Compass Security

[The ICT-Security Experts]

SAML 2.0

[Beer Talk – Berlin – 2/16/2016]

Stephan Sekula

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

May I introduce myself?

Stephan Sekula

- With Compass since August 2013
- Career: Studied Computer Science, worked in research, now gathering practical experience
- Expertise
  - Web Application Security
  - Mobile Security
  - Social Engineering basics (from Psychology minor)

Hobbies

- Cooking & baking
- Bicycling
- Climbing
- IT-Security

Agenda

- Introduction to SAML
- Use-Cases
- Protocol Details

- SAML Attacks
- Demo Exploit
- Remediation

WEB

Security

Crossdomain

Assertion

Markup

Single Sign-On

Such wow!

Language

Introduction to SAML – Components

Client/User

- Wants to authenticate (i.e., assert a particular identity)

Service Provider (SP)

- Provides a certain service the client wants to use
- Trusts certain Identity Providers (and their Assertions)
  - SP ascertains a user's identity based on IdP's Assertion

Identity Provider (IdP)

- Checks the clients' identity
- Issues SAML Assertions ("proof of identity")
  - Communicates these Assertions to the Service Provider

Agenda

- Introduction to SAML
- Use-Cases
- Protocol Details

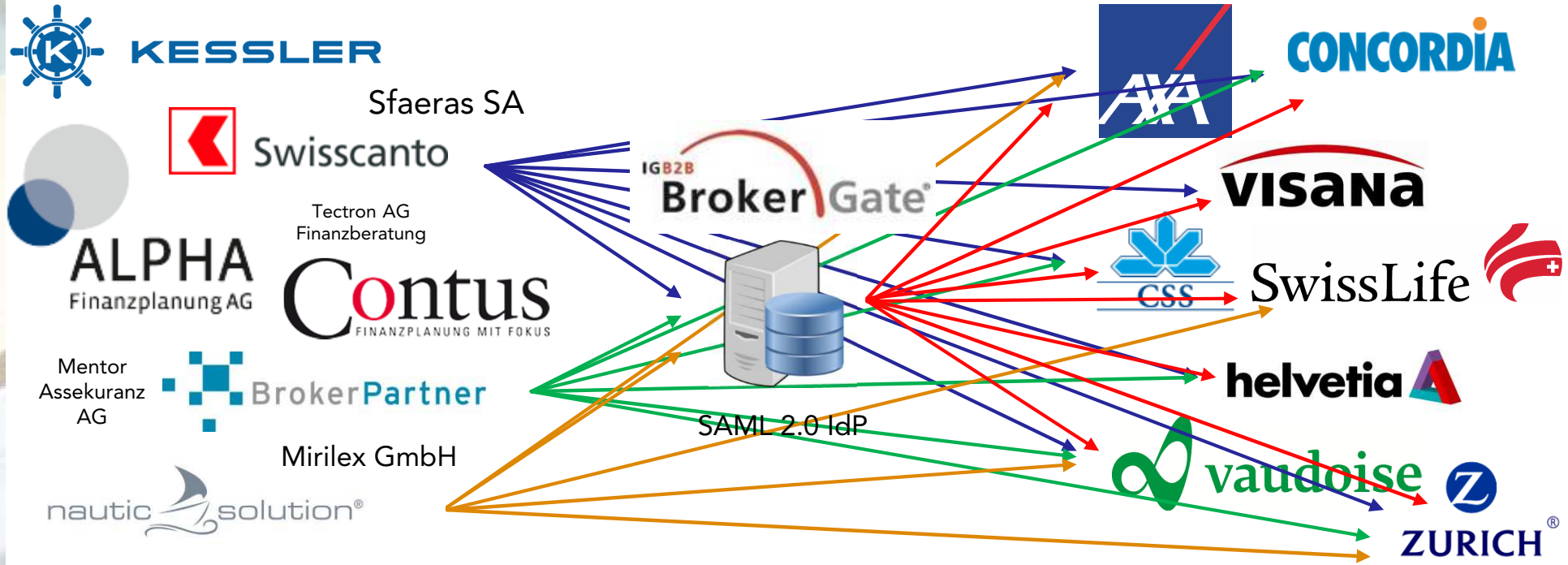
- SAML Attacks
- Demo Exploit
- Remediation

