With Great Power Comes Great Pwnage

Area41 Security Conference
Zürich, June 10th 2016

antoine.neuenschwander@compass-security.com
roland.bischofberger@compass-security.com

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

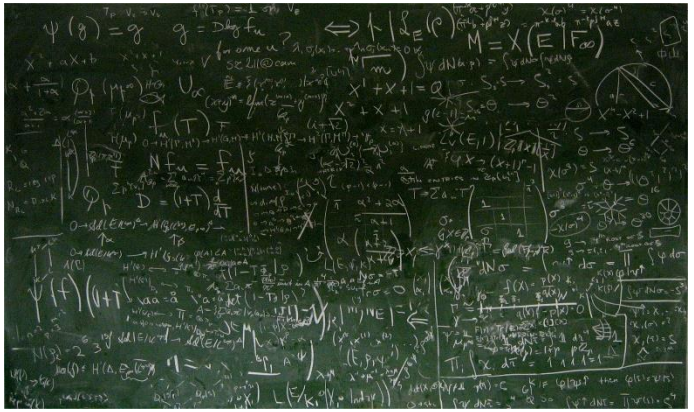
Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

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



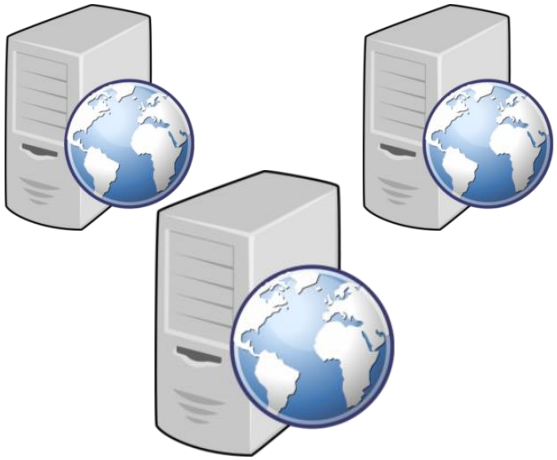
