



With Great Power Comes Great Pwnage

Area41 Security Conference
Zürich, June 10th 2016

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

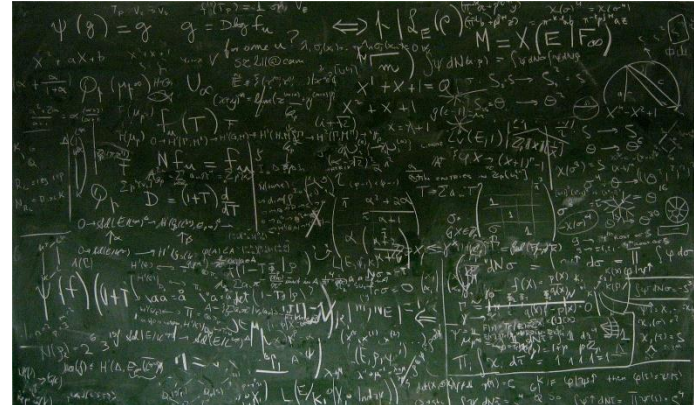
Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

Hello



- ◆ Introduction to SAML
- ◆ Use-Cases
- ◆ Protocol Details



- ◆ SAML Attacks
- ◆ Demo
- ◆ Remediation

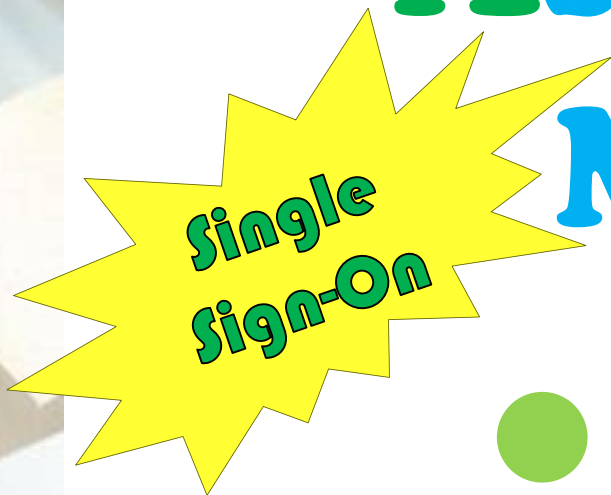




Security



Assertion



Markup



Language





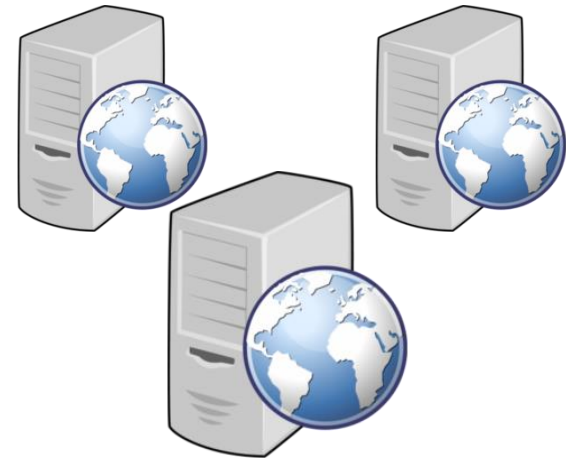
