entitlement information

SAML profiles define how the SAML assertions, protocols, and bindings are combined and constrained to provide greater interoperability in particular usage scenarios, e.g. Web Browser SSO Profile

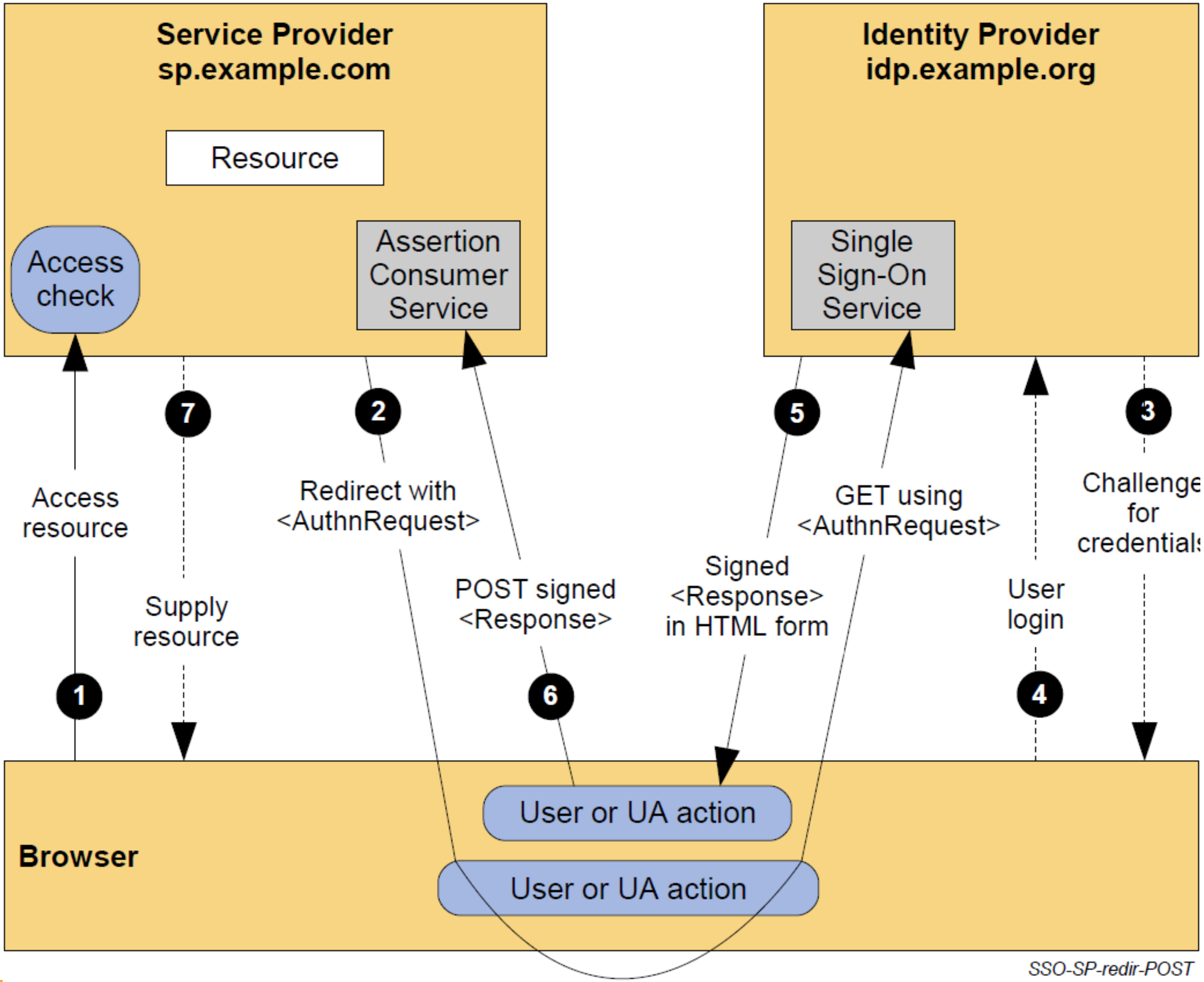
Bindings specify how the various messages can be carried over underlying transport protocols, e.g. HTTP redirect or POST

SAML defines a number of **protocol** messages, e.g.
authentication request, artifact resolution or single logout

With an **Assertion** a IdP confirms to a SP the identity of an subject including the used authentication method