- SAML Attacks
- Demo
- Remediation

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

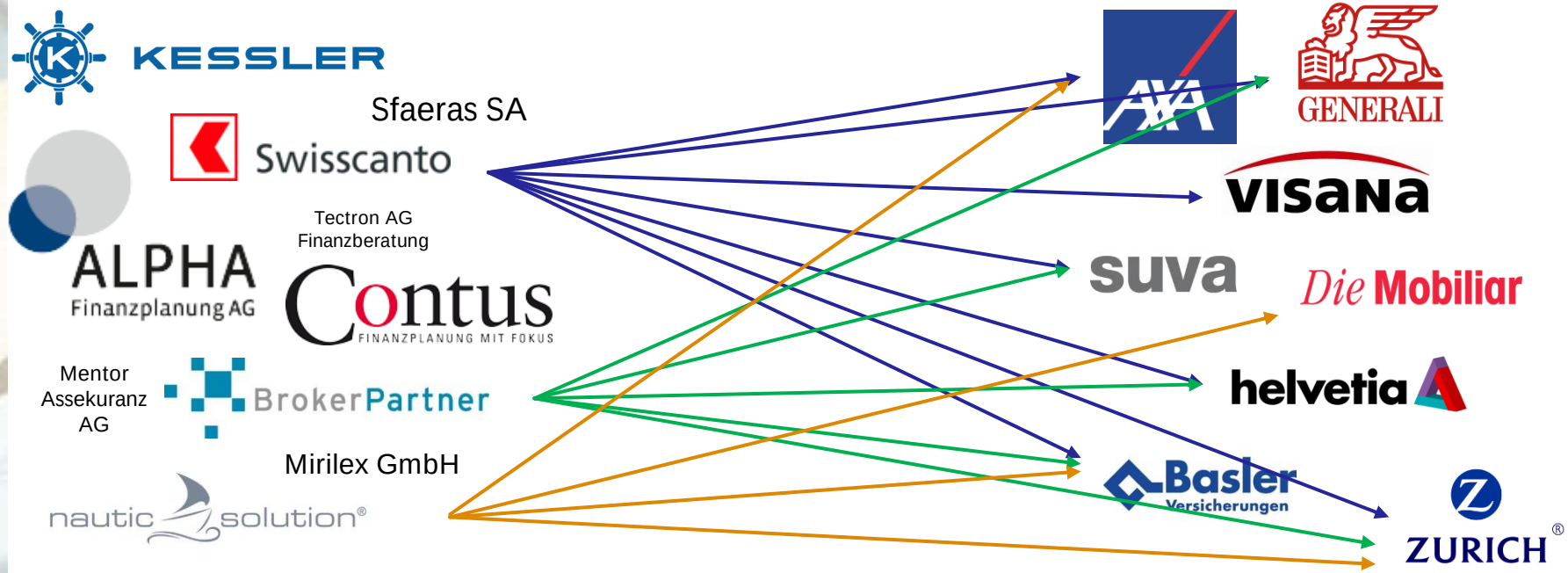
USE-CASES

Use-Case: IG B2B BrokerGate

941 Brokers,
4295 Users

IGB2B for Insurers +Brokers®

21 Insurers (13 online)
Broker portal as
Service Providers

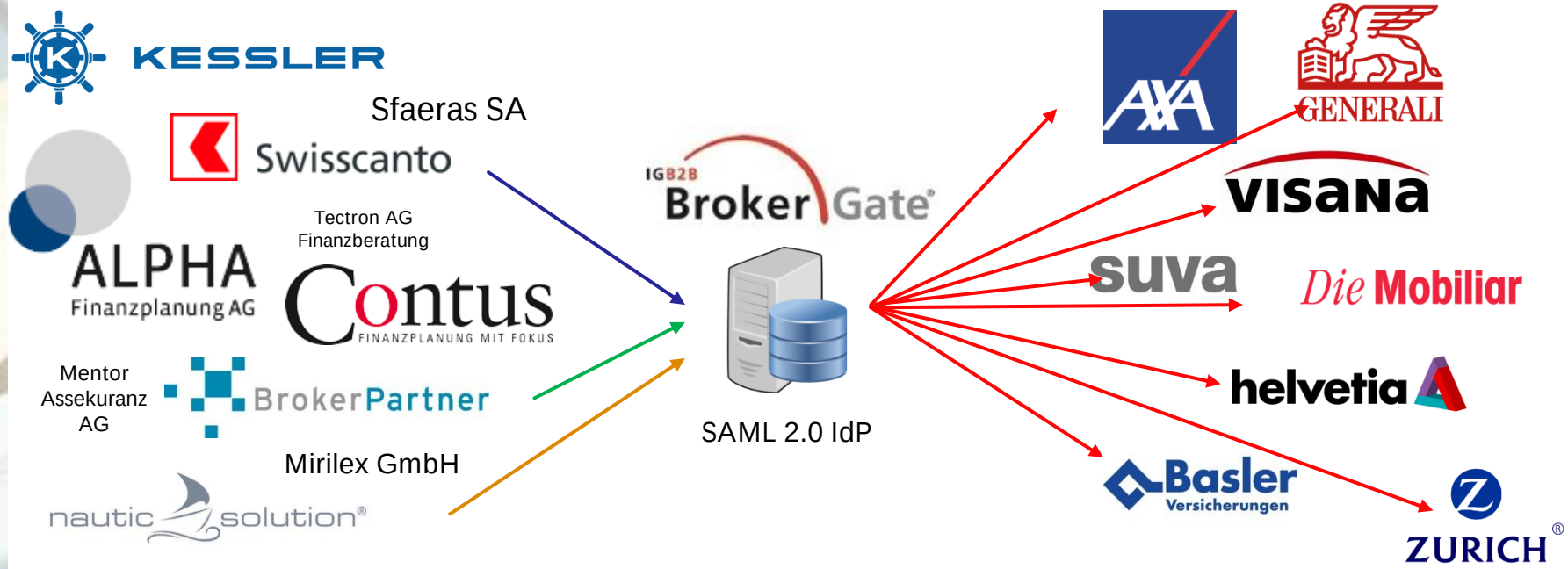


Use-Case: IG B2B BrokerGate

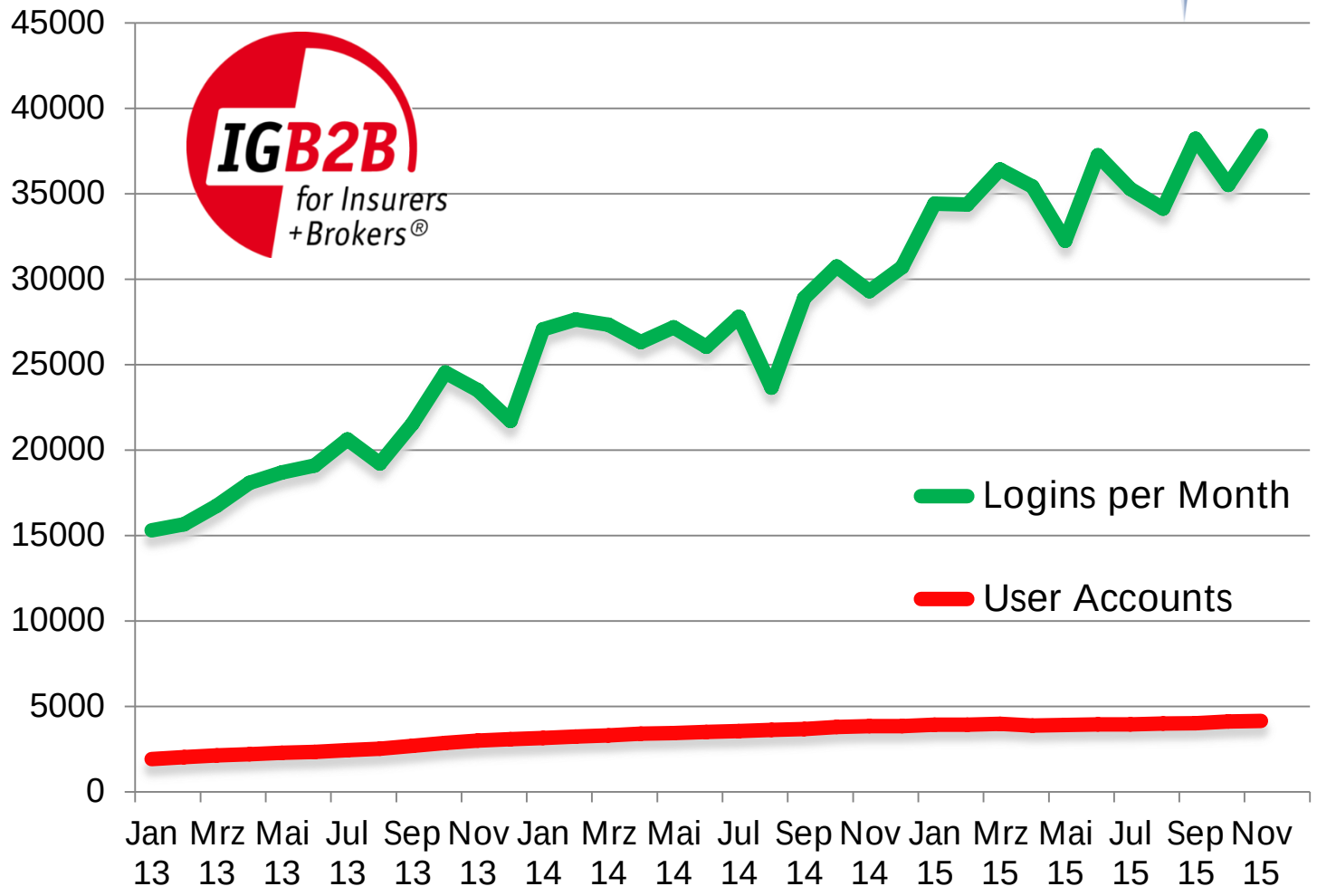