Client / User

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

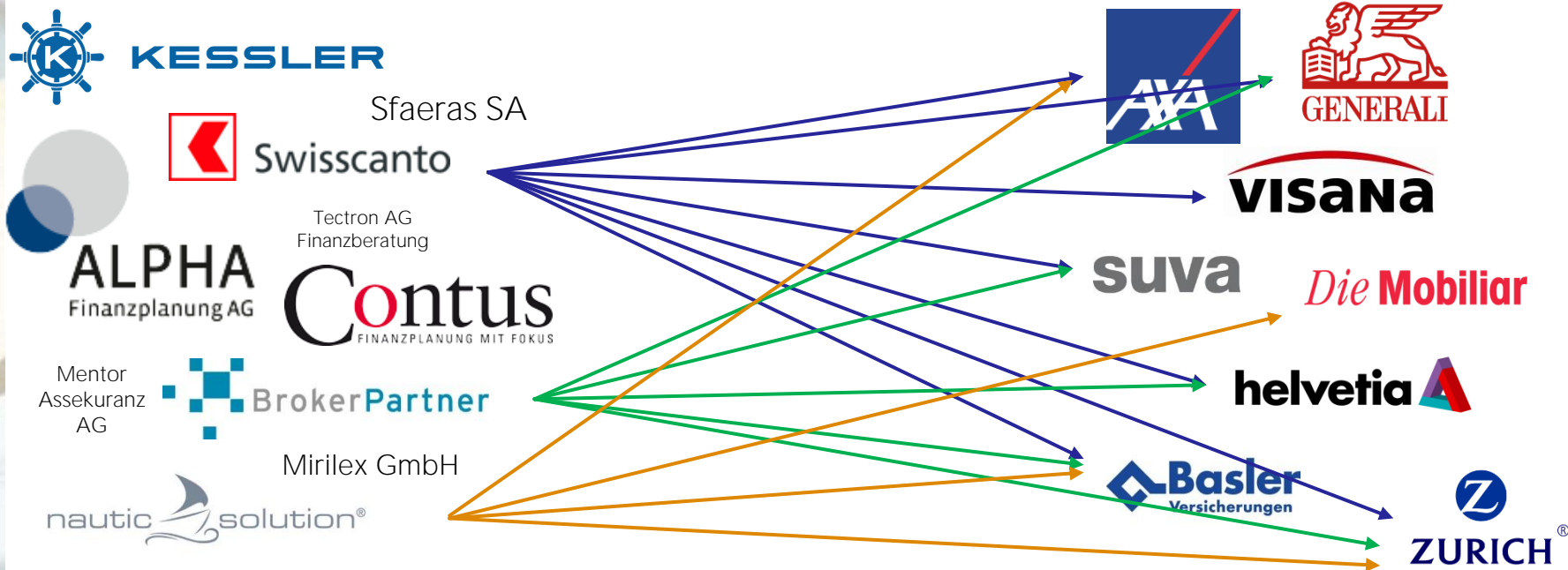
Use-Case: IG B2B BrokerGate



941 Brokers,
4295 Users



21 Insurers (13 online)
Broker portal as
Service Providers



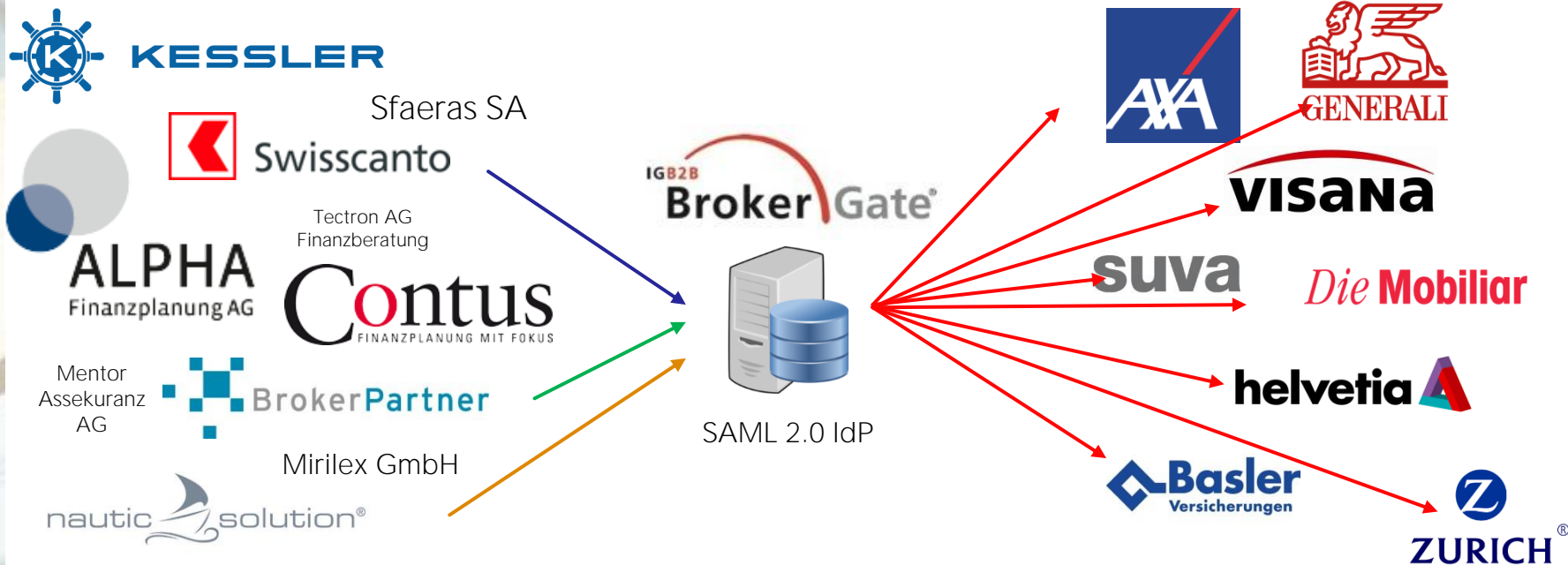
Use-Case: IG B2B BrokerGate



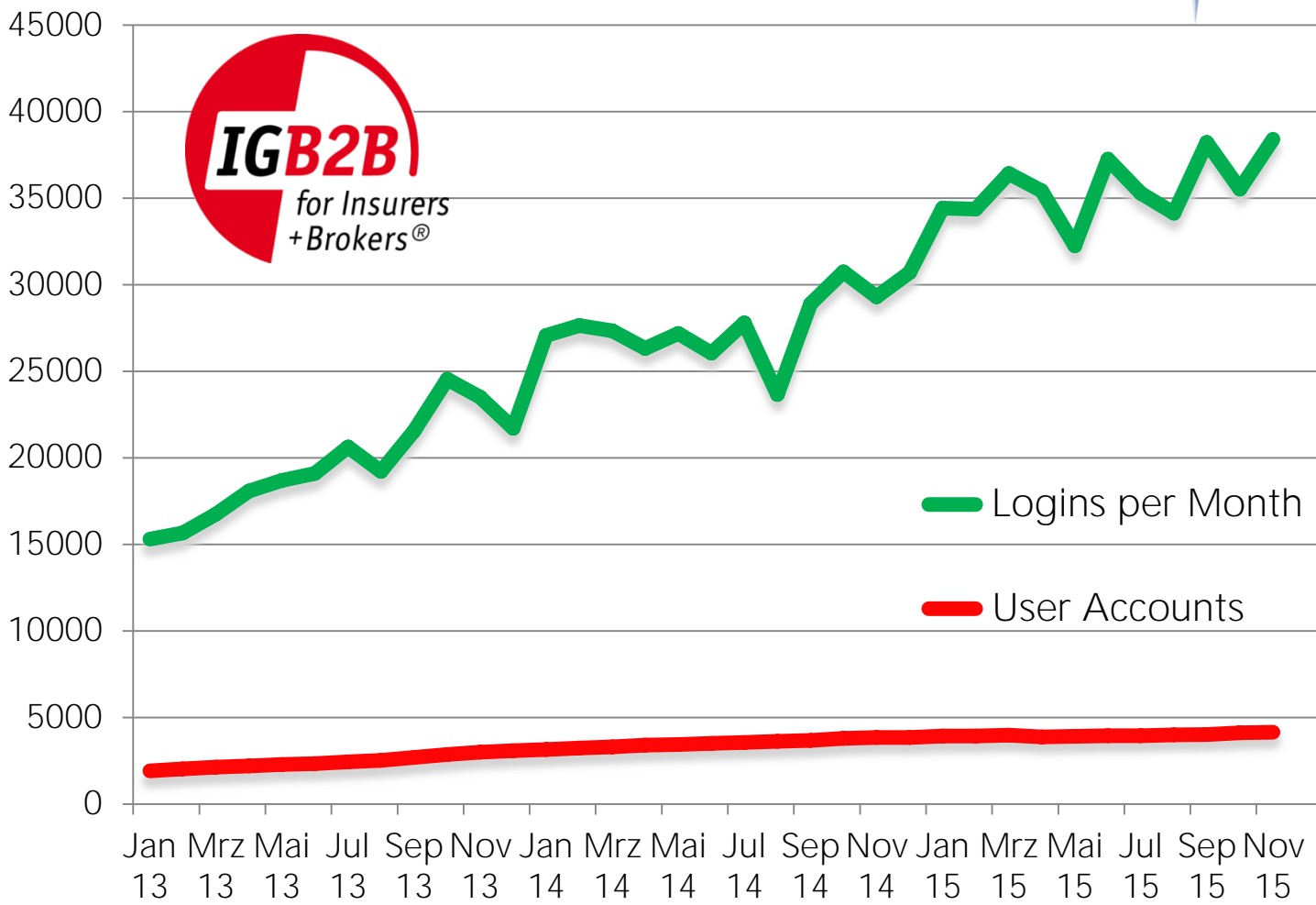
941 Brokers,
4295 Users



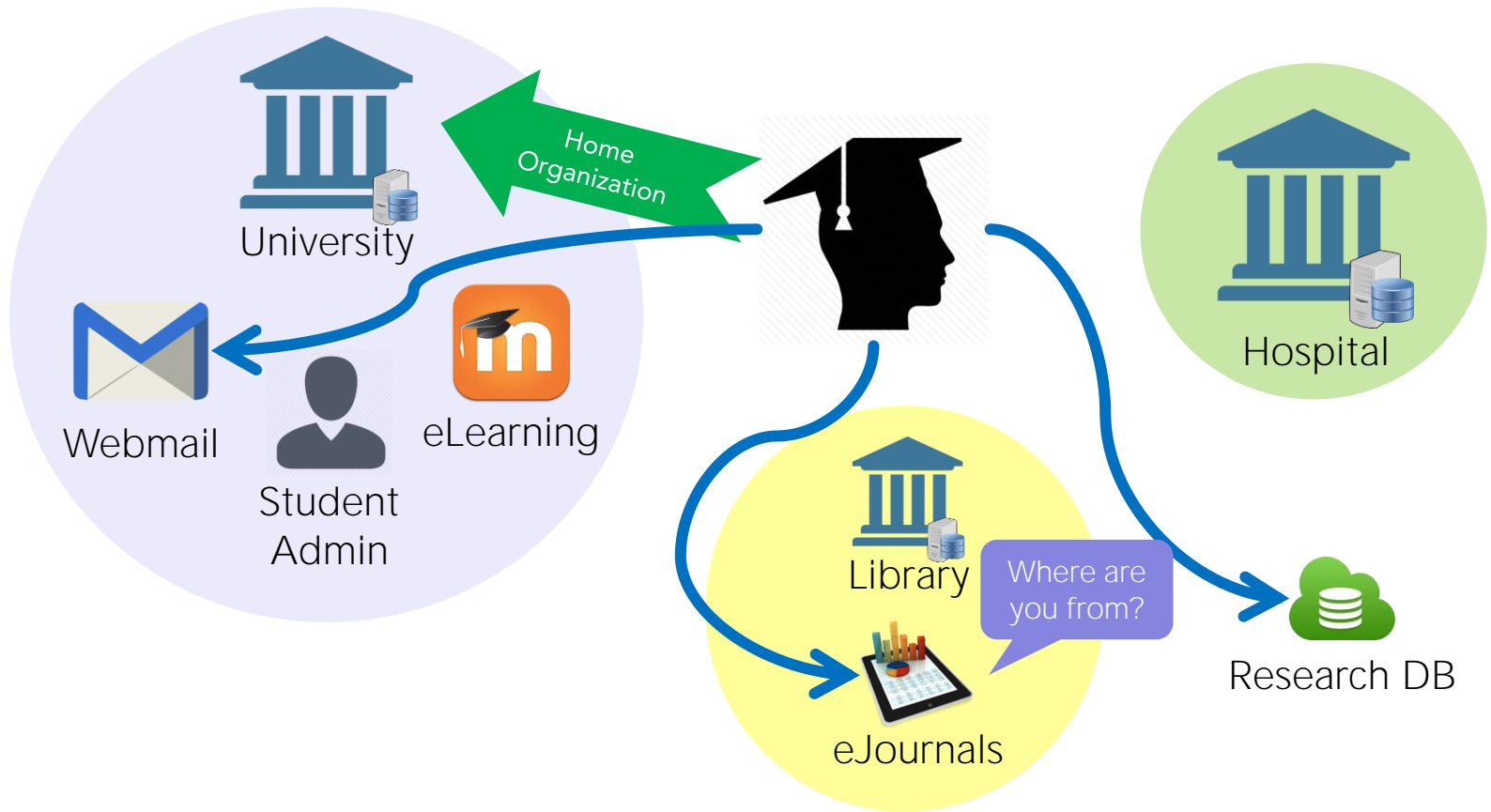
21 Insurers (13 online)
Broker portal as
Service Providers