Use-Case – IG B2B BrokerGate

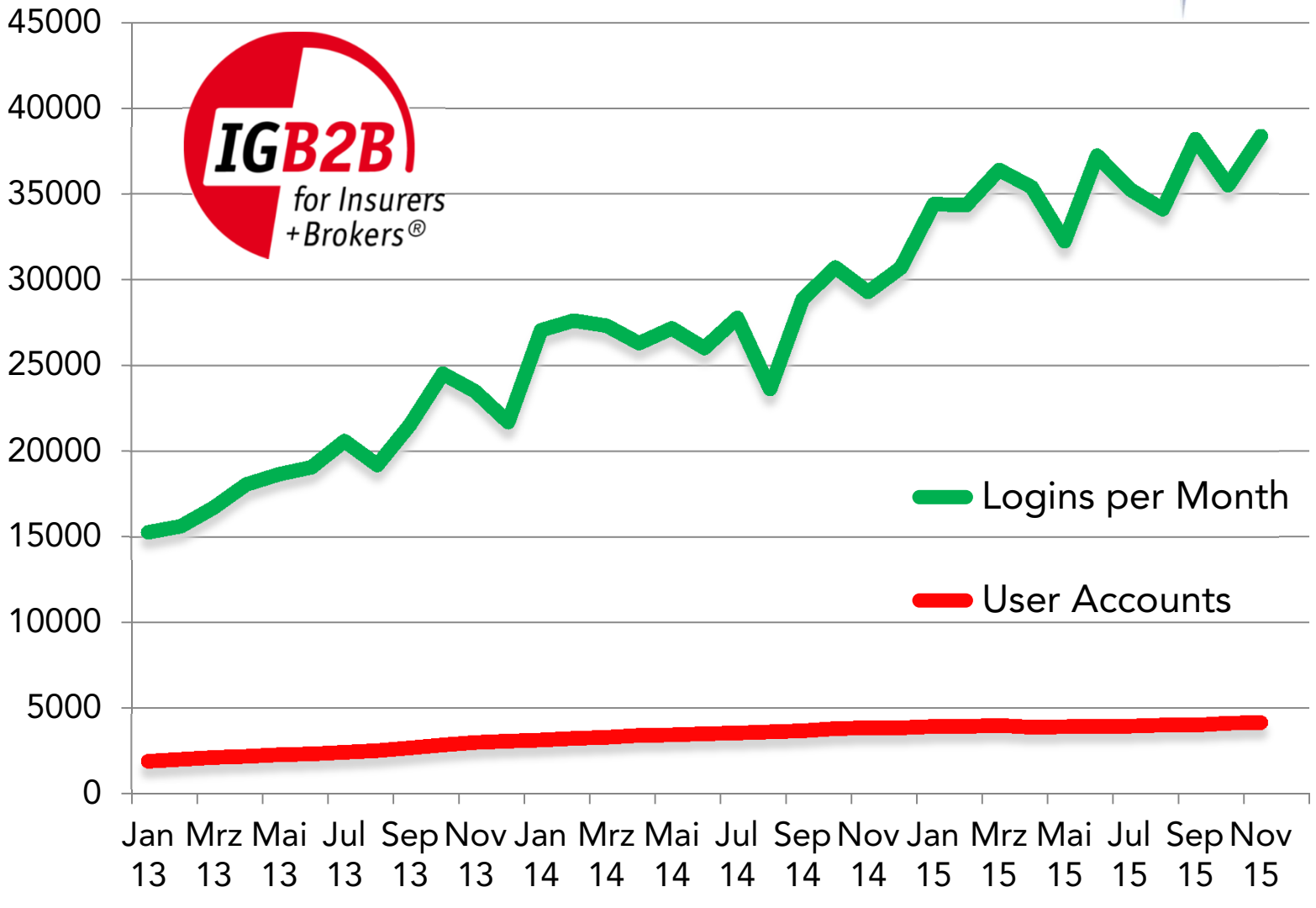
941 Brokers
4146 Users

IGB2B for Insurers +Brokers®

22 Insurances
(Service Providers)

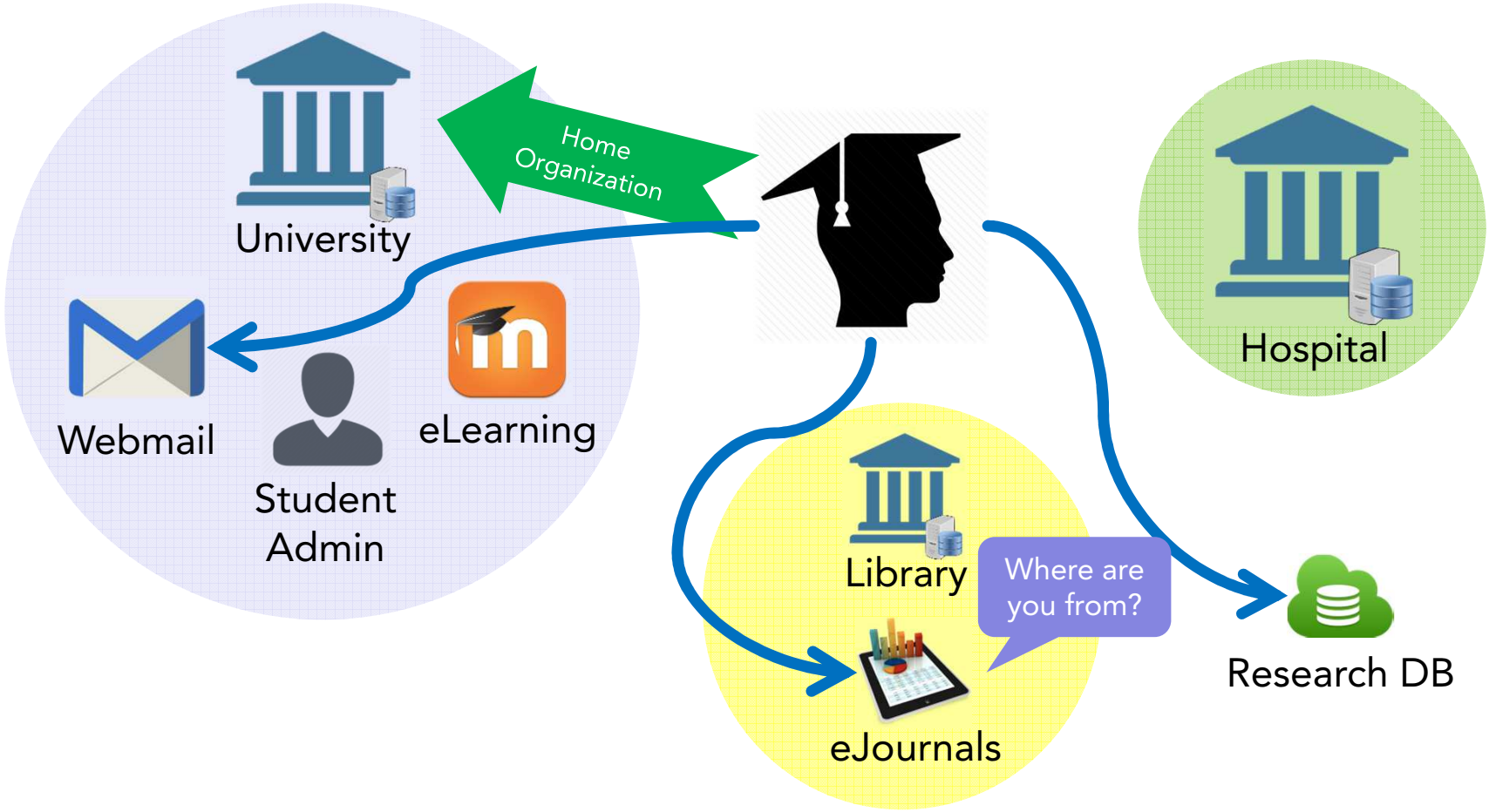


Use-Case – IG B2B BrokerGate



Use-Case – SWITCHaai

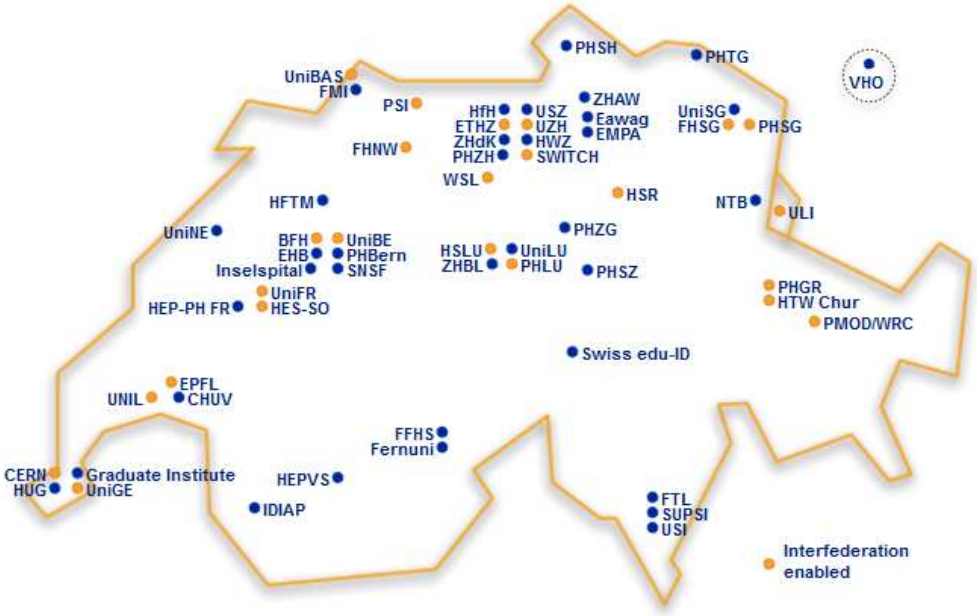
SWITCH

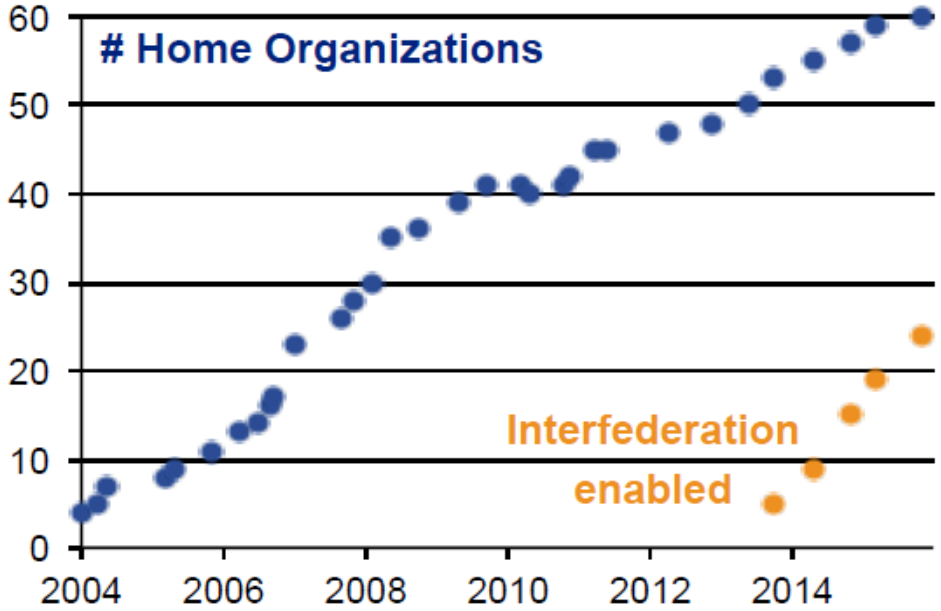


aai: Authentication and Authorization Infrastructure

Use-Case – SWITCHaai