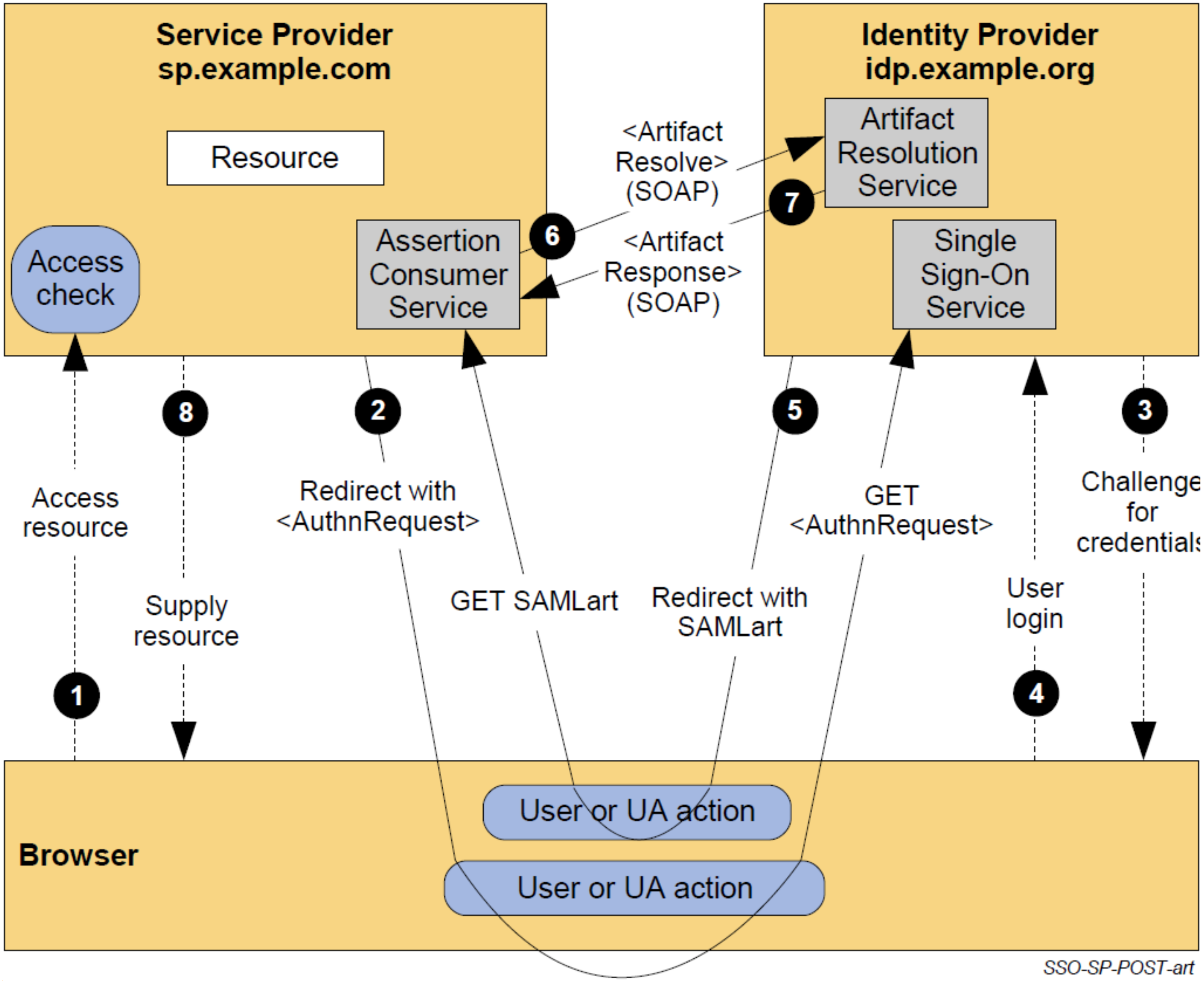
Web Browser SSO Profile

SP-Initiated SSO with Redirect and POST Bindings

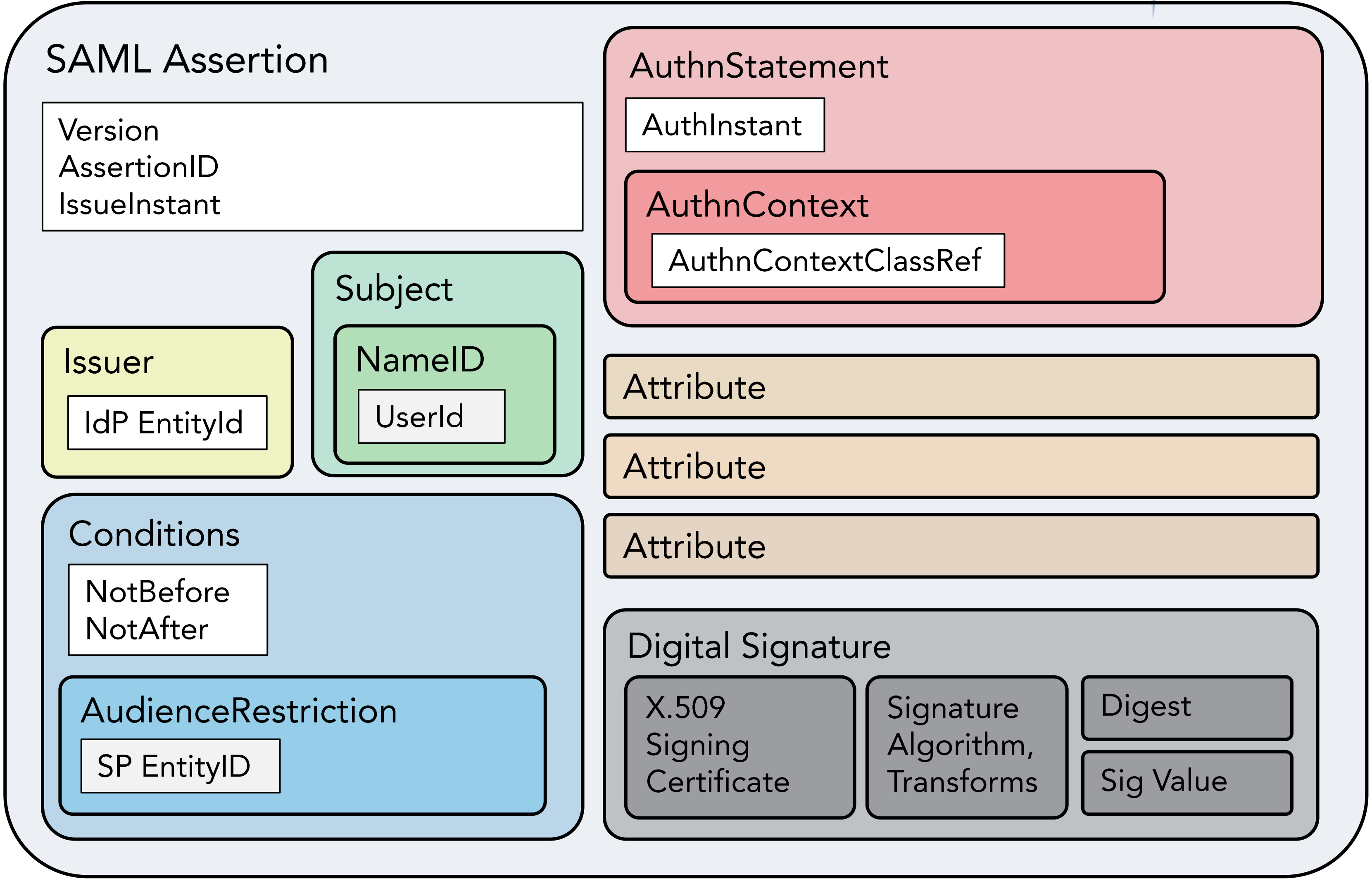