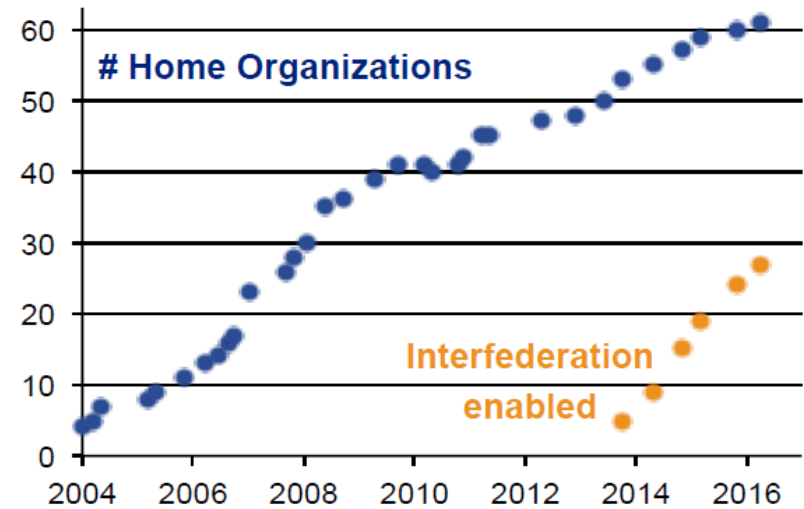
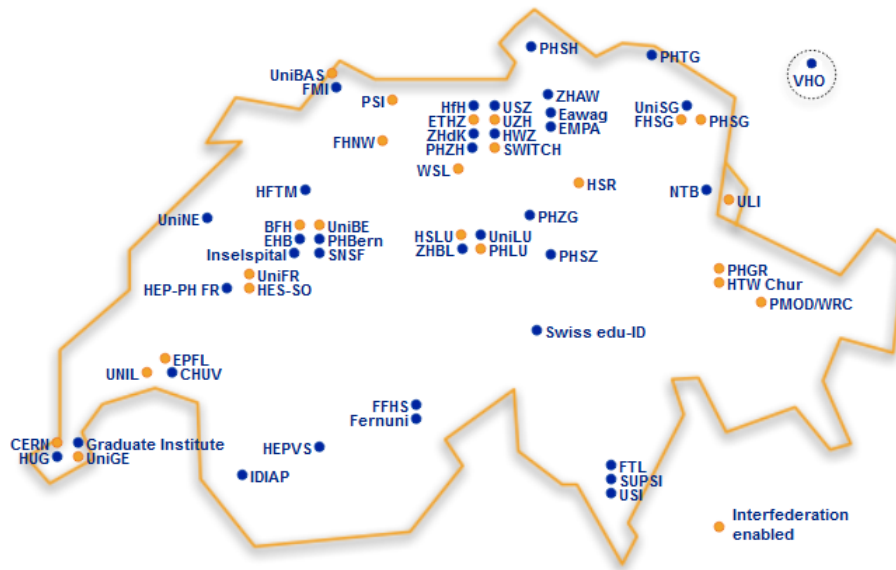
Use-Case: IG B2B BrokerGate



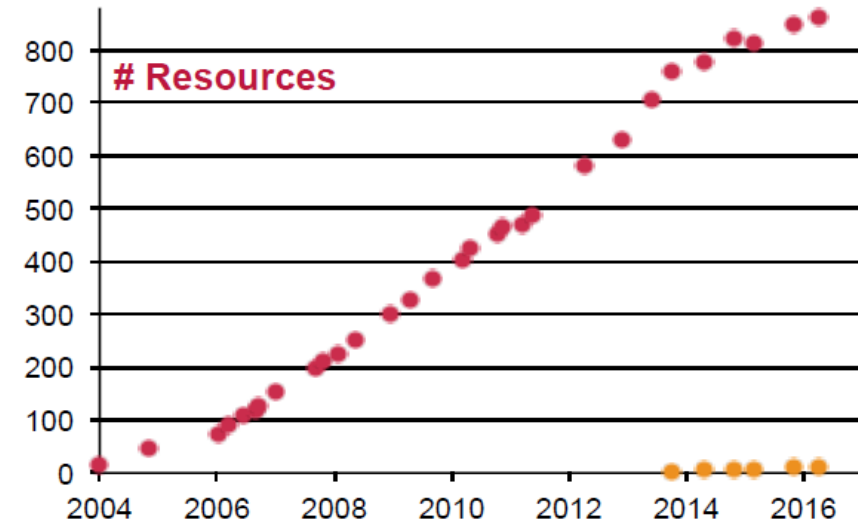
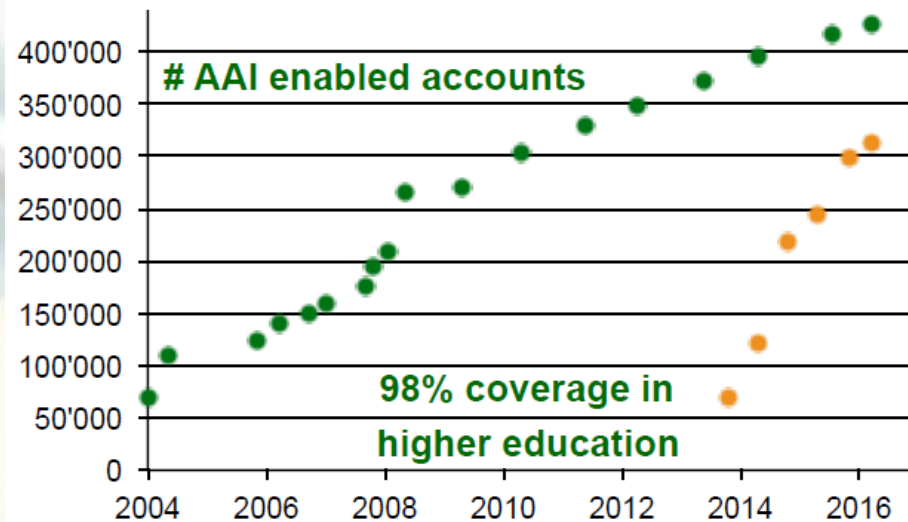
SWITCH