941 Brokers,
4295 Users

IGB2B for Insurers +Brokers®

21 Insurers (13 online)
Broker portal as
Service Providers

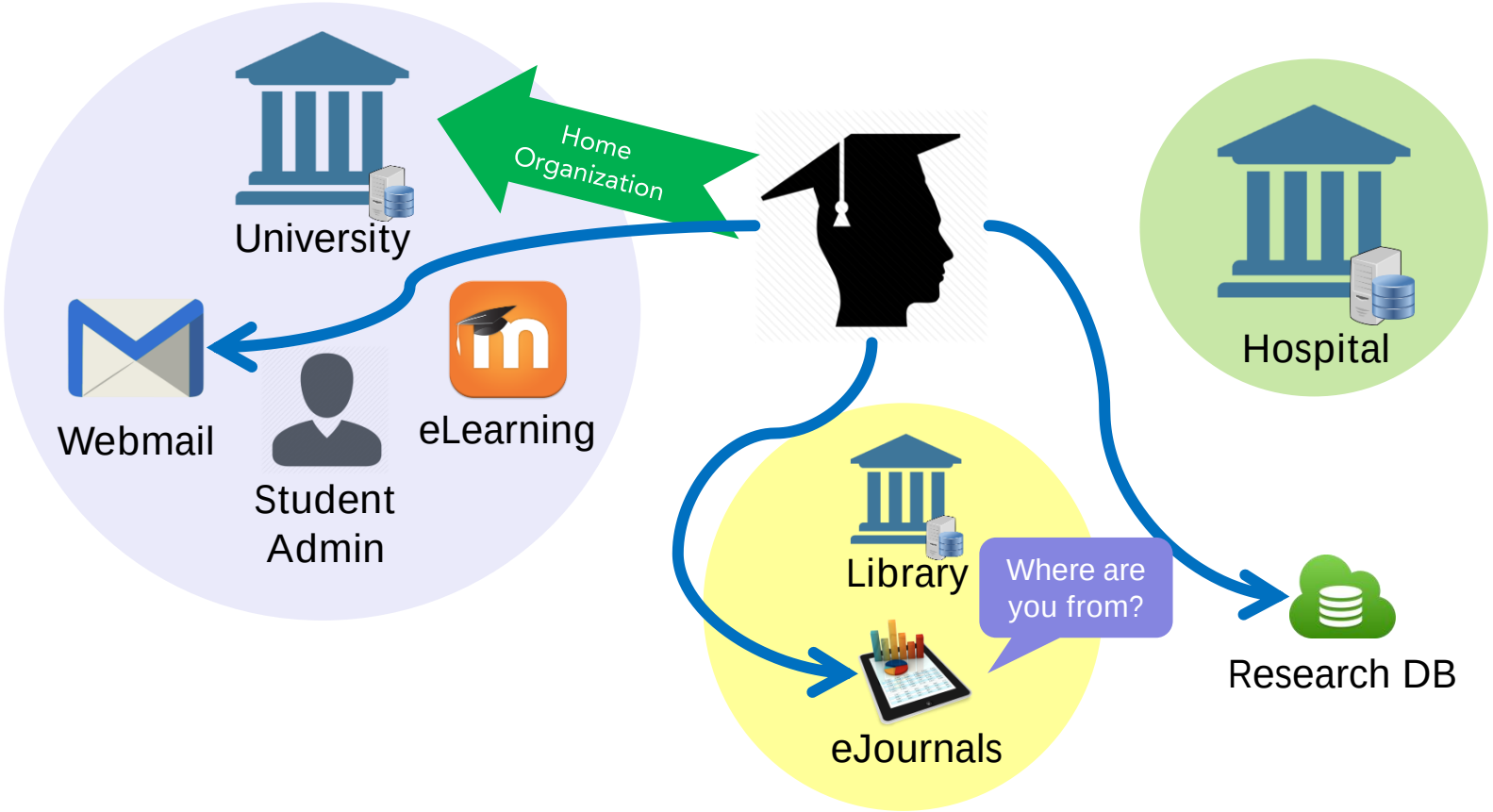


Use-Case: IG B2B BrokerGate



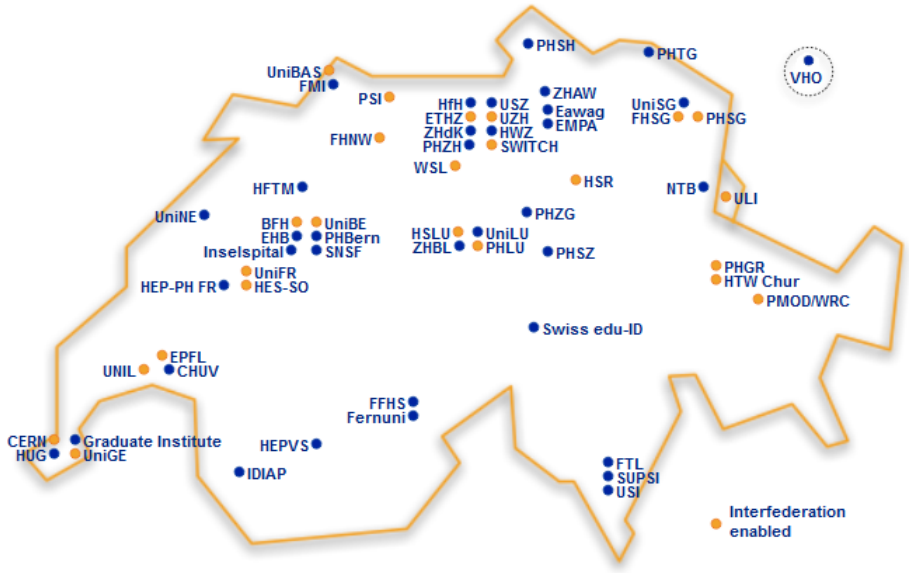
Use-Case: SWITCHaai

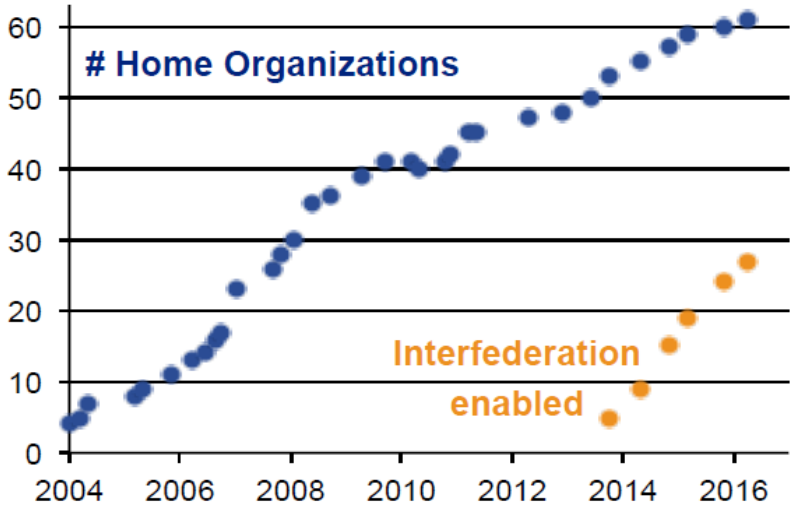
SWITCH



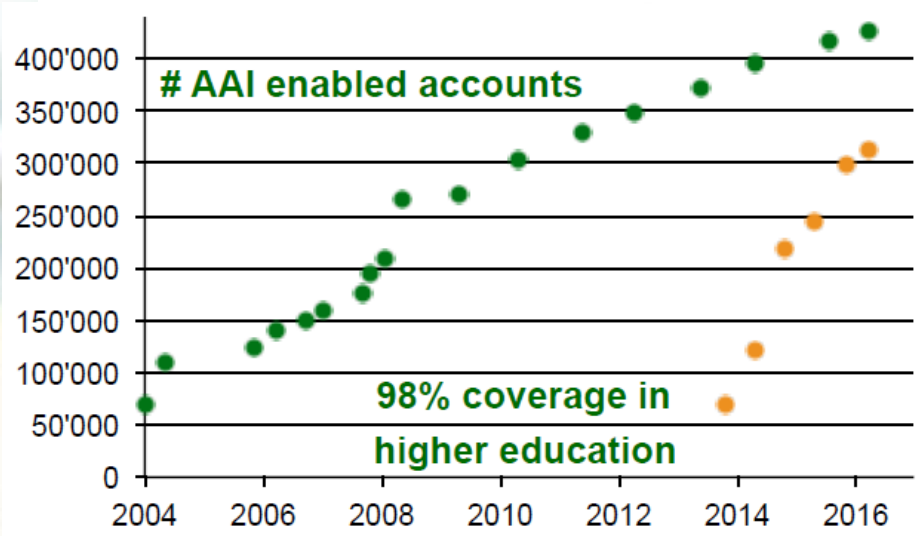
Use-Case: SWITCHaai

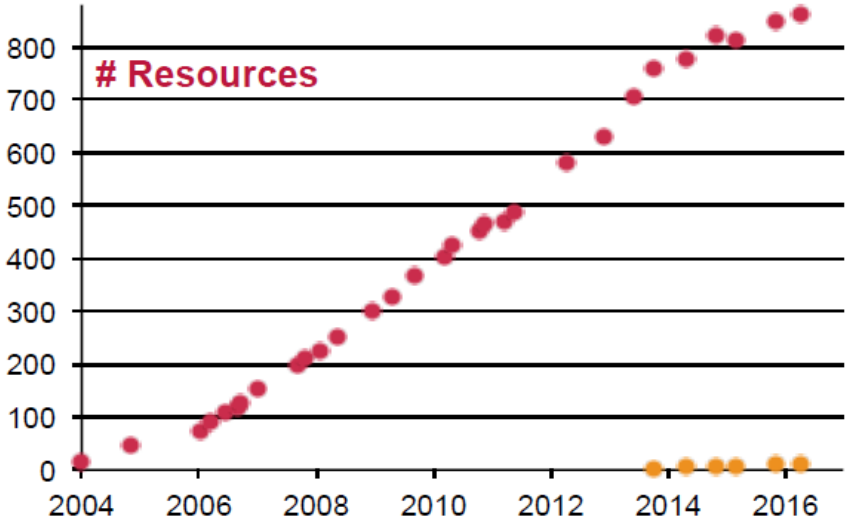