Web Browser SSO Profile (Artifact)

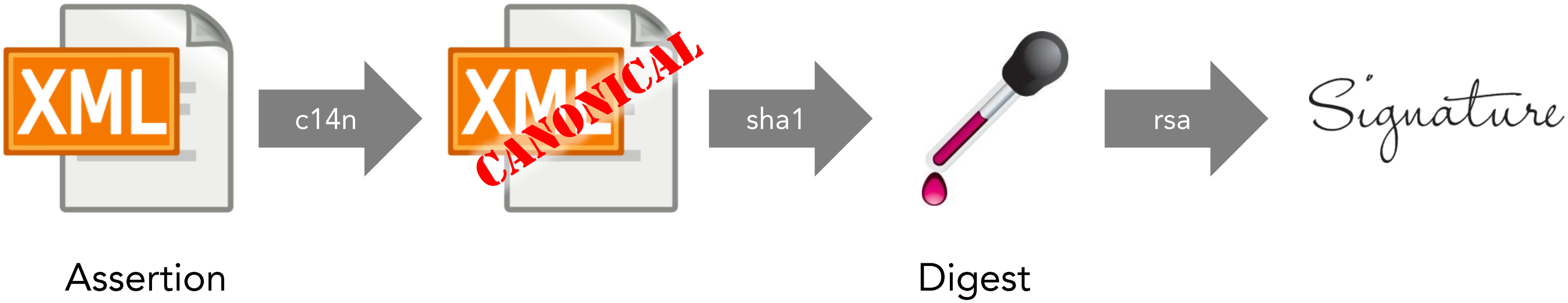
SP-Initiated SSO with POST/Artifact Bindings