SWITCH



SWITCH



On Average: 52 SAML authentication requests per minute



SAML 2.0 FUNDAMENTALS

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

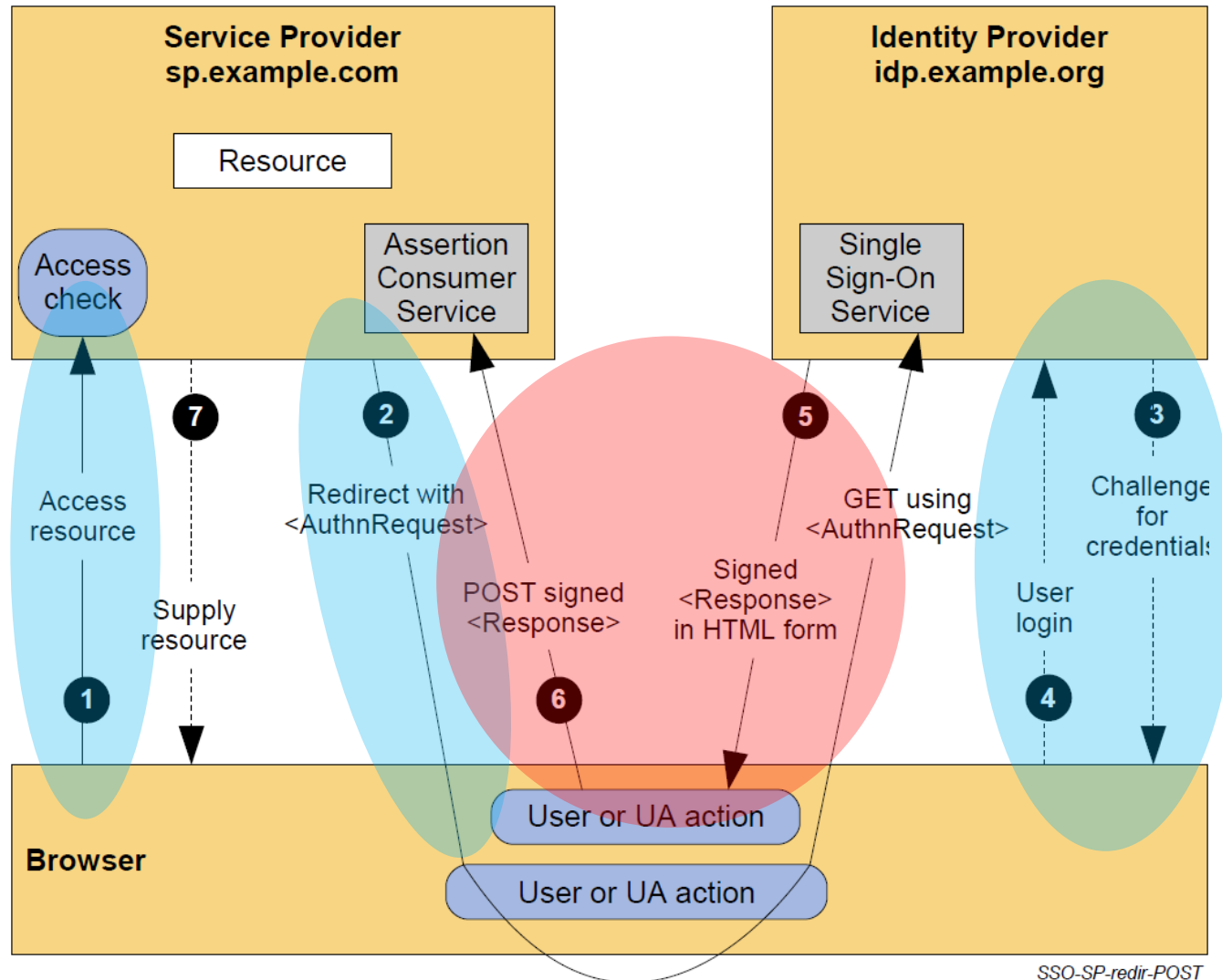
SAML defines a number of **protocol** messages, e.g. authentication request, artifact resolution or single logout