SWITCH





Use-Case: SWITCHaai

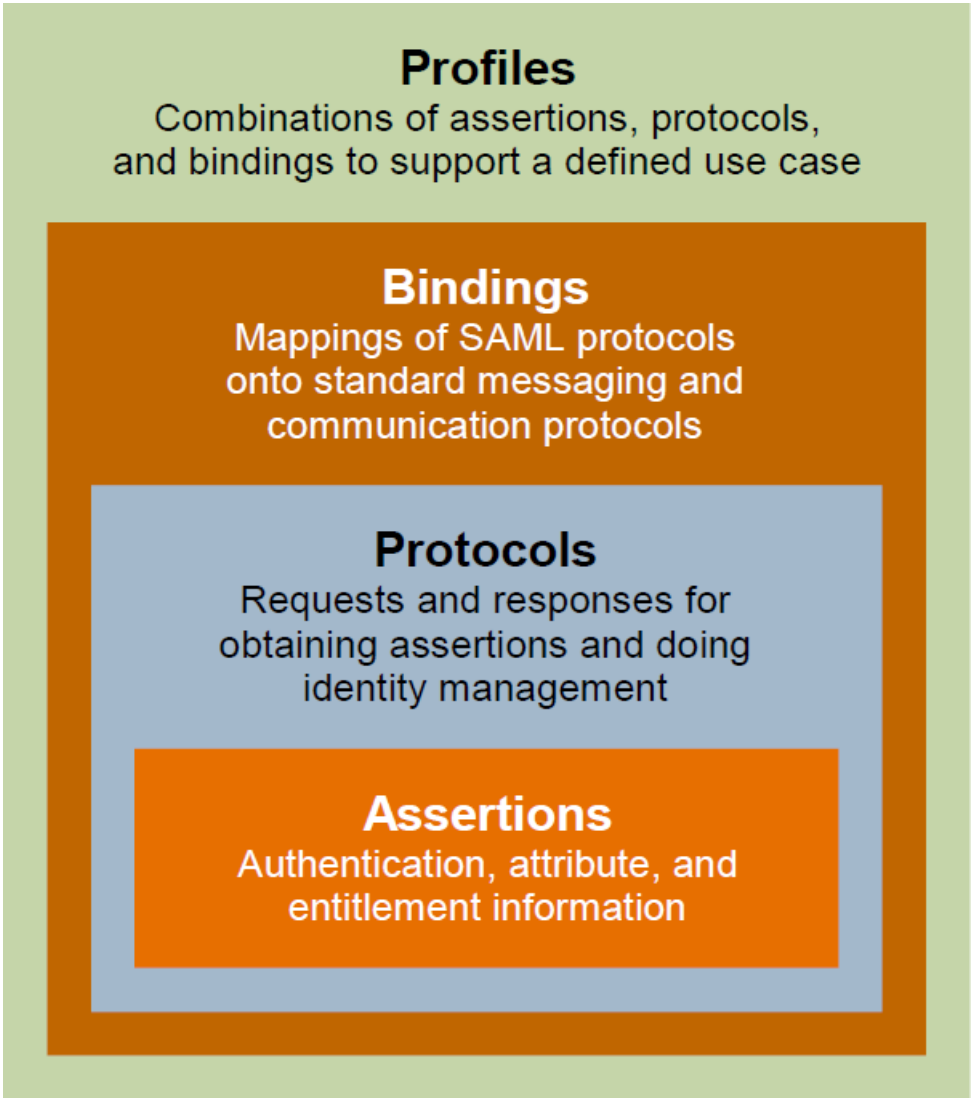




On Average: 52 SAML authentication requests per minute

SAML 2.0 FUNDAMENTALS

SAML – The Overall Picture



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

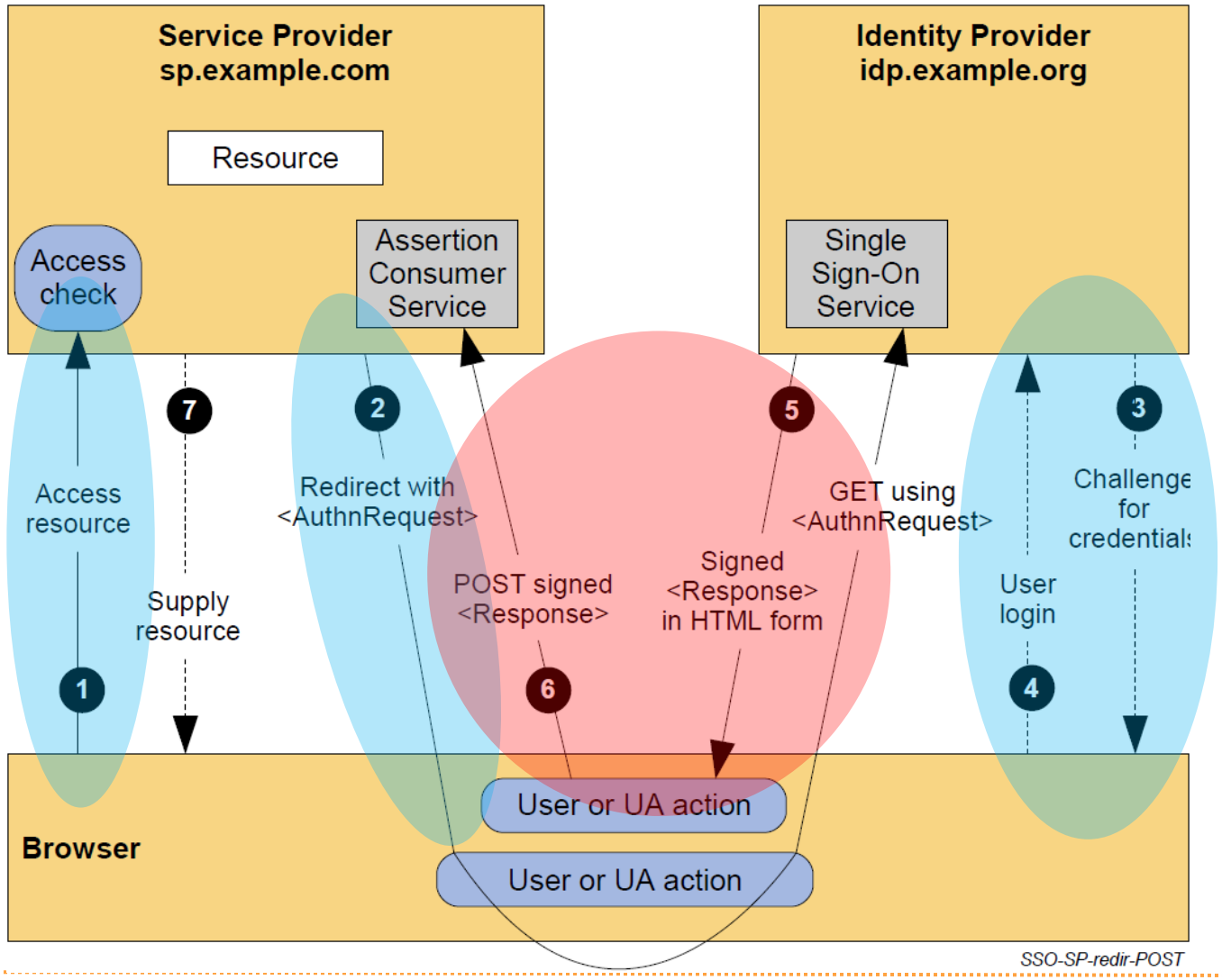
Bindings specify how the various messages can be carried over underlying transport protocols, e.g. HTTP redirect or POST