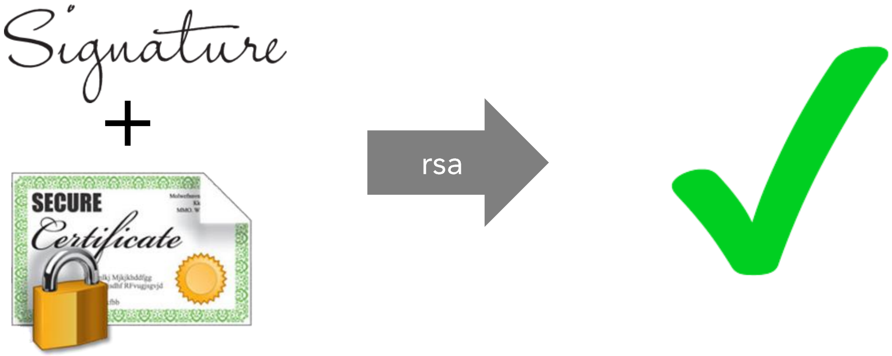


Security Assertion



XML Signature





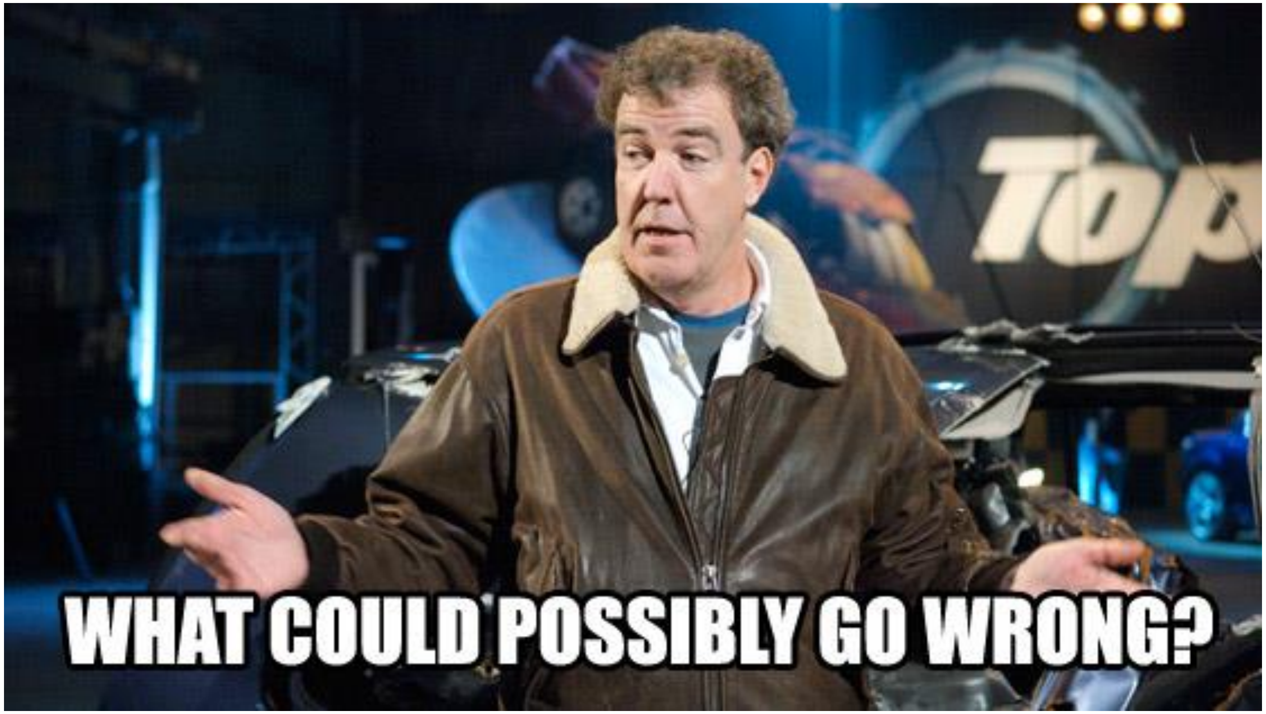
Any questions so far?