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

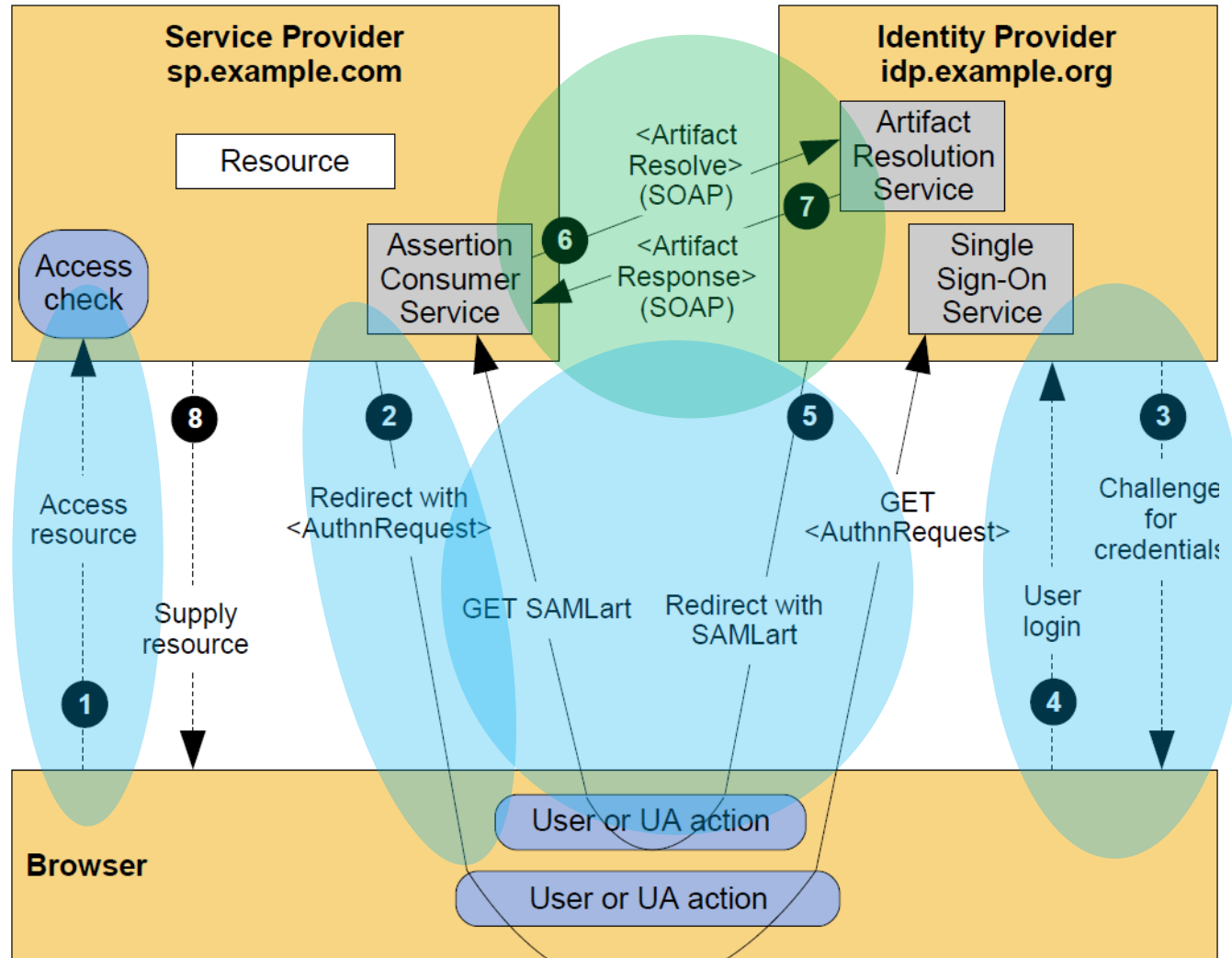


SSO-SP-redir-POST

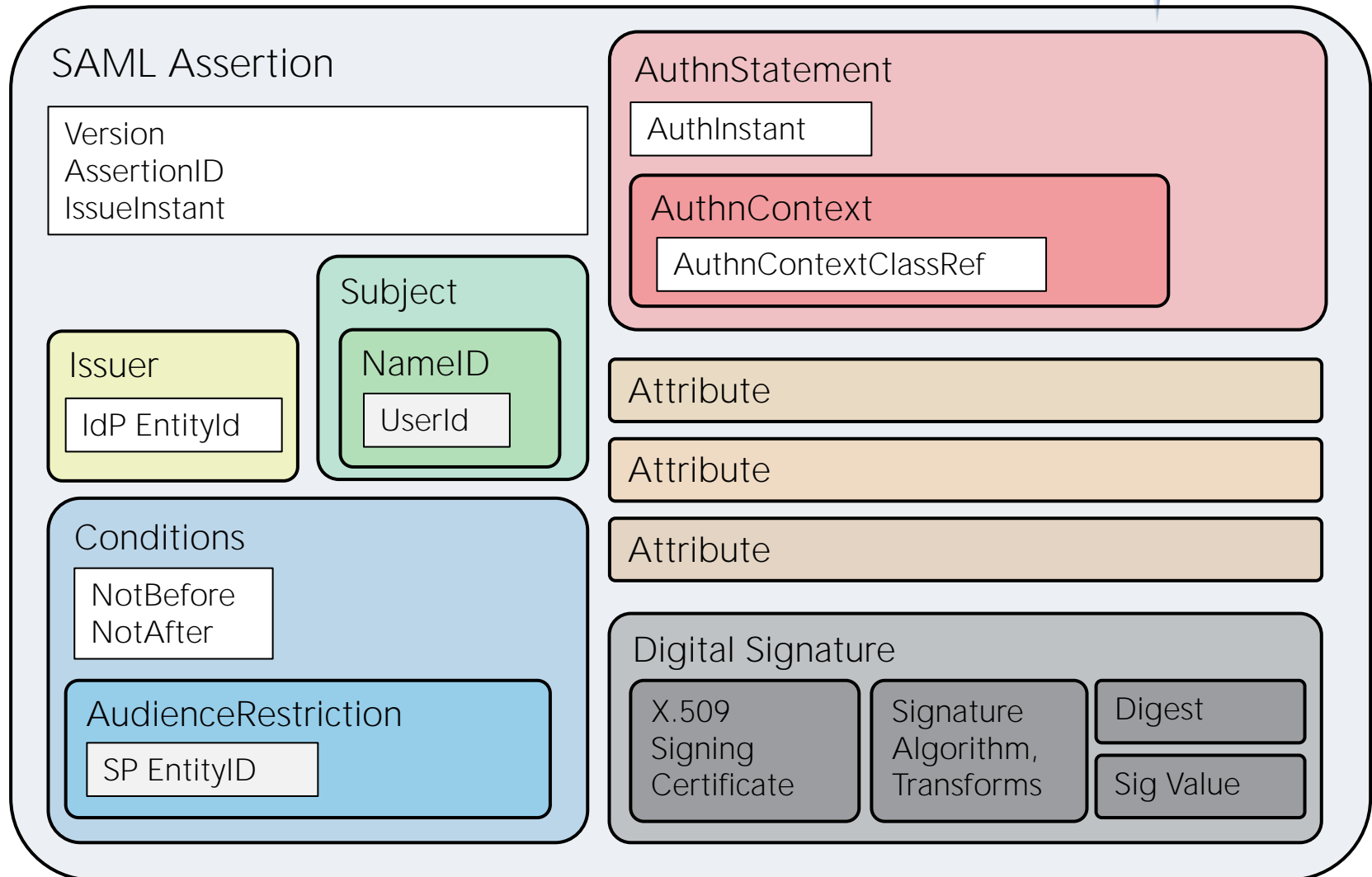
Web Browser SSO Profile (Artifact)



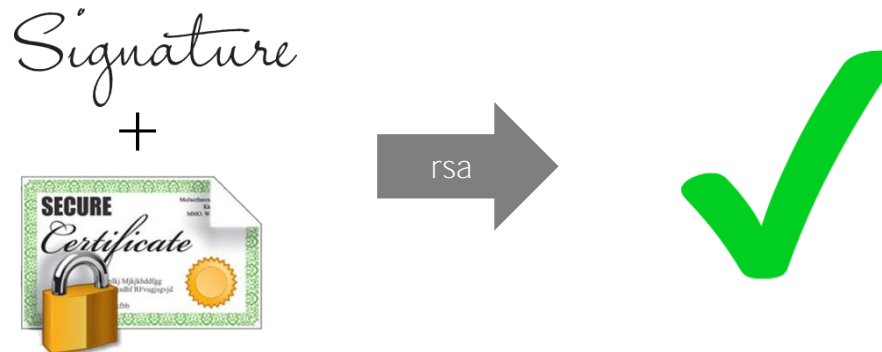
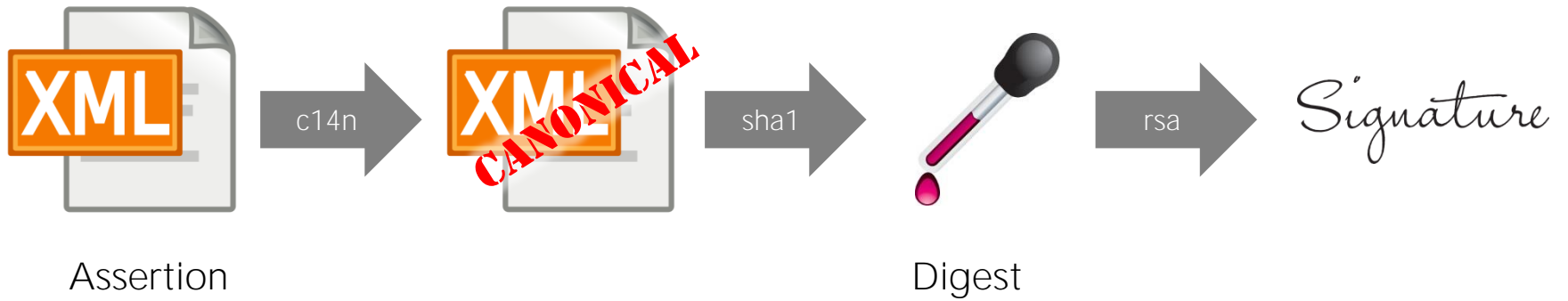
SP-Initiated SSO with POST/Artifact Bindings