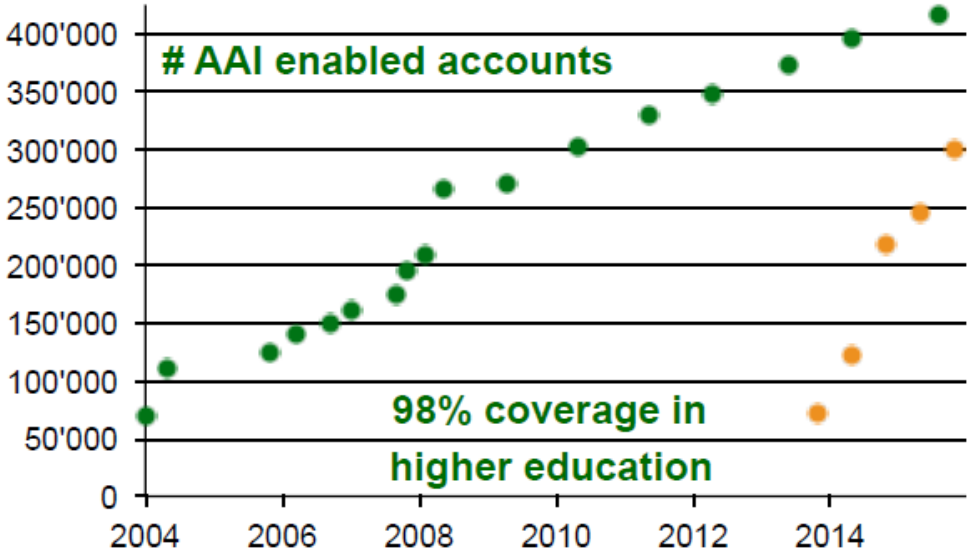
SWITCH

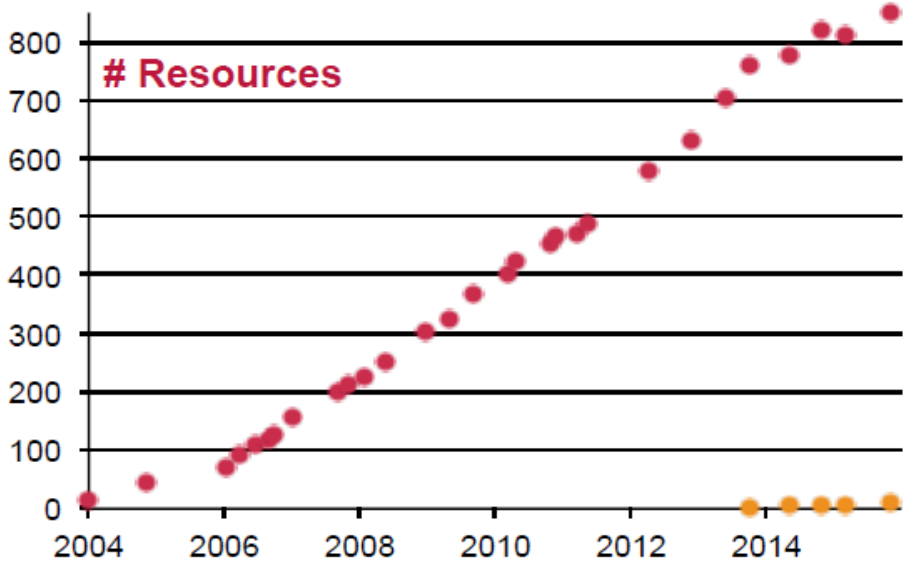




Use-Case – SWITCHaai

SWITCH





On average:
50 SAML authentication requests per second

Agenda

- Introduction to SAML
- Use-Cases
- Protocol Details

- SAML Attacks
- Demo Exploit
- Remediation

SAML – Protocol Details

SAML Profiles are a combination of SAML Assertions, Protocols, and Bindings for particular use cases, e.g., "Web Browser SSO Profile"