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

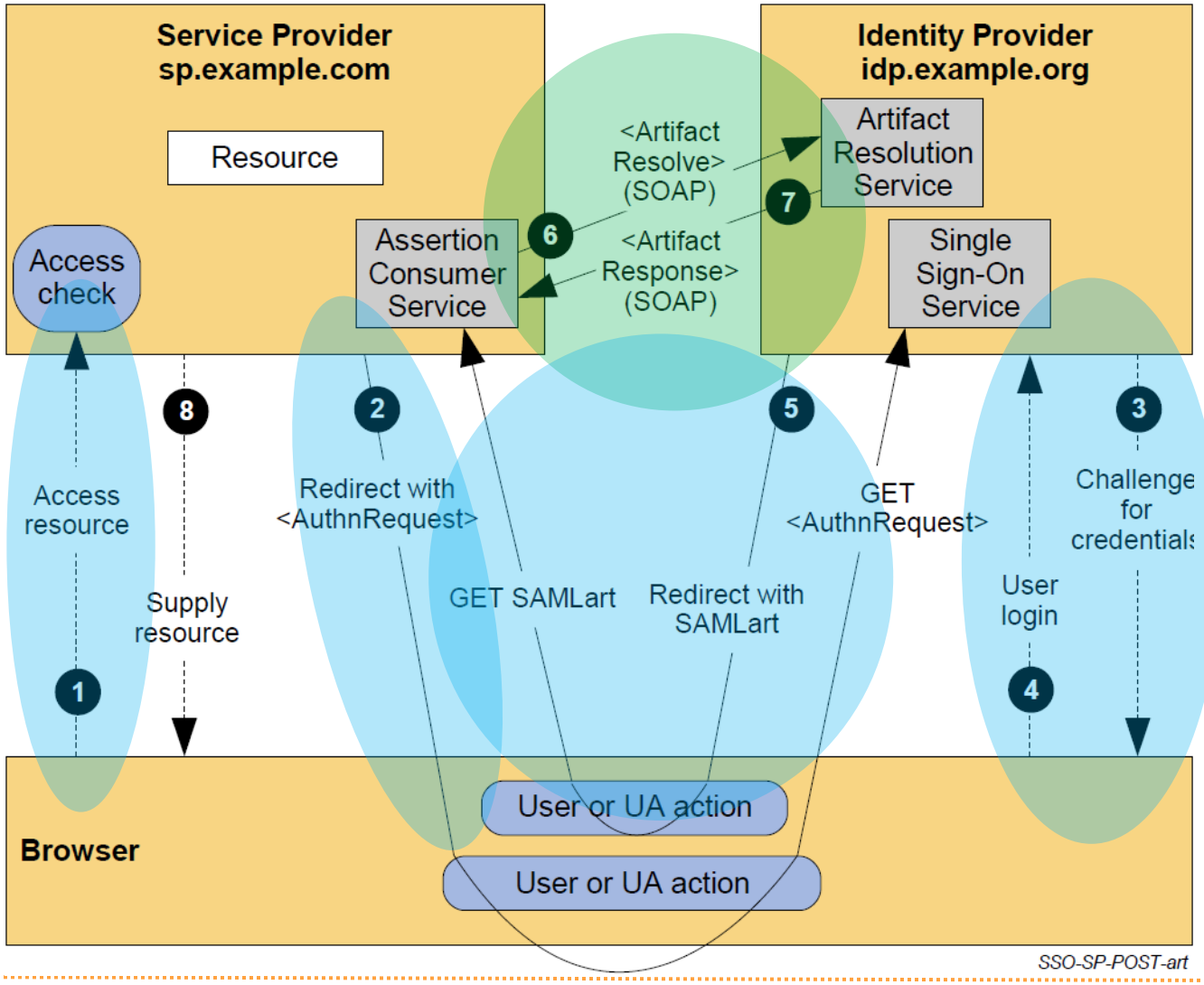
Web Browser SSO Profile

SP-Initiated SSO with Redirect and POST Bindings

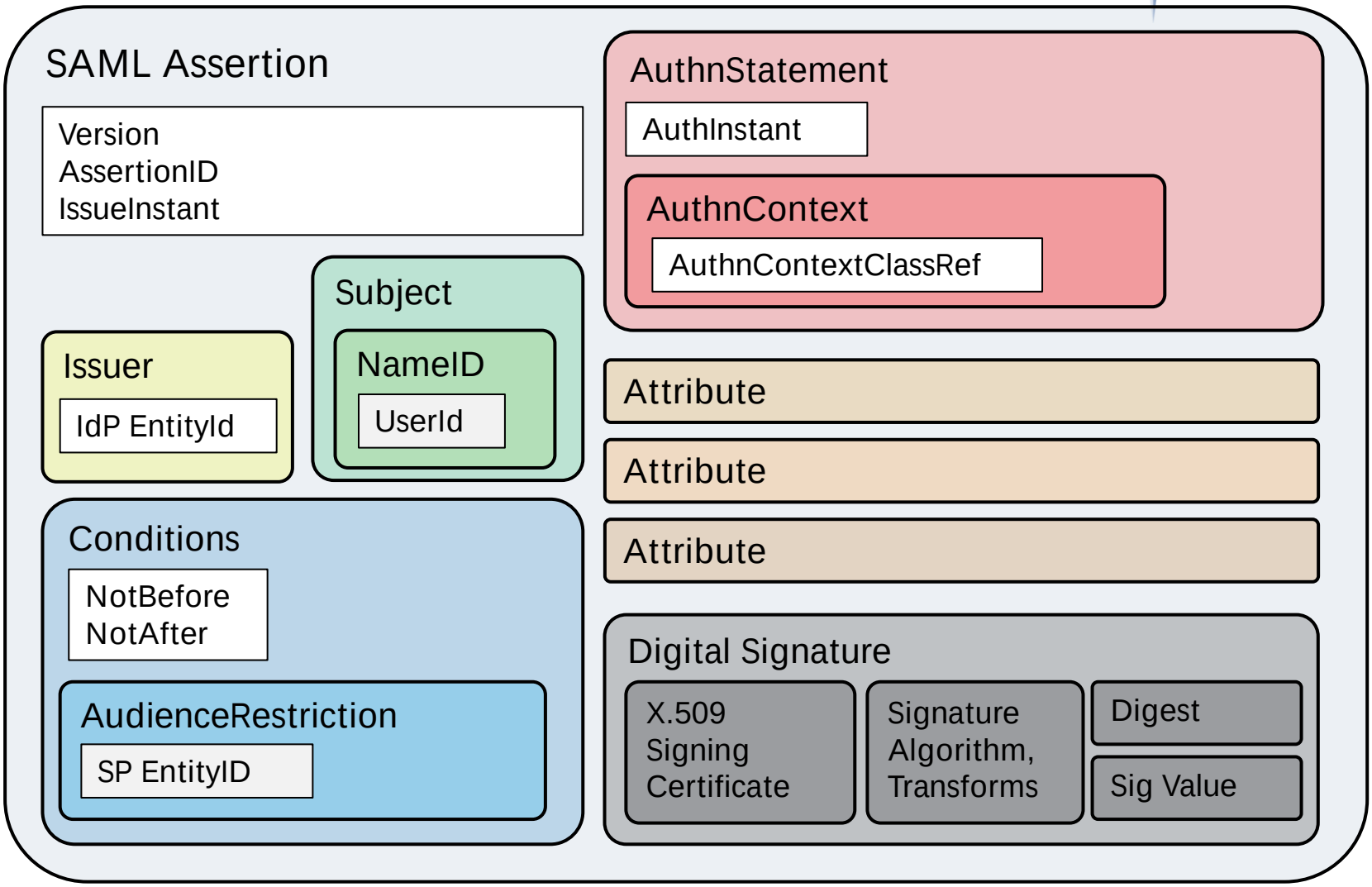


Web Browser SSO Profile (Artifact)

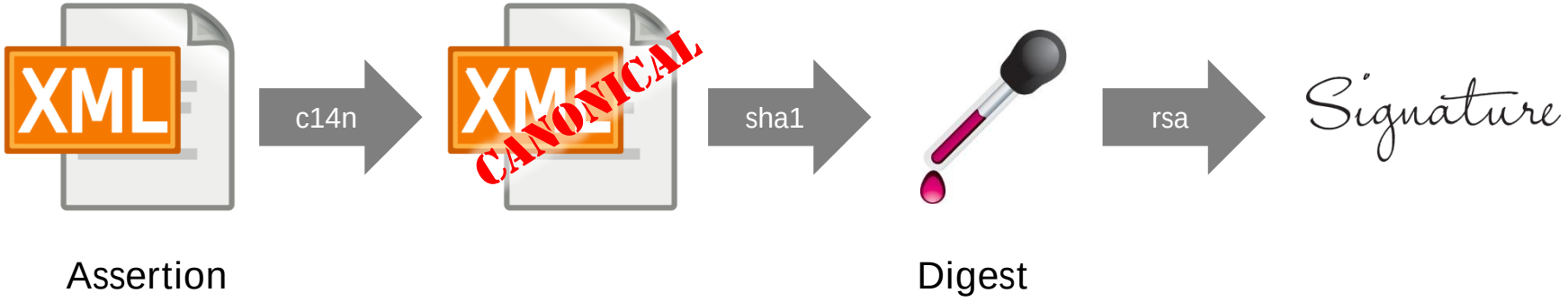
SP-Initiated SSO with POST/Artifact Bindings