SSO-SP-POST-art



XML Signature

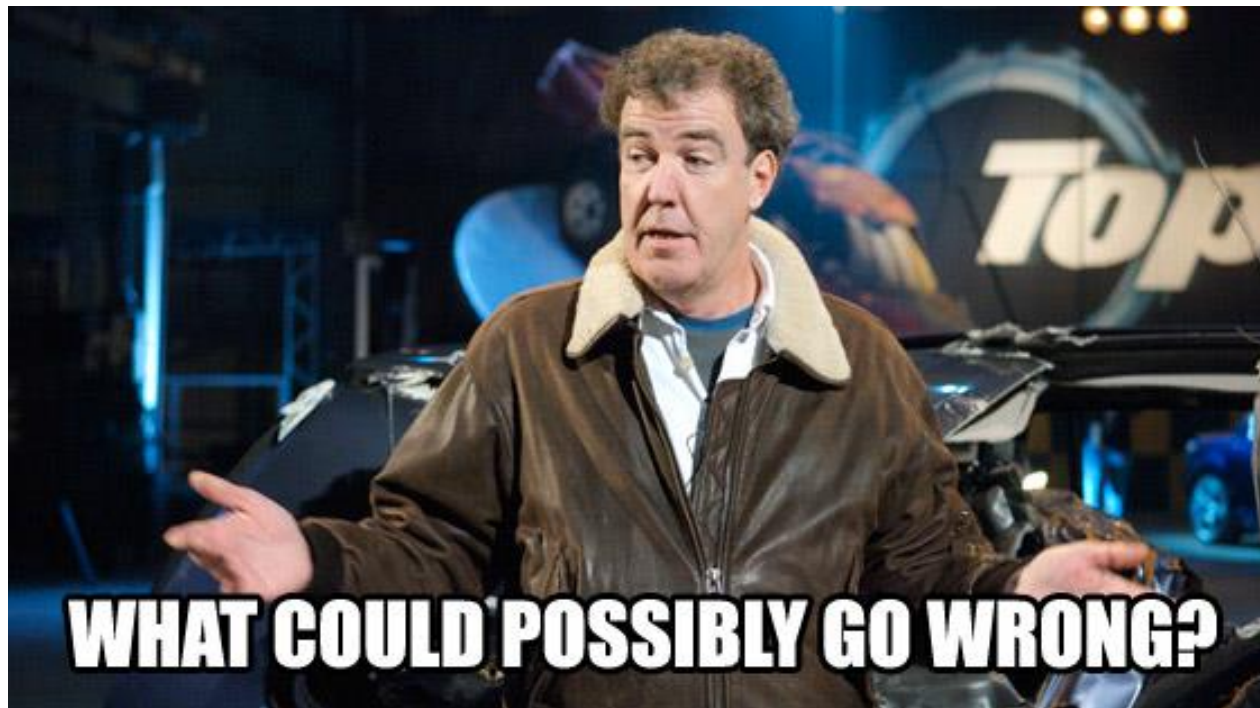




SAML ATTACKS

Technologies

- ◆ SAML
- ◆ XML Signatures
- ◆ X.509 Certificates





Security is hard

about
geocreepy



The road to hell is paved with SAML Assertions

Posted on Τετ 27 Απρίλιος 2016 in [bounty](#)

TL;DR

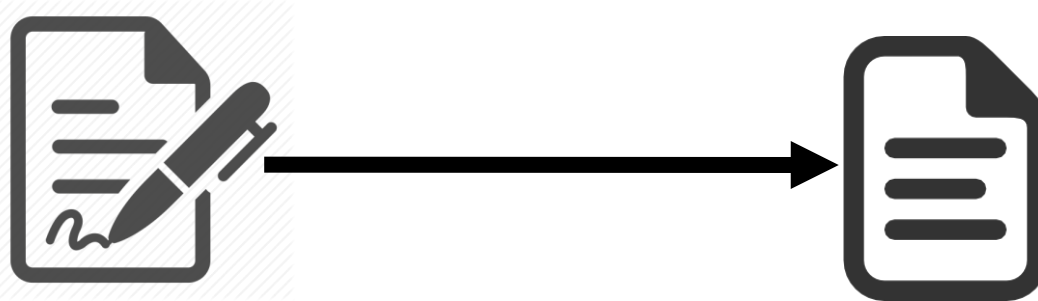
A vulnerability in Microsoft Office 365 SAML Service Provider implementation allowed for cross domain authentication bypass affecting **all** federated domains. An attacker exploiting this vulnerability could gain unrestricted access to a victim's Office 365 account, including access to their email,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

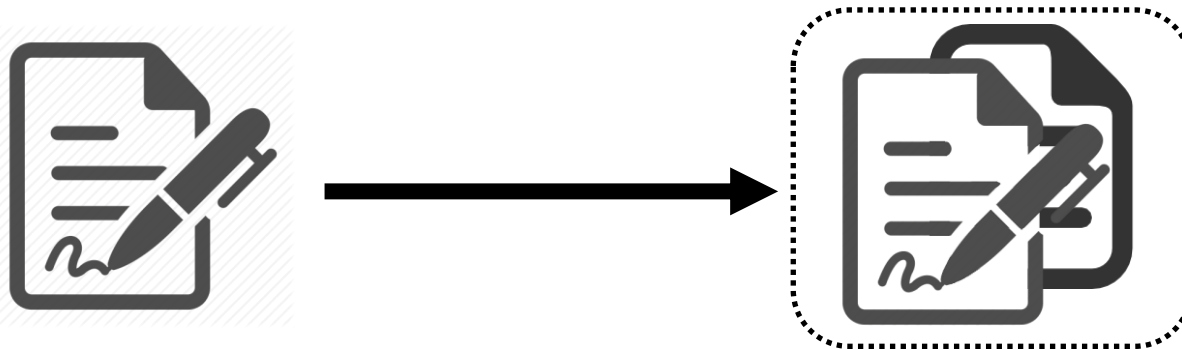
- ✦ Log out other users due to a guessable IDs
- ✦ Replay an eavesdropped SAML Message
 - ✦ Google for Messages, Stack Overflow

- ◆ Signature Exclusion (simply delete Signature)