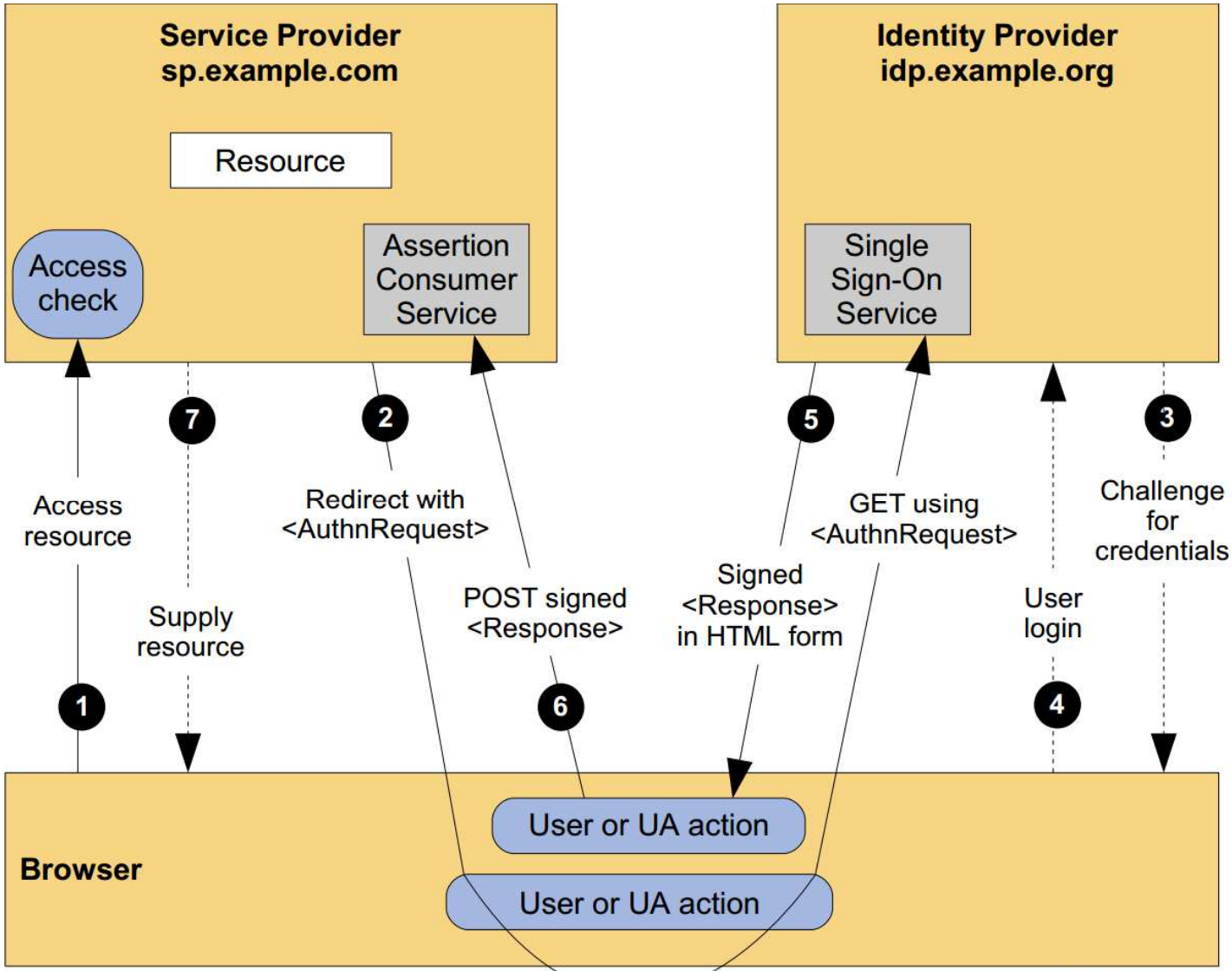
Bindings specify how the various messages are carried over underlying transport protocols, e.g., HTTP redirect or POST

SAML defines a number of **Protocol** messages, e.g., "authentication request", "artifact resolution", and "single logout"

An IdP uses **Assertions** to convey a subject's identity (including the used authentication method) to an SP

Web Browser SSO Profile (Redirect/POST)