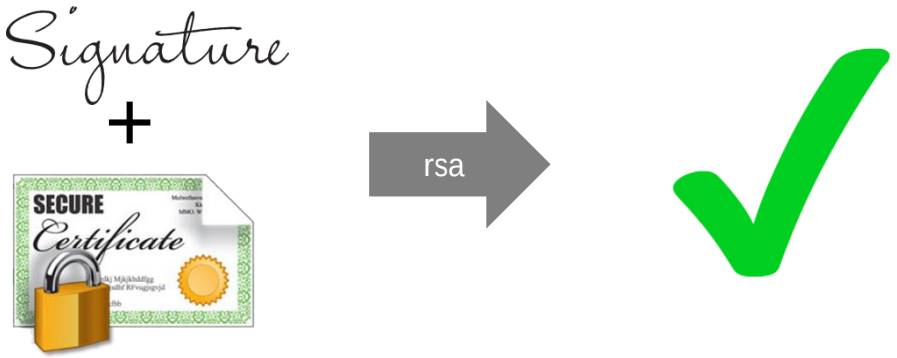


Security Assertion



XML Signature

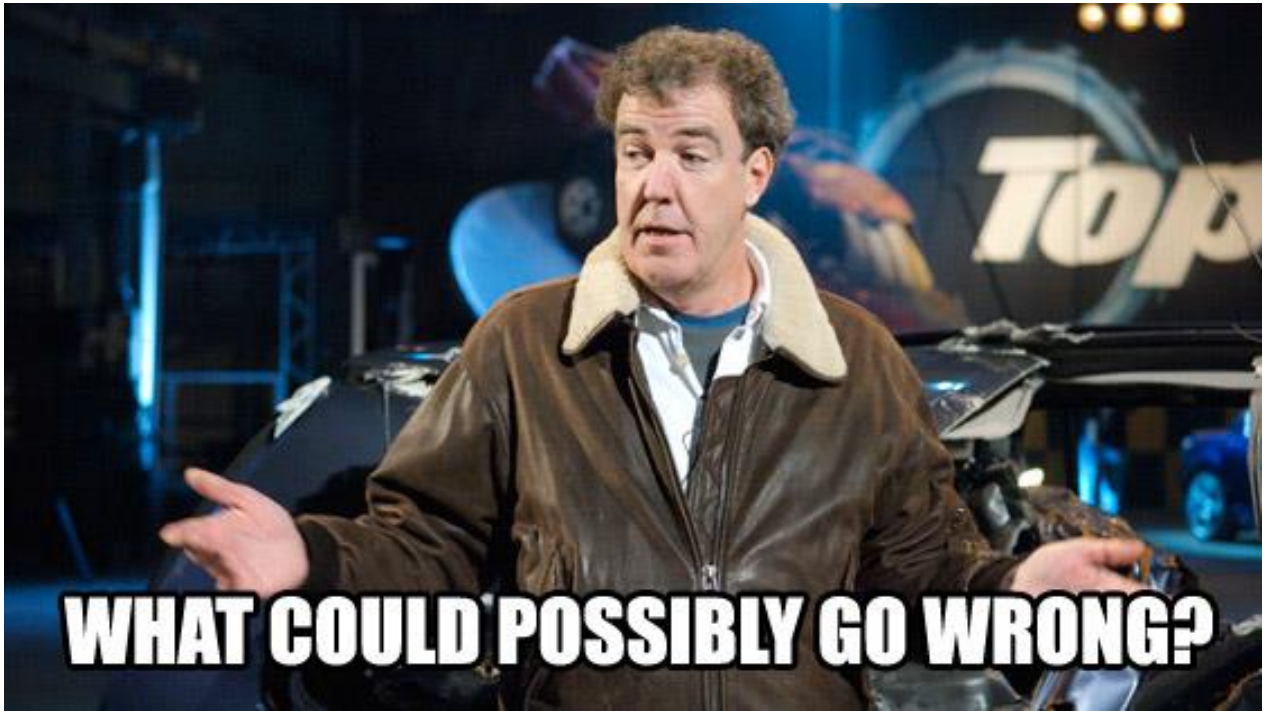




SAML ATTACKS

Technologies

- SAML
- XML Signatures
- X.509 Certificates



Security is hard

about

geocreepy

HOME | ARCHIVES | CATEGORIES | TAGS | ATOM

The road to hell is paved with SAML Assertions

Posted on Τετ 27 Απρίλιος 2016 in bounty

TL;DR

A vulnerability in Microsoft Office 365 SAML Service Provider implementation allowed for cross domain authentication bypass affecting **all** federated domains. An attacker exploiting this vulnerability could gain unrestricted access to a victim's Office 365 account, including access to their email, files stored in OneDrive etc.

This vulnerability was jointly discovered by Klemen Bratec from Šola prihodnosti Maribor, and Ioannis Kakavas from Greek Research and Technology Network and this blog post is cross-posted here and on Klemen's blog.

Microsoft fixed the vulnerability within **7 hours** of our report and handled the disclosure process admirably.

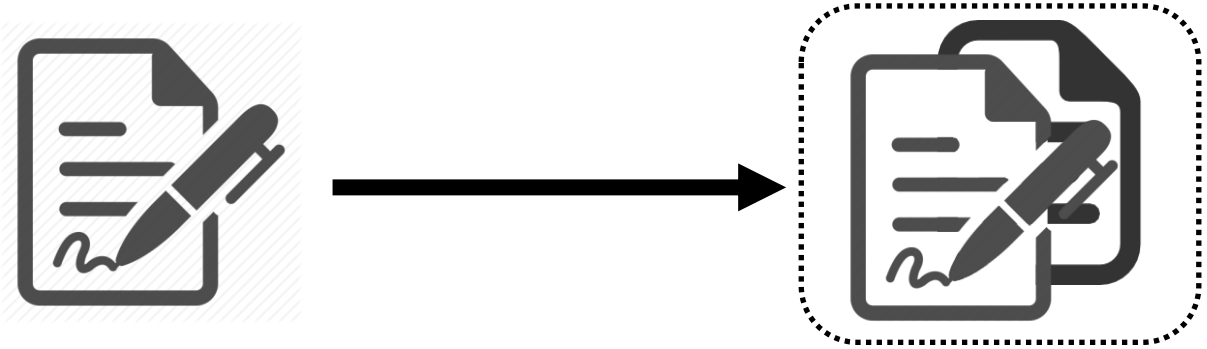
SAML Attacks - SAML

- Log out other users due to a guessable IDs
- Replay an eavesdropped SAML Message
  - Google for Messages, Stack Overflow