CYBER
ATTACKS
AHEAD

SAML Attacks

Technologies

- SAML
- XML Signatures
- X.509 Certificates



SAML Attacks - SAML

- Logout other users due to a guessable Session ID

- Replay a eavesdropped SAML Message

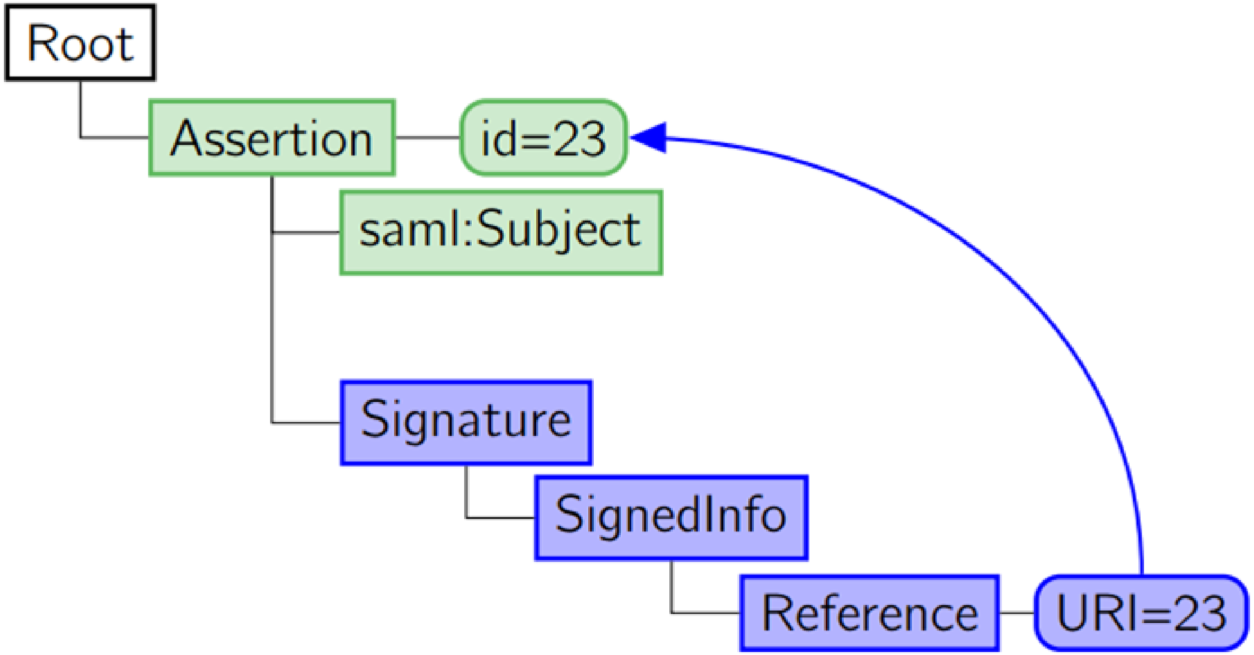
SAML Attacks - XML

- Signature Exclusion (simply delete Signature)

- XML Signature Wrapping

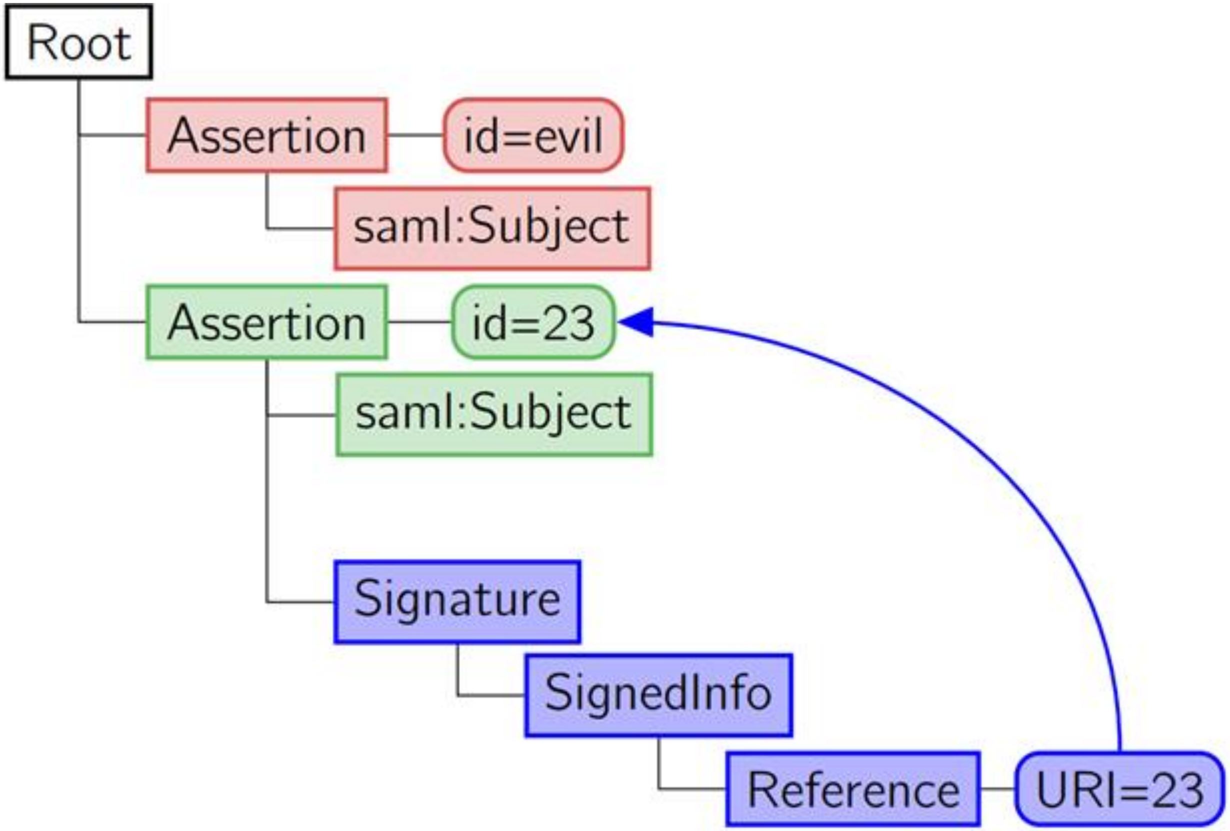
SAML Attacks - XML

Normal SAML Message:



SAML Attacks - XML

Manipulated SAML Message (XSW):



SAML Attacks – Certificate Tampering

Precondition: Certificate is embedded in the message

- «clone» a certificate, generate new key material and sign message
- Same like above but «clone» whole chain
- Use a certificate signed by other official CA
- Use a revoked certificate

INDIANA
OPERATOR DRIVER LICENSE
MR. BEAN
508 E 3RD STREET APT 8
BLOOMINGTON, IN 47401
INDIANA
The Sunshine State
G544-061-73-925-0
DONALD BEAN
2110 BLUE RIDGE DR
TAMPA BAY, FL.30042-0006
DRIVER LICENSE CLASS E
INDIANA
suspended