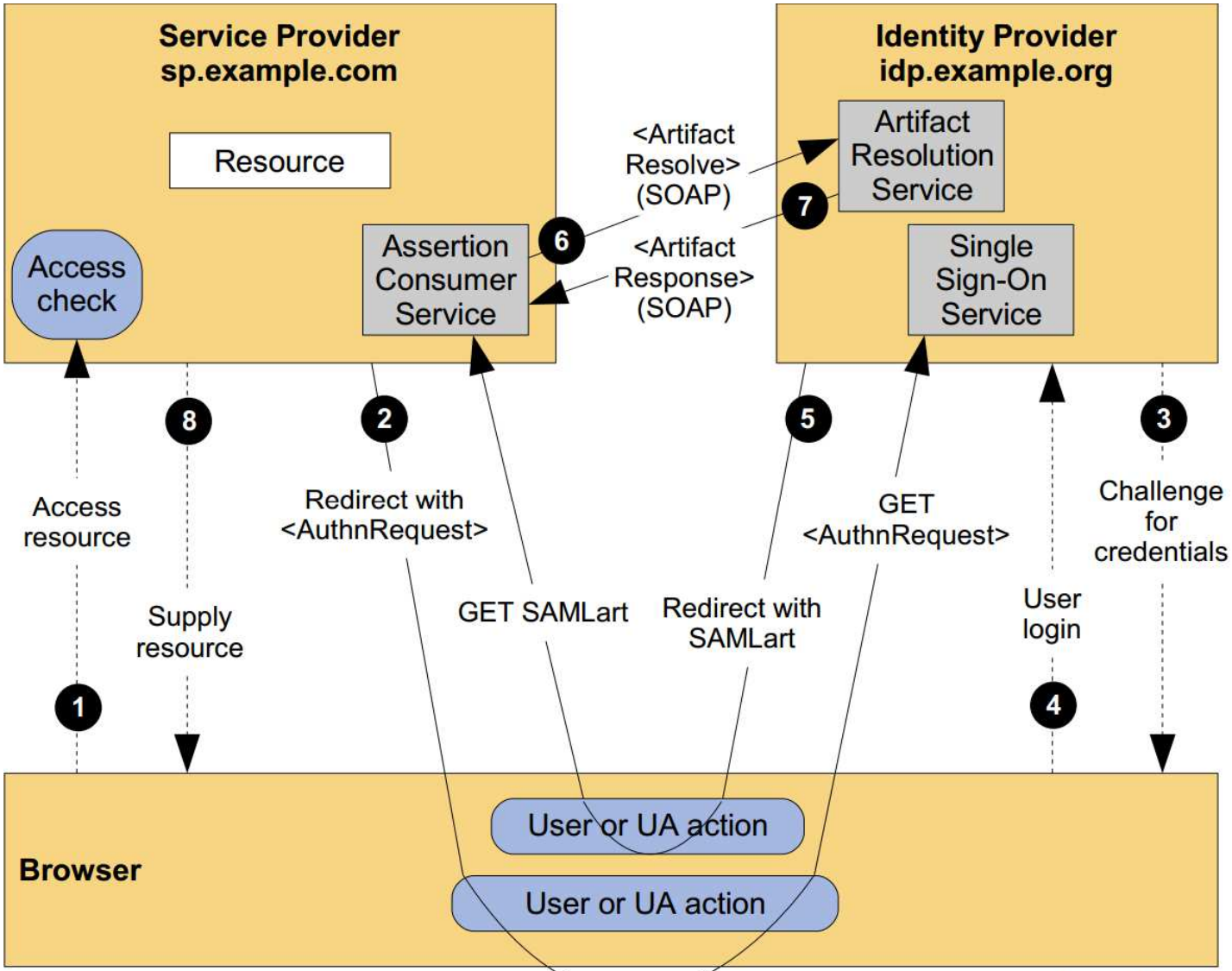
SP-Initiated SSO with Redirect and POST Bindings



Source: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf

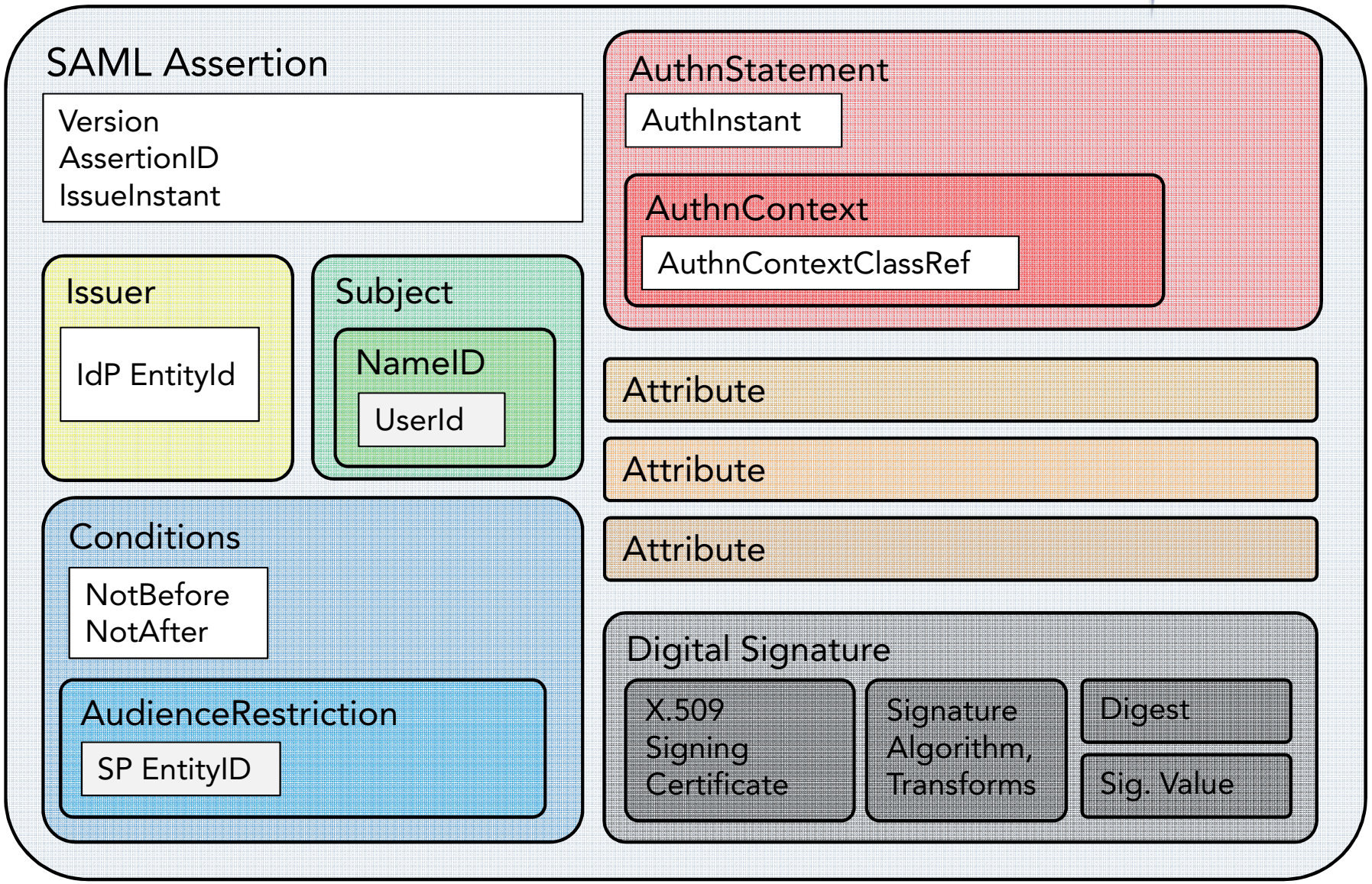
Web Browser SSO Profile (Artifact)