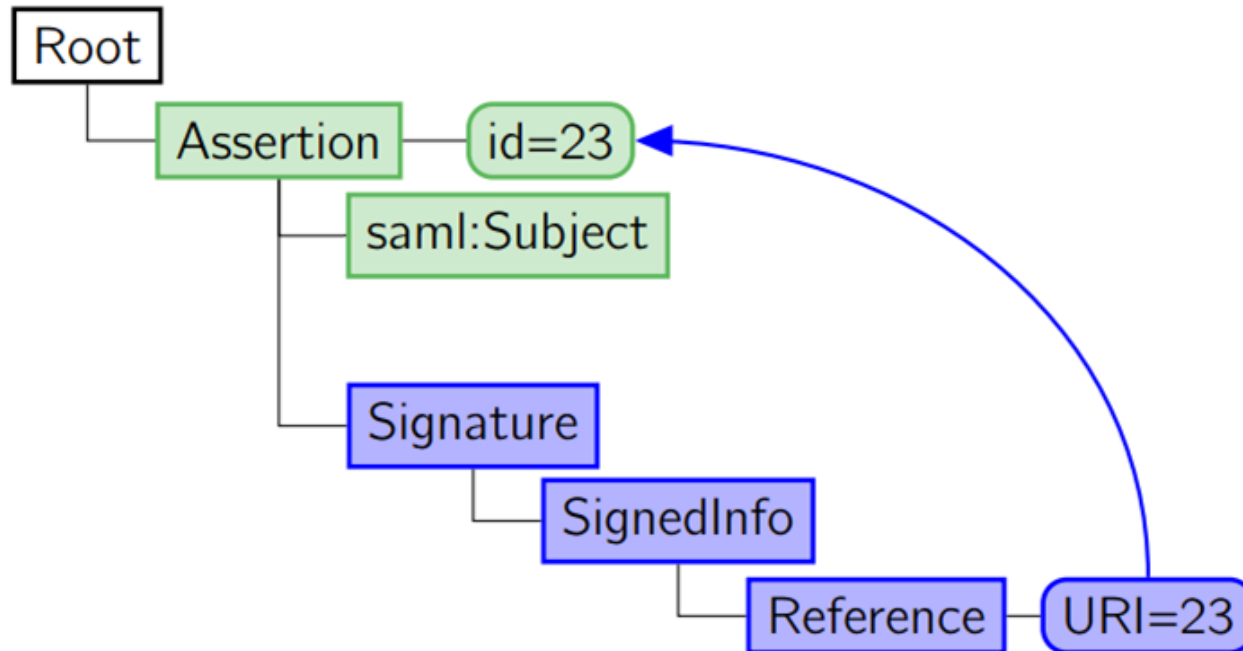


- ◆ XML Signature Wrapping

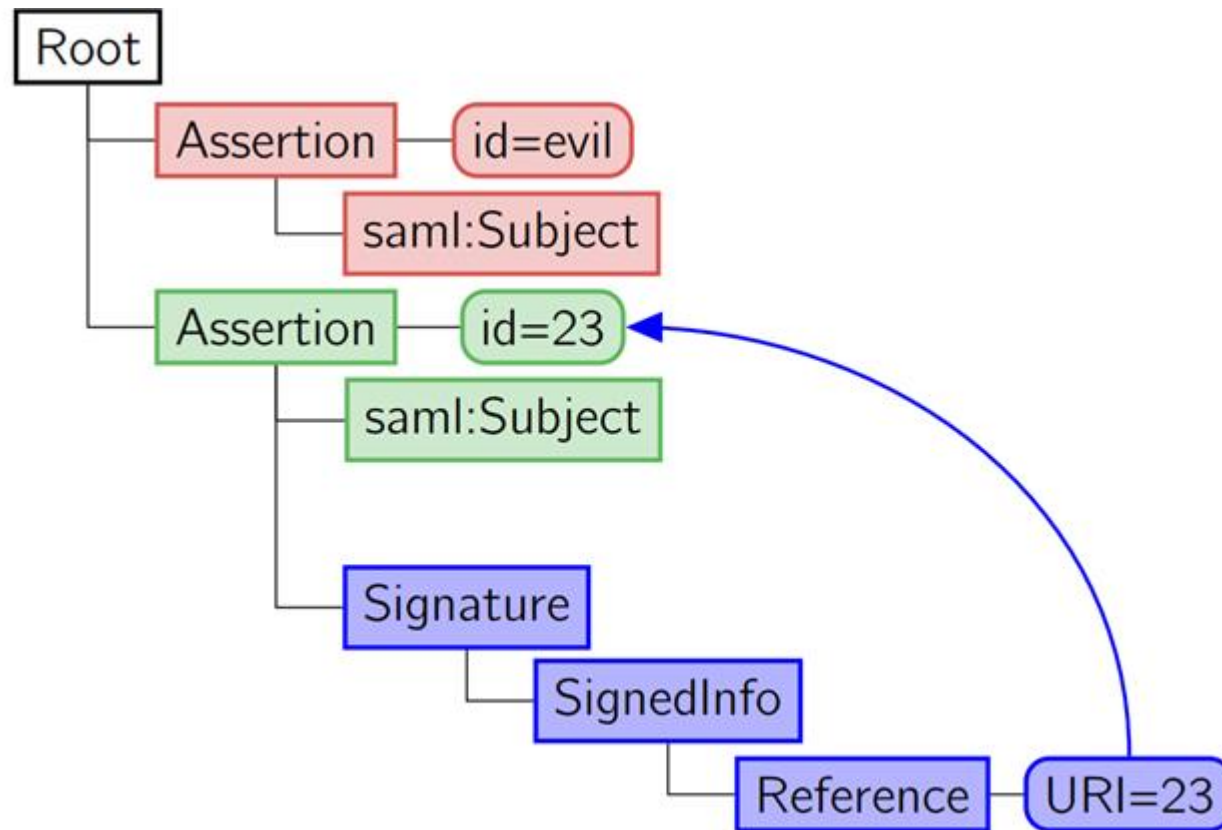
- ◆ Paper «On Breaking SAML: Be Whoever You Want to Be», 2012



◆ Normal Message



◆ Manipulated Message (XSW)