Demo Exploit

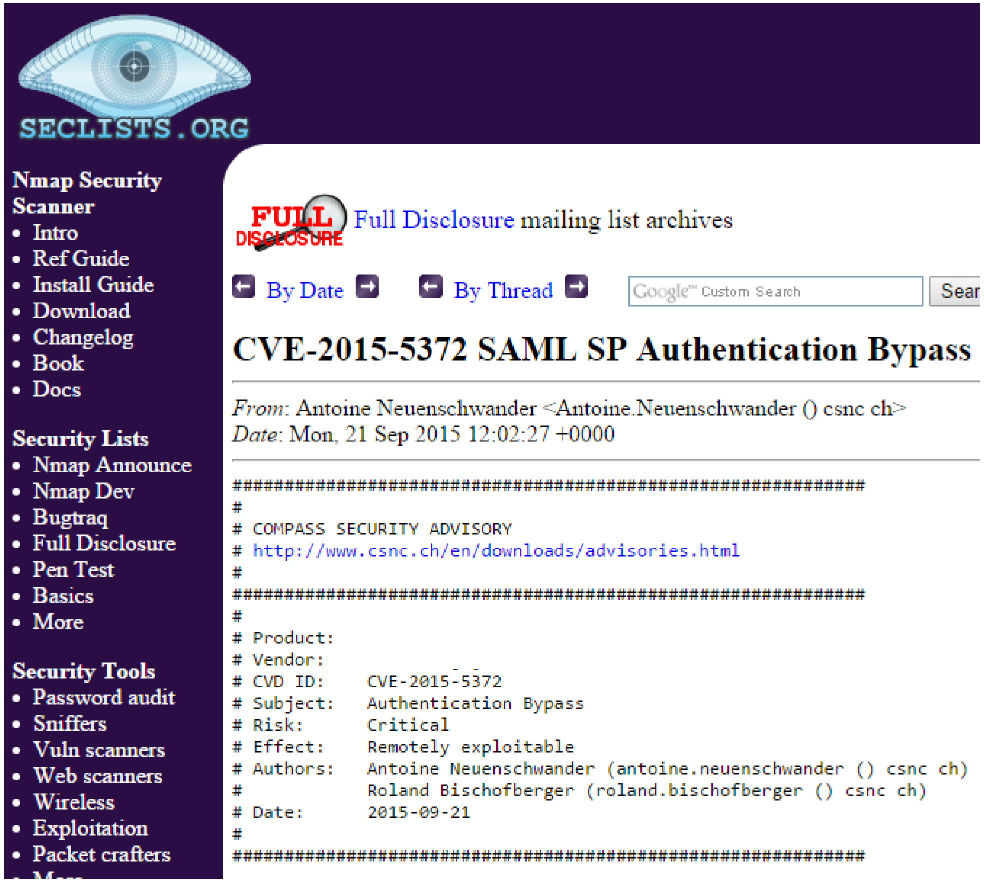
Found in June 2015 by Compass Security

CVE-2015-5372

using **SAML POST-Binding**

not matching all attributes of the X.509 certificate embedded

in the assertion **against the certificate from the identity provider** (IdP)



SECLISTS.ORG

Nmap Security Scanner

- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists

- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools

- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters

FULL DISCLOSURE Full Disclosure mailing list archives

By Date By Thread Google™ Custom Search Sear

CVE-2015-5372 SAML SP Authentication Bypass

From: Antoine Neuenschwander <Antoine.Neuenschwander () csnc ch>
Date: Mon, 21 Sep 2015 12:02:27 +0000

```
##############################################################
#
# COMPASS SECURITY ADVISORY
# http://www.csnc.ch/en/downloads/advisories.html
#
##############################################################
#
# Product:
# Vendor:
# CVD ID:     CVE-2015-5372
# Subject:    Authentication Bypass
# Risk:       Critical
# Effect:     Remotely exploitable
# Authors:    Antoine Neuenschwander (antoine.neuenschwander () csnc ch)
#             Roland Bischofberger (roland.bischofberger () csnc ch)
# Date:       2015-09-21
#
##############################################################
```