SP-Initiated SSO with POST/Artifact Bindings



Source: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf

SAML Assertion



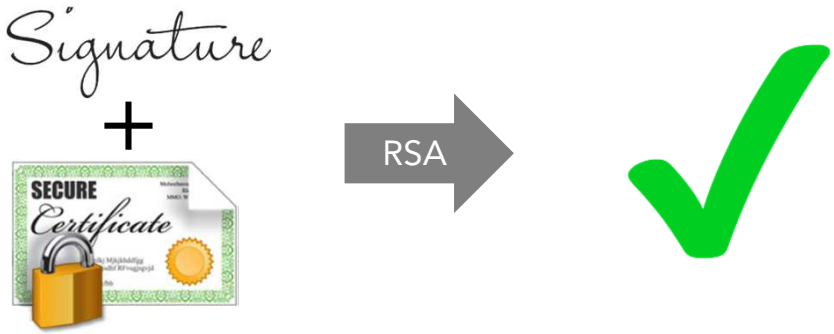
XML Signature

Assertion Signing:

Assertion

Digest

Signature Verification:



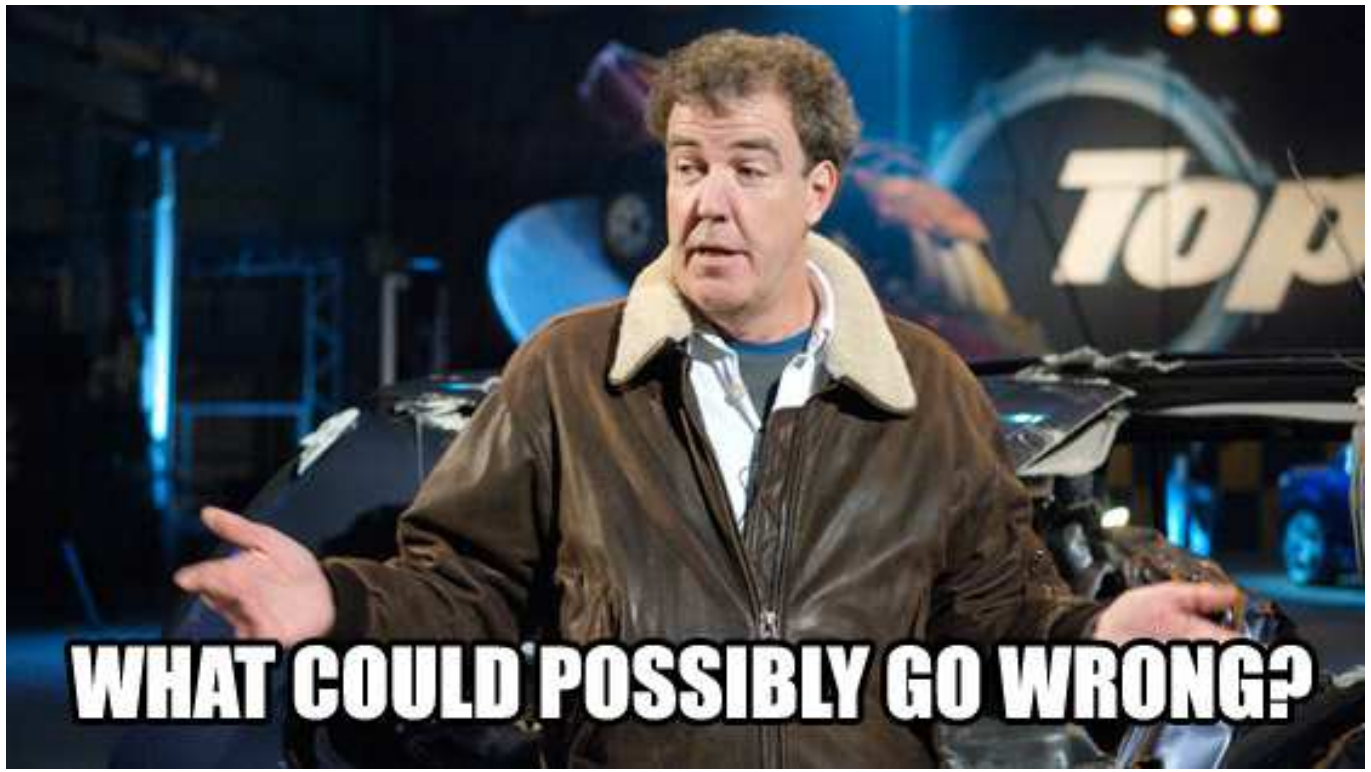
Agenda

- Introduction to SAML
- Use-Cases
- Protocol Details

- SAML Attacks
- Demo Exploit
- Remediation

Technologies

- SAML
- XML Signatures
- X.509 Certificates



SAML Attacks – SAML

Guessable Session ID

- Attacker is able to logout other users

Eavesdropped SAML Message

- Attacker captures SAML message
- Attacker replays captured message

SAML Attacks – XML

Signature Exclusion

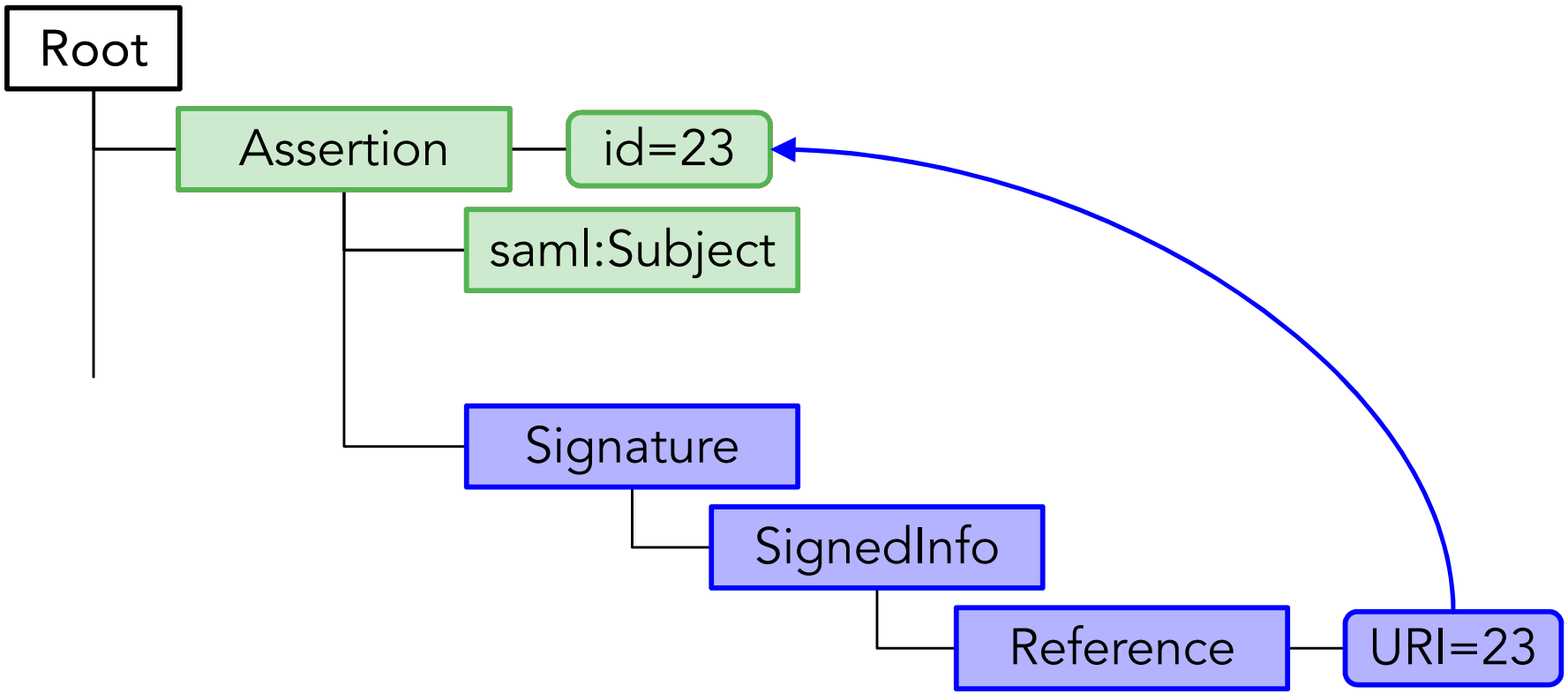
- XML signature is deleted

XML Signature Wrapping (XSW)

- Manipulating XML contents while keeping the signature valid

SAML Attacks – Signature Wrapping

SAML Message (XSW)



SAML Attacks – Certificate Tampering

Precondition: Certificate is embedded in the message

Types of attacks:

- "Clone" a certificate, generate new key material, sign message
- Same as above, but "clone" entire chain
- Use a certificate signed by another official CA
- Use a revoked certificate

Agenda

- Introduction to SAML
- Use-Cases
- Protocol Details

- SAML Attacks
- Demo Exploit
- Remediation

Demo Exploit

CVE-2015-5372 SAML SP Authentication Bypass

- Discovered in June 2015 by Compass Security
- Preconditions:
  - SAML POST Binding is used
  - SP does not validate all attributes contained in X.509 certificate
  - SP uses certificate contained in the SAML message (not the one in its certificate store)