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



Found in June 2015 by Compass Security

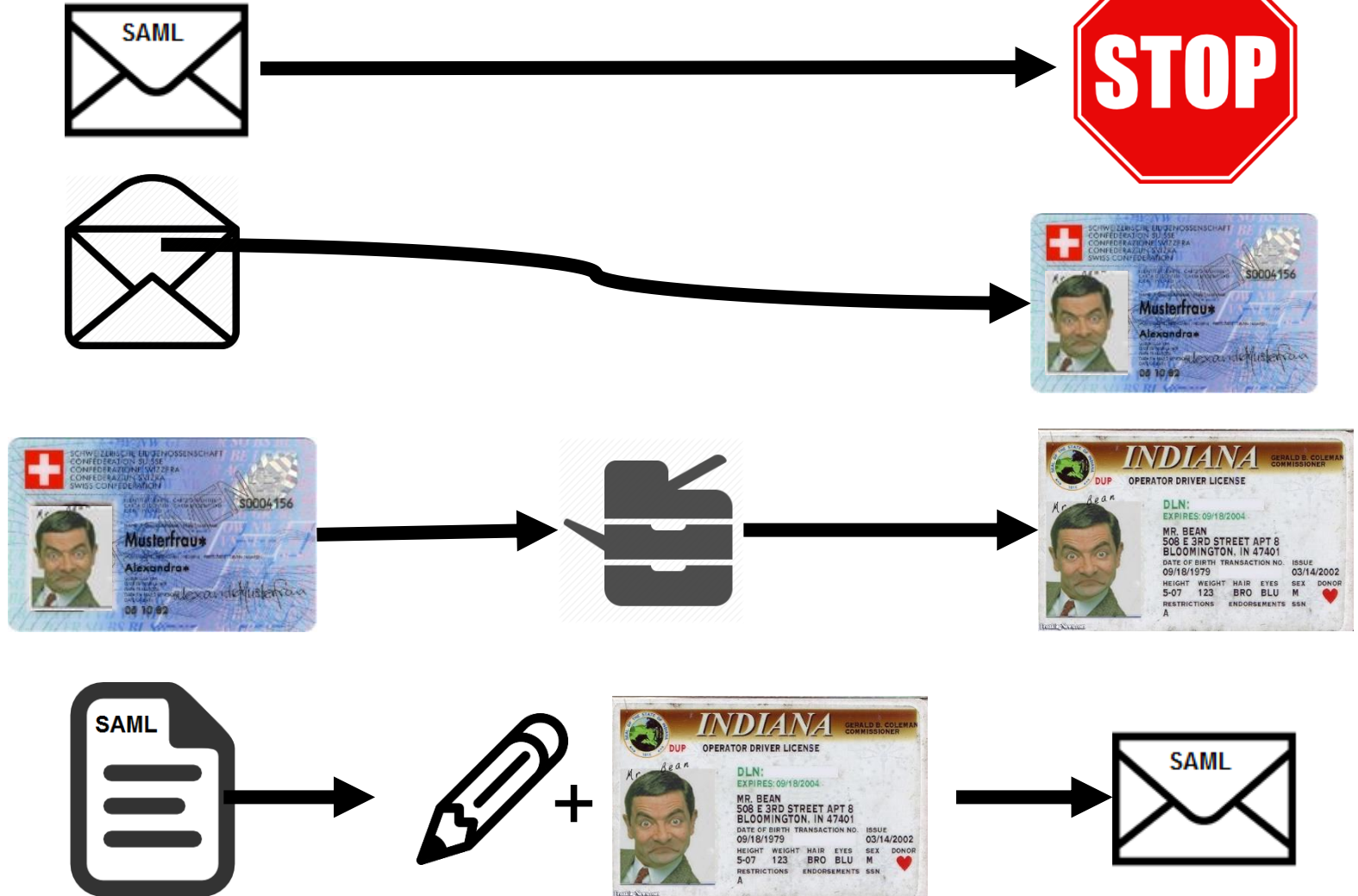
using SAML POST-Binding

not matching all attributes
of the X.509 certificate
embedded

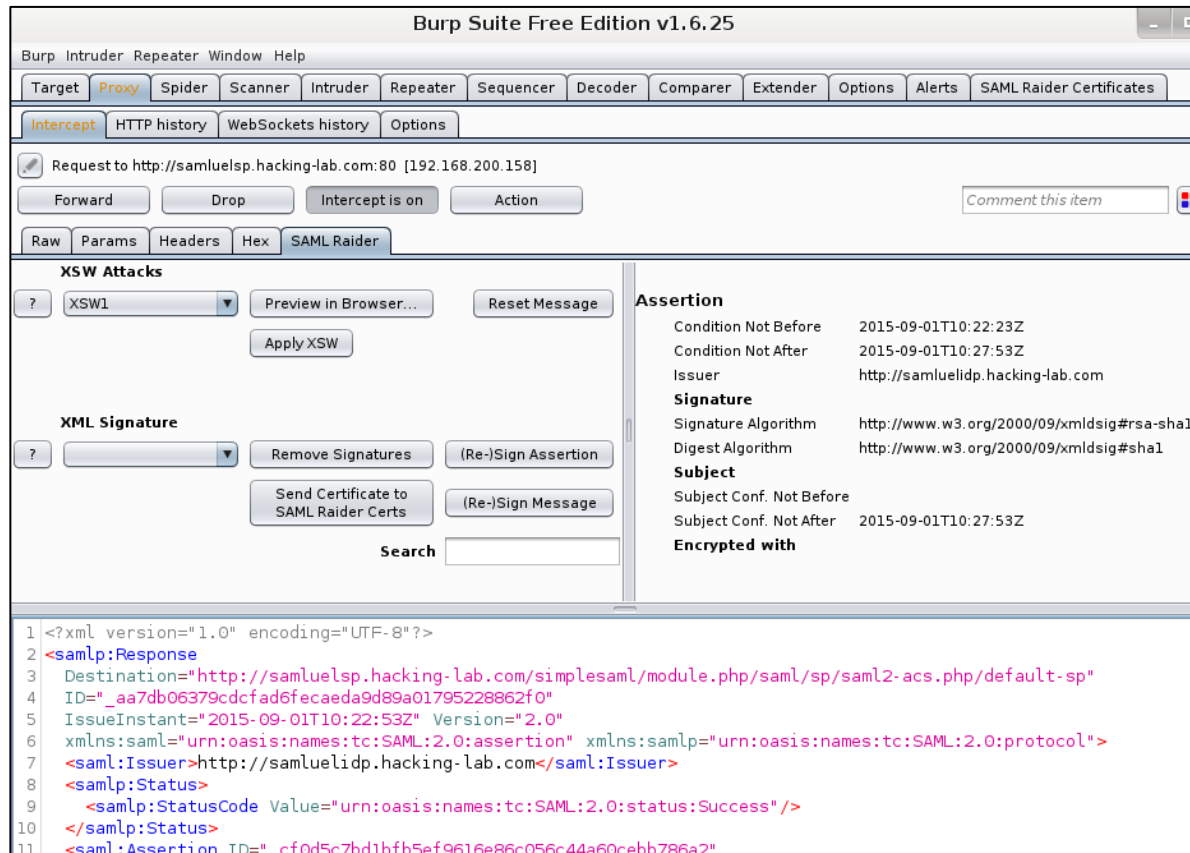
in the assertion against the
certificate from the
identity provider (IdP)

A screenshot of a web page from SECLISTS.ORG. The page has a dark purple header with a stylized eye logo and the text "SECLISTS.ORG". On the left side, there is a navigation menu with sections: "Nmap Security Scanner" (with sub-items: Intro, Ref Guide, Install Guide, Download, Changelog, Book, Docs), "Security Lists" (with sub-items: Nmap Announce, Nmap Dev, Bugtraq, Full Disclosure, Pen Test, Basics, More), and "Security Tools" (with sub-items: Password audit, Sniffers, Vuln scanners, Web scanners, Wireless, Exploitation, Packet crafters). The main content area shows a "FULL DISCLOSURE" banner, a search bar, and a list of mailing list archives. The selected archive is titled "SAML SP Authentication Bypass". Below the title, it shows the sender "Antoine Neuenschwander <Antoine.Neuenschwander () csnc ch>" and the date "Mon, 21 Sep 2015 12:02:27 +0000". The body of the email contains a "COMPASS SECURITY ADVISORY" with a link to "http://www.csnc.ch/en/downloads/advisories.html". The advisory details include: Product: Authentication Bypass, Vendor: Critical, CVD ID: Remotely exploitable, Subject: Authentication Bypass, Risk: Critical, Effect: Remotely exploitable, Authors: Antoine Neuenschwander (antoine.neuenschwander () csnc ch) and Roland Bischofberger (roland.bischofberger () csnc ch), and Date: 2015-09-21.

Demo Exploit



SAMLRaider Extension for Burp



Burp Suite Free Edition v1.6.25

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

Forward Drop Intercept is on Action

Raw Params Headers Hex **SAMLRaider**

XSW Attacks

XSW1 Preview in Browser... Reset Message Apply XSW

XML Signature

Remove Signatures (Re-)Sign Assertion Send Certificate to SAMLRaider Certs (Re-)Sign Message Search

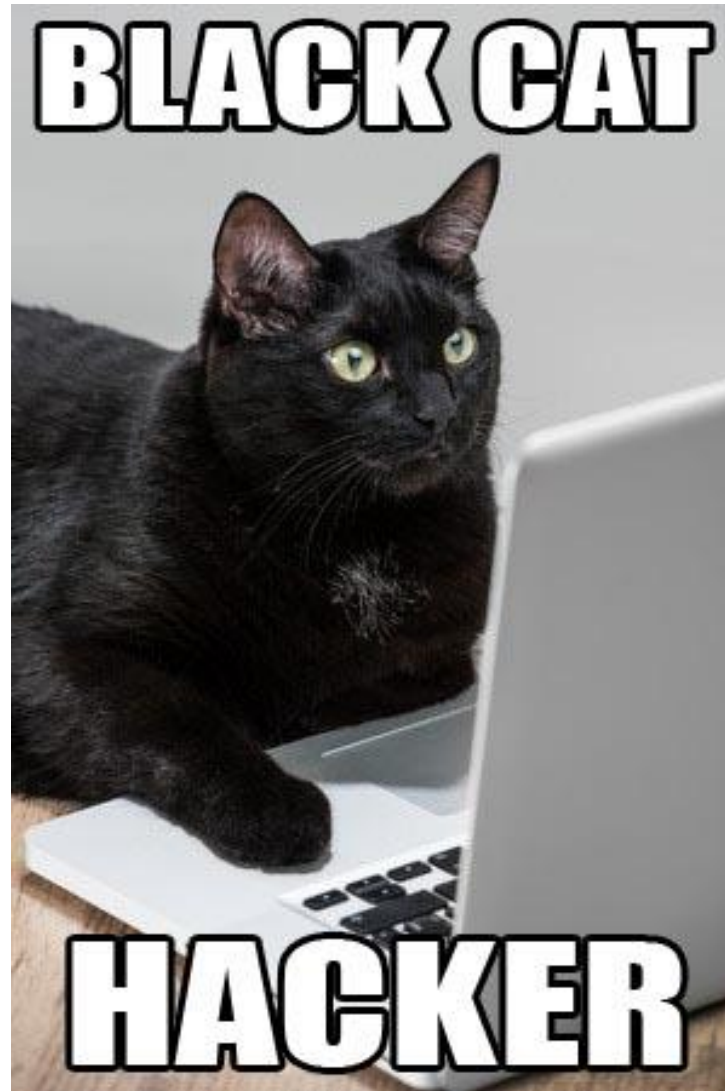
Assertion

Condition Not Before 2015-09-01T10:22:23Z
 Condition Not After 2015-09-01T10:27:53Z
 Issuer <http://samuelidp.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
Encrypted with

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <samlp:Response
3   Destination="http://samluelsp.hacking-lab.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp"
4   ID="_aa7db06379cdcfd6fecaeda9d89a01795228862f0"
5   IssueInstant="2015-09-01T10:22:53Z" Version="2.0"
6   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
7   <saml:Issuer>http://samuelidp.hacking-lab.com</saml:Issuer>
8   <samlp:Status>
9     <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
10  </samlp:Status>
11  <saml:Assertion ID="cf0d5c7bd1bfb5ef9616e86c056c44a60cebb786a2">
    
```

<https://github.com/SAMLRaider/SAMLRaider>





REMEDiations

- ✦ 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>