Demo Exploit

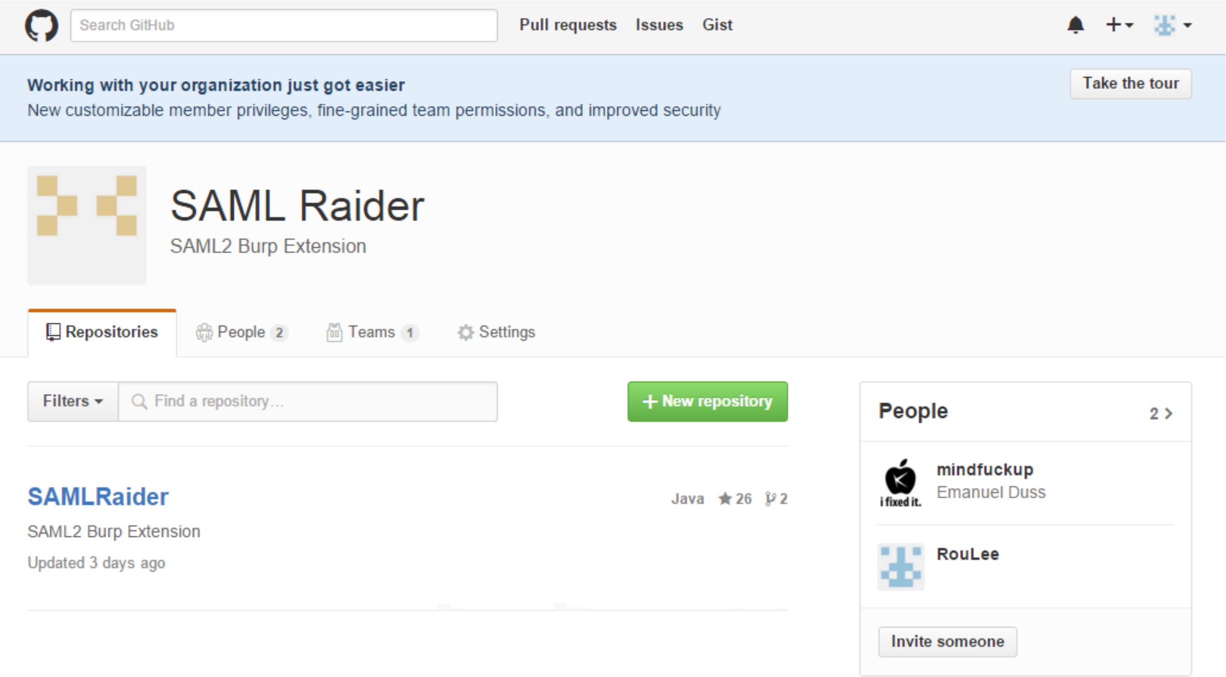
- Intercept Assertion
- Extract certificate
- «clone» certificate, generate new keys
- Alter assertion, e.g. change username to admin
- Remove signature and sign the assertion with the «cloned» certificate

- Problem: Complicated workflow → Assertion is often only valid for some minutes

SAMLRaider

- Solution: SAMLRaider Extension for Burp
  - Developed as a Bachelor thesis
  - In cooperation with Compass Security

https://github.com/SAMLRaider/SAMLRaider



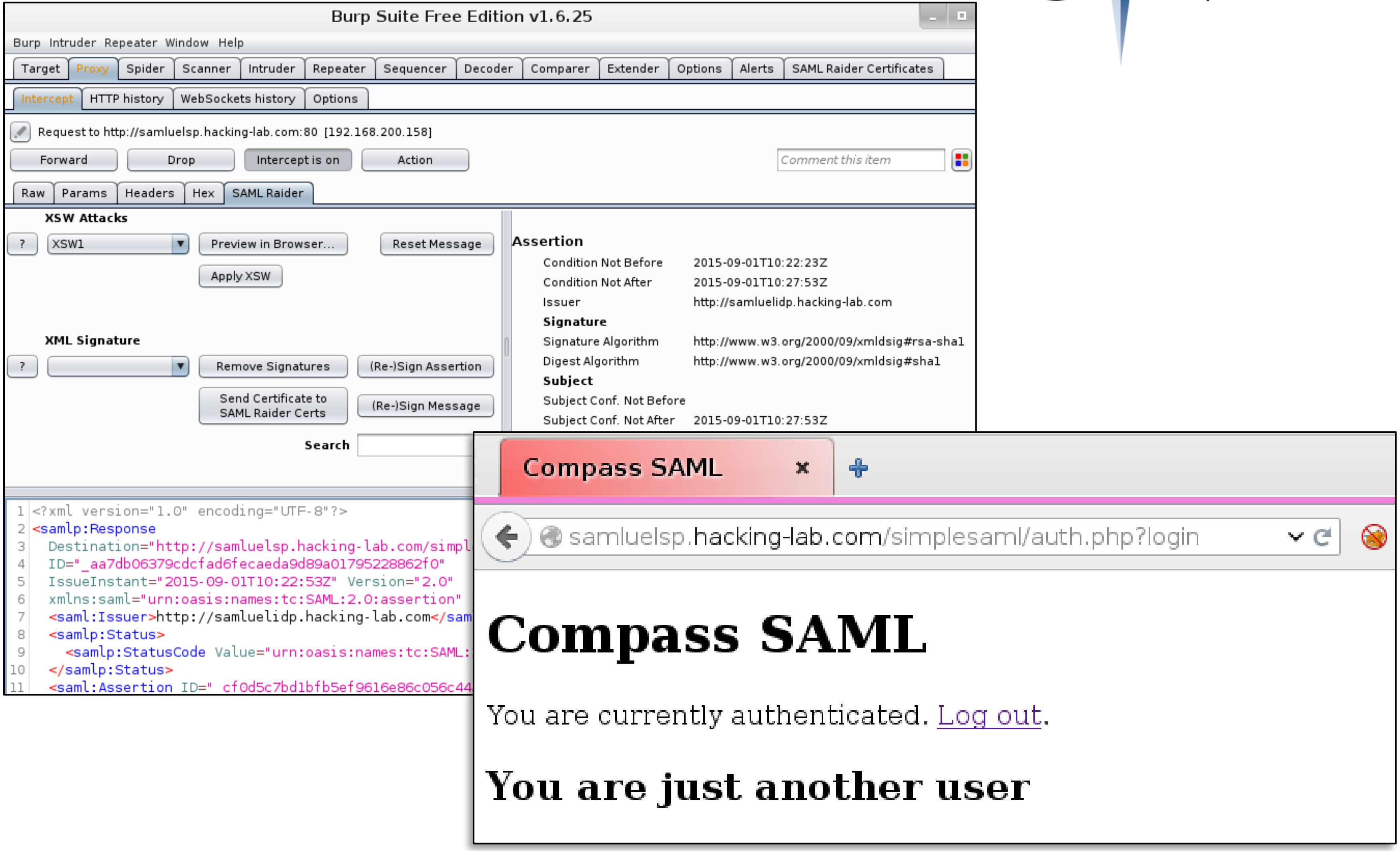
Working with your organization just got easier
New customizable member privileges, fine-grained team permissions, and improved security