Demo Exploit

CVE-2015-5372 SAML SP Authentication Bypass

```
#################################################################
#
# COMPASS SECURITY ADVISORY
# http://www.csnc.ch/en/downloads/advisories.html
#
#################################################################
#
# Product:    [CUT BY COMPASS]
# Vendor:     [CUT BY COMPASS]
# 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

Steps

1. Intercept Assertion
2. Extract certificate
3. “Clone” certificate; generate new keys
4. Manipulate Assertion, e.g., change username
5. Remove original signature; sign manipulated Assertion using the “cloned” certificate

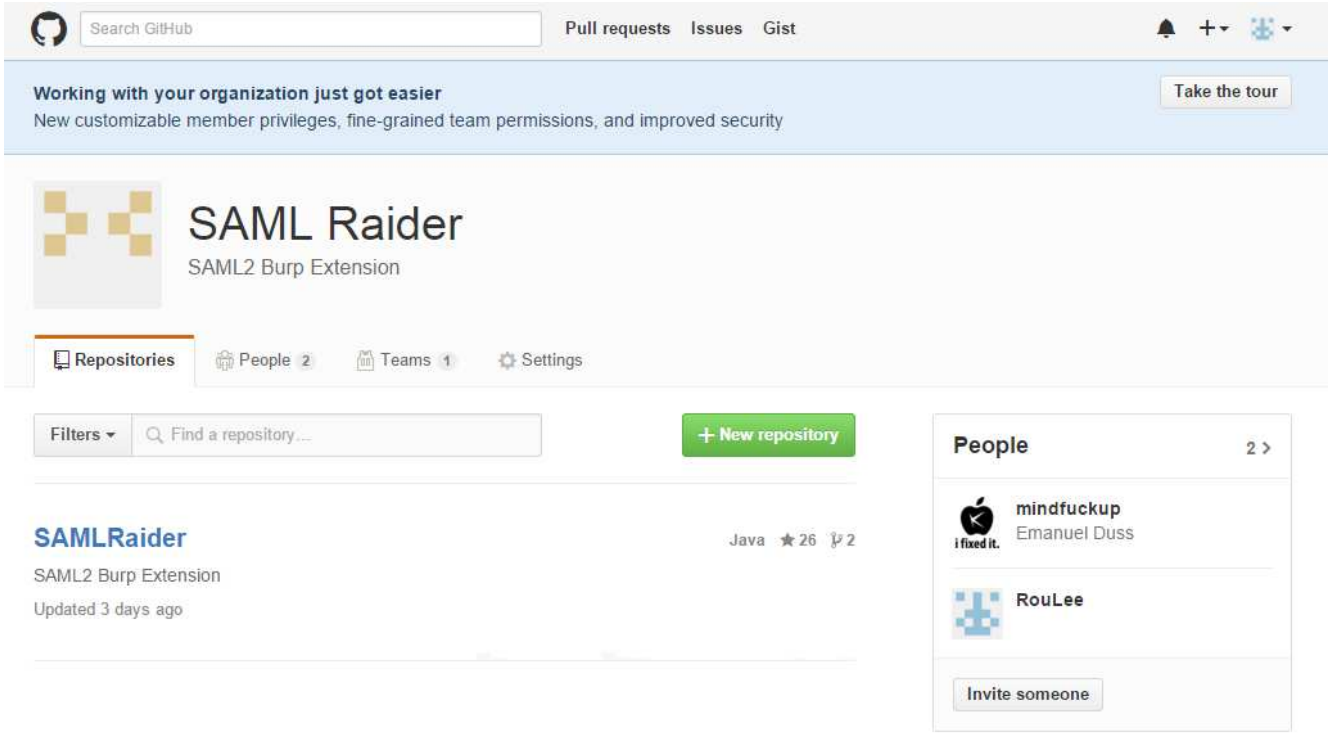
Problem

- Complicated workflow
- Assertion is often only valid for some minutes

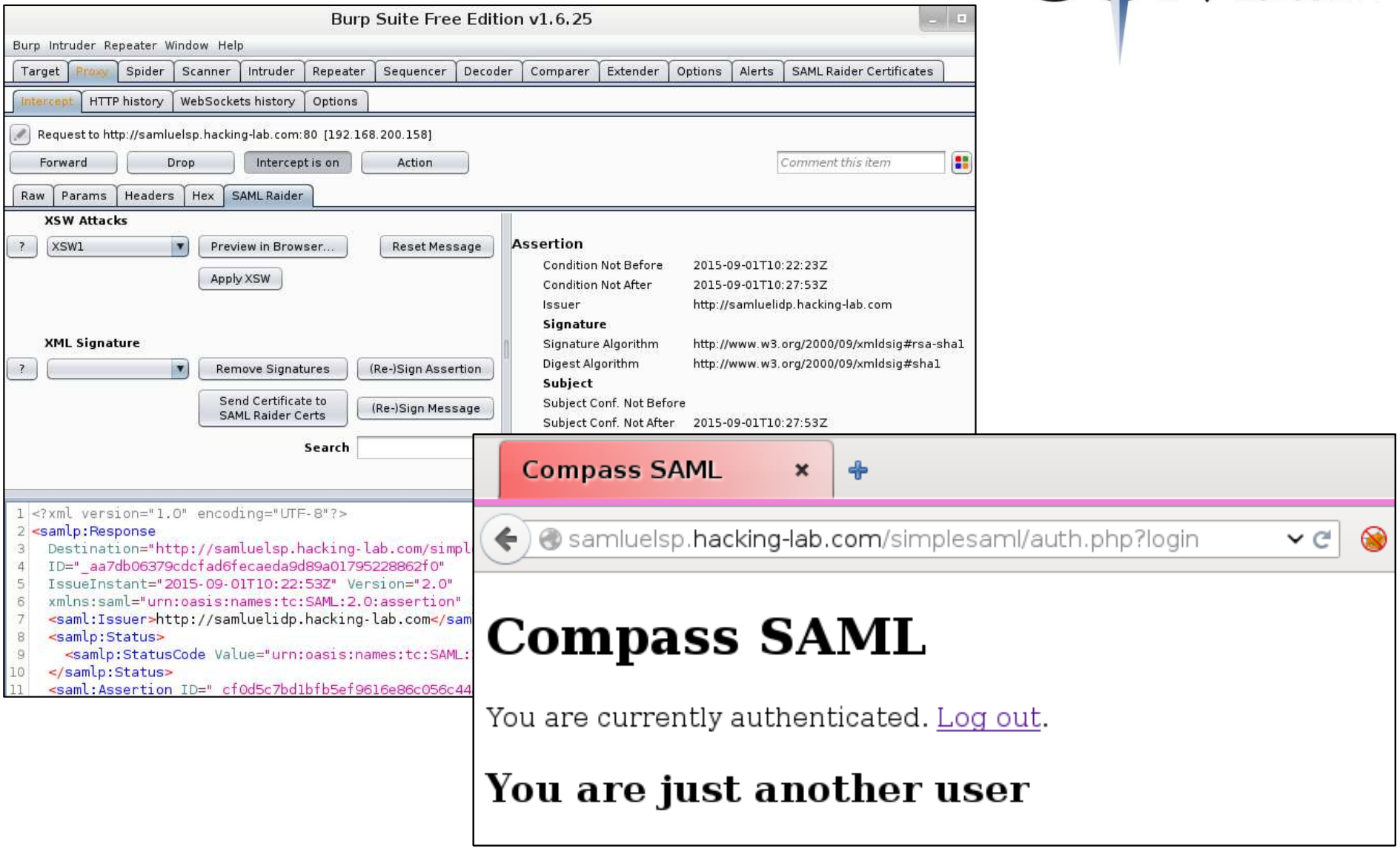
Demo Exploit

Solution

- SAMLRaider extension for burp
  - Developed as part of a Bachelor thesis (in cooperation with Compass Security)
  - https://github.com/SAMLRaider/SAMLRaider



Demo Exploit



Agenda

- Introduction to SAML
- Use-Cases
- Protocol Details

- SAML Attacks
- Demo Exploit
- Remediation

Remediation

- Use artifact binding (no contents stored on client)
- If POST Binding is required:
  - Use encrypted messages
  - Only process signed XML tree (delete other contents)
  - Use key material on the SP or IdP (not embedded keys)
  - Add a random number to every signed element that has been verified successfully
    - This number needs to be checked in following steps
    - This requires a modified XML schema

Open discussion

Thank you for your attention!

Contact

Compass Security Deutschland GmbH

Tauentzienstr. 18
10789 Berlin
Germany

team@csnc.de | www.csnc.de | +49 30 21 00 253-0

Secure File Exchange: www.filebox-solution.com

PGP-Fingerprint:
41CC 087A BF87 832F 7F0C 5FC3 CC36 7645 DAC0 B1EE