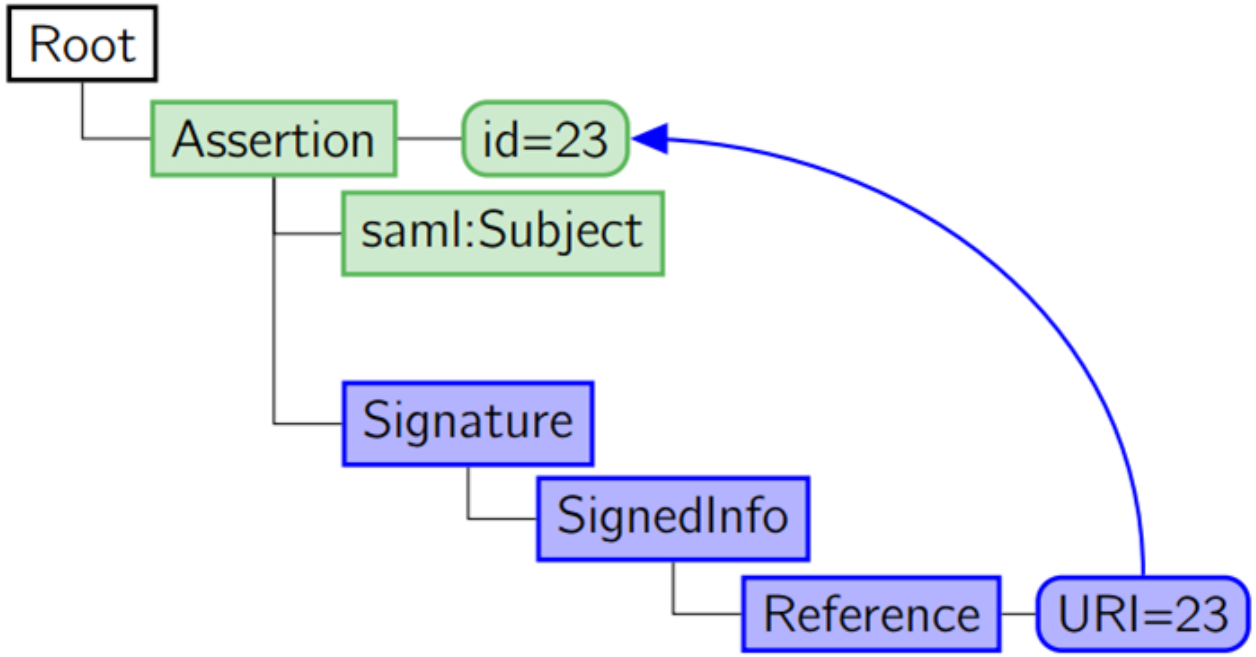
SAML Attacks - XML

- Signature Exclusion (simply delete Signature)

- XML Signature Wrapping
  - Paper «On Breaking SAML: Be Whoever You Want to Be», 2012

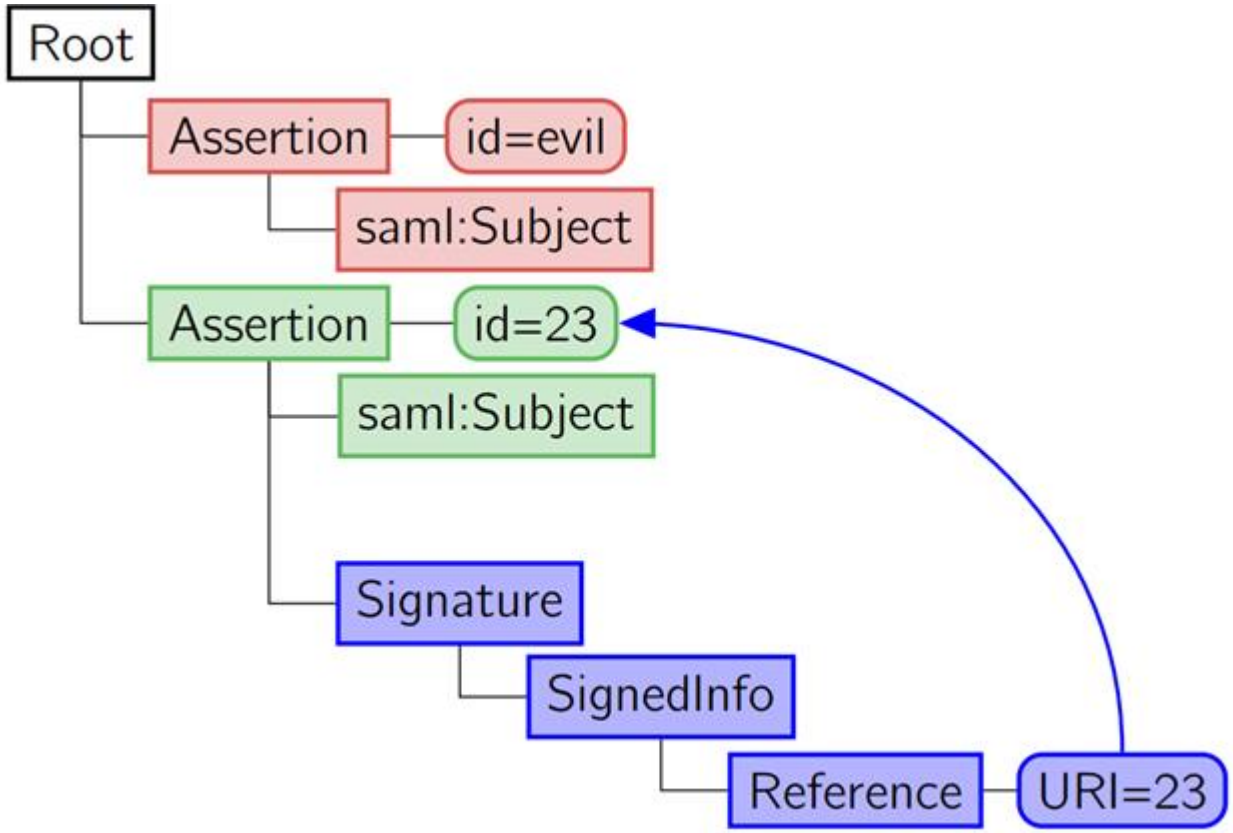


- Normal Message



SAML Attacks - XML

- Manipulated Message (XSW)



SAML Attacks – Certificate Tampering

Precondition: Certificate is embedded in the message

- «clone» a certificate, generate new key material
- Use a certificate signed by other official CA
- Use a revoked certificate