SAML Raider

SAML2 Burp Extension

SAMLRaider
SAML2 Burp Extension
Updated 3 days ago

Demo Exploit


Burp Suite Free Edition v1.6.25
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts SAML Raider Certificates
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex SAML Raider
XSW Attacks
?
XSW1
Preview in Browser...
Reset Message
Apply XSW
XML Signature
?
Remove Signatures
(Re-)Sign Assertion
Send Certificate to SAML Raider Certs
(Re-)Sign Message
Search
Compass SAML
×

Request to http://samluelsp.hacking-lab.com:80 [192.168.200.158]

Assertion

Condition Not Before	2015-09-01T10:22:23Z
Condition Not After	2015-09-01T10:27:53Z
Issuer	http://samluelidp.hacking-lab.com
Signature	
Signature Algorithm	http://www.w3.org/2000/09/xmldsig#rsa-sha1
Digest Algorithm	http://www.w3.org/2000/09/xmldsig#sha1
Subject	
Subject Conf. Not Before	
Subject Conf. Not After	2015-09-01T10:27:53Z

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response
  Destination="http://samluelsp.hacking-lab.com/simpl
  ID="_aa7db06379cdcfad6fecaeda9d89a01795228862f0"
  IssueInstant="2015-09-01T10:22:53Z" Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  <saml:Issuer>http://samluelidp.hacking-lab.com</sam
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:
  </samlp:Status>
  <saml:Assertion ID=" cf0d5c7bd1bfb5ef9616e86c056c44
```

samluelsp.hacking-lab.com/simplesaml/auth.php?login

Compass SAML

You are currently authenticated. Log out.

You are just another user

SAML Attacks - Mitigation

- Use artifact binding (no content on client)
- If POST-binding is necessary:
  - Use encrypted messages

  - Only process signed XML tree (delete other content)
  - Use key material on the SP or IdP and not embedded keys
  - Add a random number to every successfully verified signed element
    - Check this random number in next steps
    - This needs a modified XML Schema

Questions?

Subscribers
manipulation
potentially
executed
automates
manually
Switzerland
Display
Bischofberger
supports
Single
penetration
Identity
assertions
Manipulating
Assertion
illustrates
graph
illustrated
consuming
HackingLab
tasks
testing
period
design
partner
errors
random
red
signatures
riskless
fields
copied
Management
für
certificates
Profile
Clone
changes
Sent
messages
3
Execute
Technik
Emanuel
vulnerabilities
common
Undo
bachelor
SOAP
deploy
Manipulate
browser
Supported
SAML
sign
XSW
SP
factor
Collaboration
technology
holders
case
Provider
IdP
le
eight
prone
project
1
Manual
decode
Perform
Therefore
Service
example
Bindings
core
6
secured
error
infrastructures
based
predefined
Webbrowser
Applied
attack
XML
flow
SignOn
Raider
POST
Send
thank
1
tester
support
created
valid
message
within
using
Profiles
new
used
Suite
Signature
X509
needs
Security
Burp
manage
HSR
Schweiz
Web
environment
Wrapping
license
nice
Hochschule
AG
solutions
extension
Redirect
Remove
keys
Rapperswil
standard
functionalities
highlighting
Preview
developed
possible
2
advisor
Services
Roland
Compass
Encode
generated
test
thesis
Edit
two
certificate
attacks
keypair
able
field
contains
Sciences
Token
Steps
short
chance
Binding
Duss
federation
arbitrary
University
received
widely
students
Software
increases
necessary
called
intercepts
point
syntax
Vulnerability