Demo Exploit

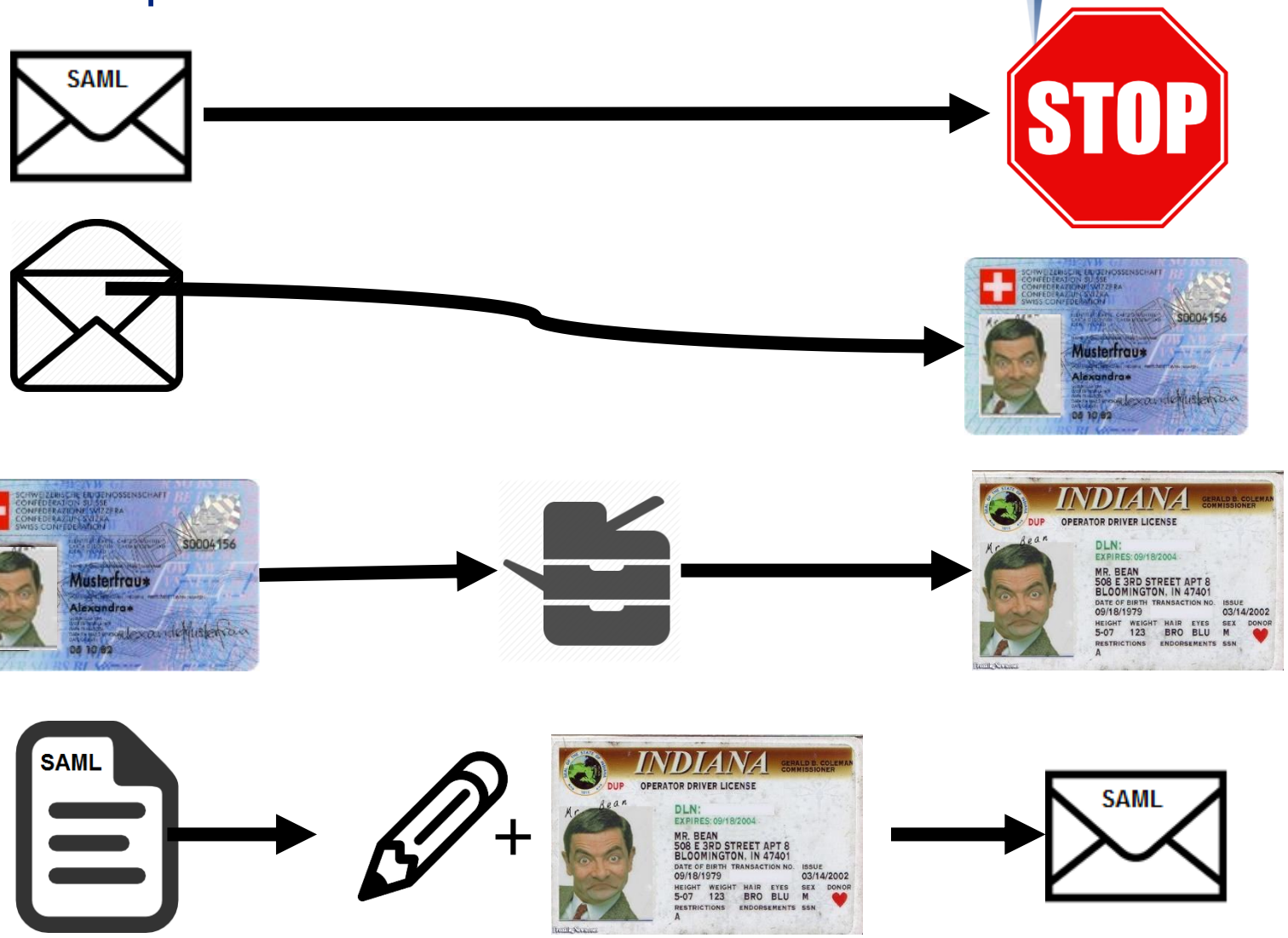
Found in June 2015 by Compass Security

using **SAML POST-Binding**

not matching all attributes of the **X.509 certificate** embedded

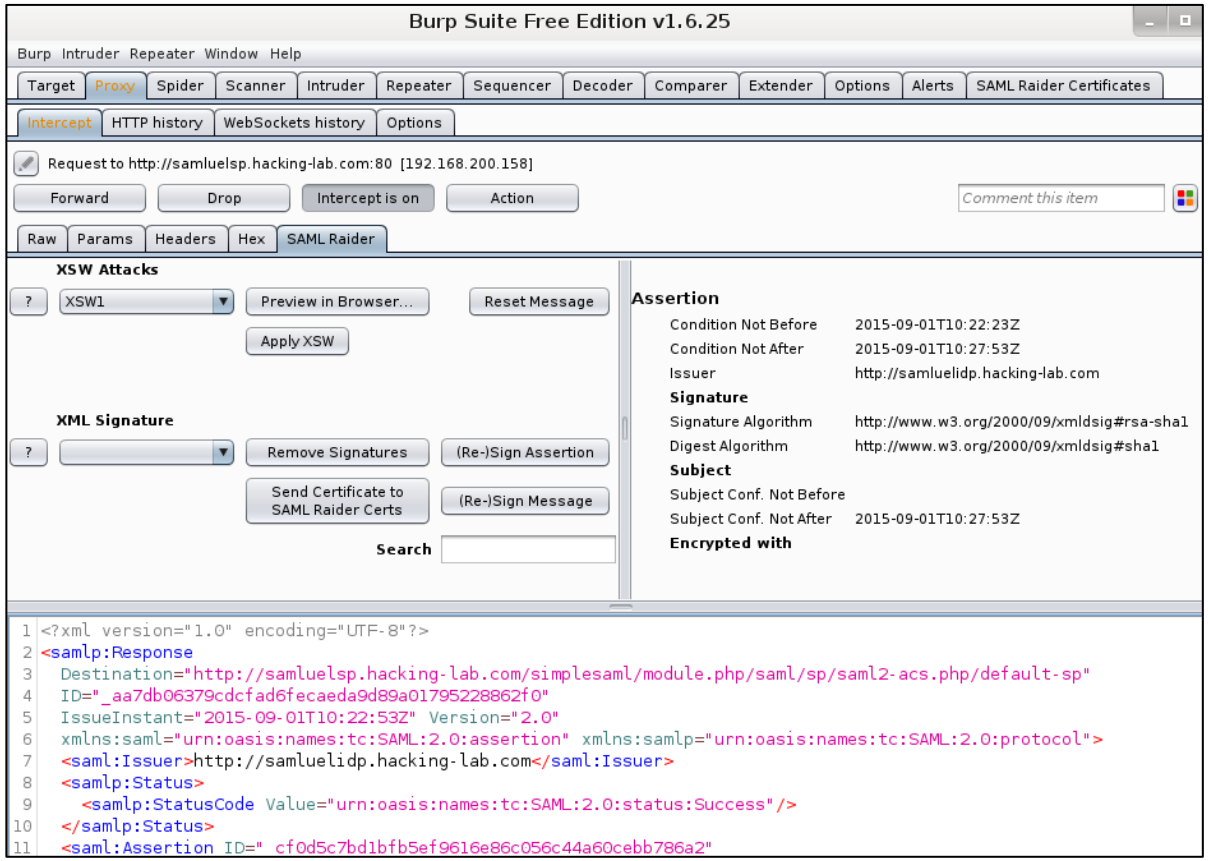
in the assertion **against the certificate from the identity provider** (IdP)

Demo Exploit



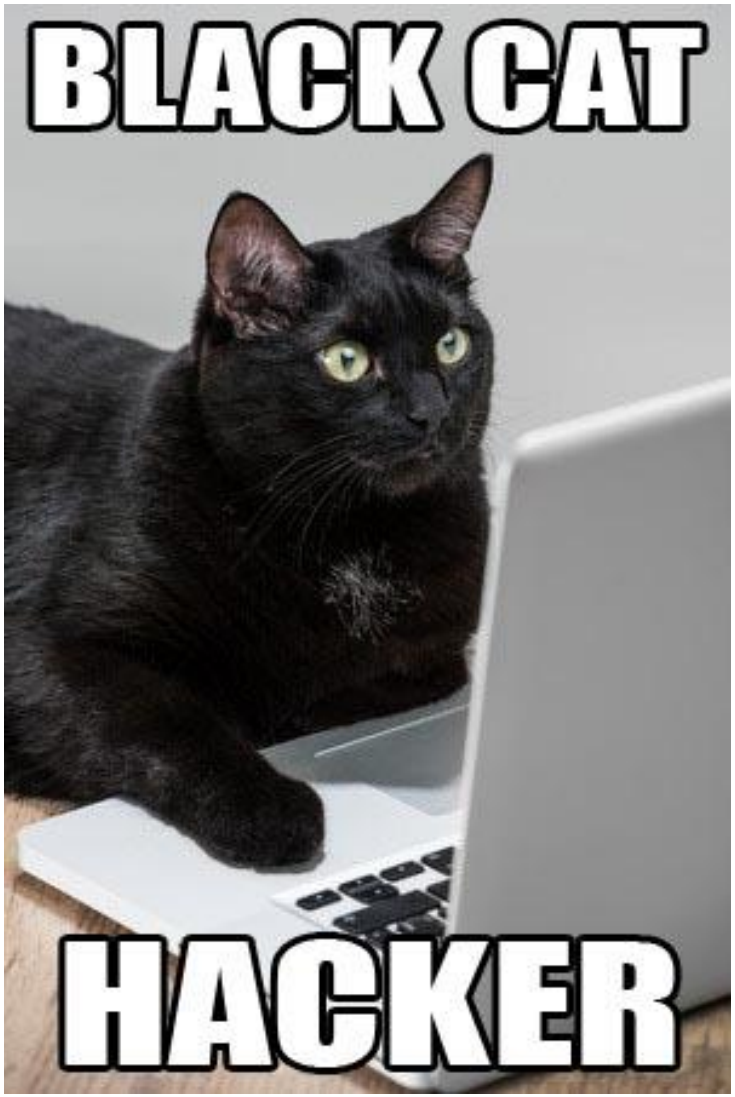
SAMLRaider

SAMLRaider Extension for Burp



https://github.com/SAMLRaider/SAMLRaider

Demo Exploit



REMEDIATIONS

SAML Attacks - Mitigation

- Configuration:
  - Use artifact binding (no content on client)
  - If POST-binding is necessary:
    - Use encrypted messages
- Implementation:
  - Only process signed XML tree (delete other content)
  - Use key material on the SP or IdP and not embedded keys

Questions?

Credits and Links:

Emanuel Duss, Bachelor Thesis and SAMLRaider

Bachelor Thesis
https://eprints.hsr.ch/464/

SAMLRaider on Github:
https://github.com/SAMLRaider/SAMLRaider


COMPASS
SECURITY