



With Great Power Comes Great Pwnage

Yverdon, November 3rd 2016

roland.bischofberger@compass-security.com

emanuel.duss@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

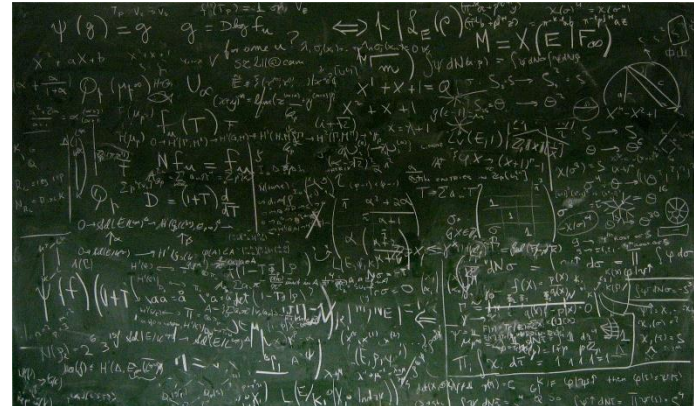
Hello



- ◆ Emanuel Duss
- ◆ Roland Bischofberger

- ◆ Security Analysts at Compass Security Schweiz

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



- ◆ SAML Attacks
- ◆ Demo
- ◆ Remediation





Security

Crossdomain

Assertion

Markup

**Such
wow!**

**single
sign-on**

Language



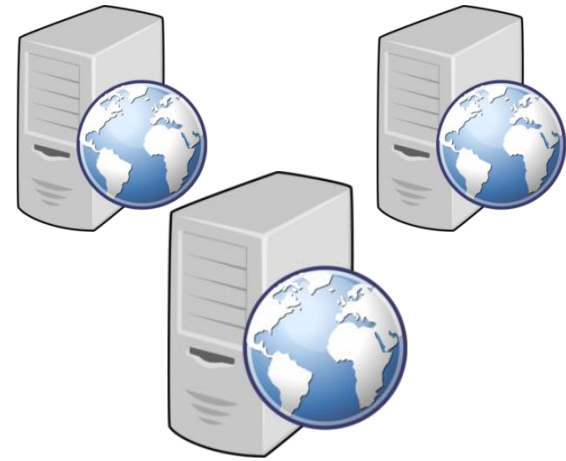


Client / User
Entity that wants to assert a particular identity



Identity Provider (IdP)

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



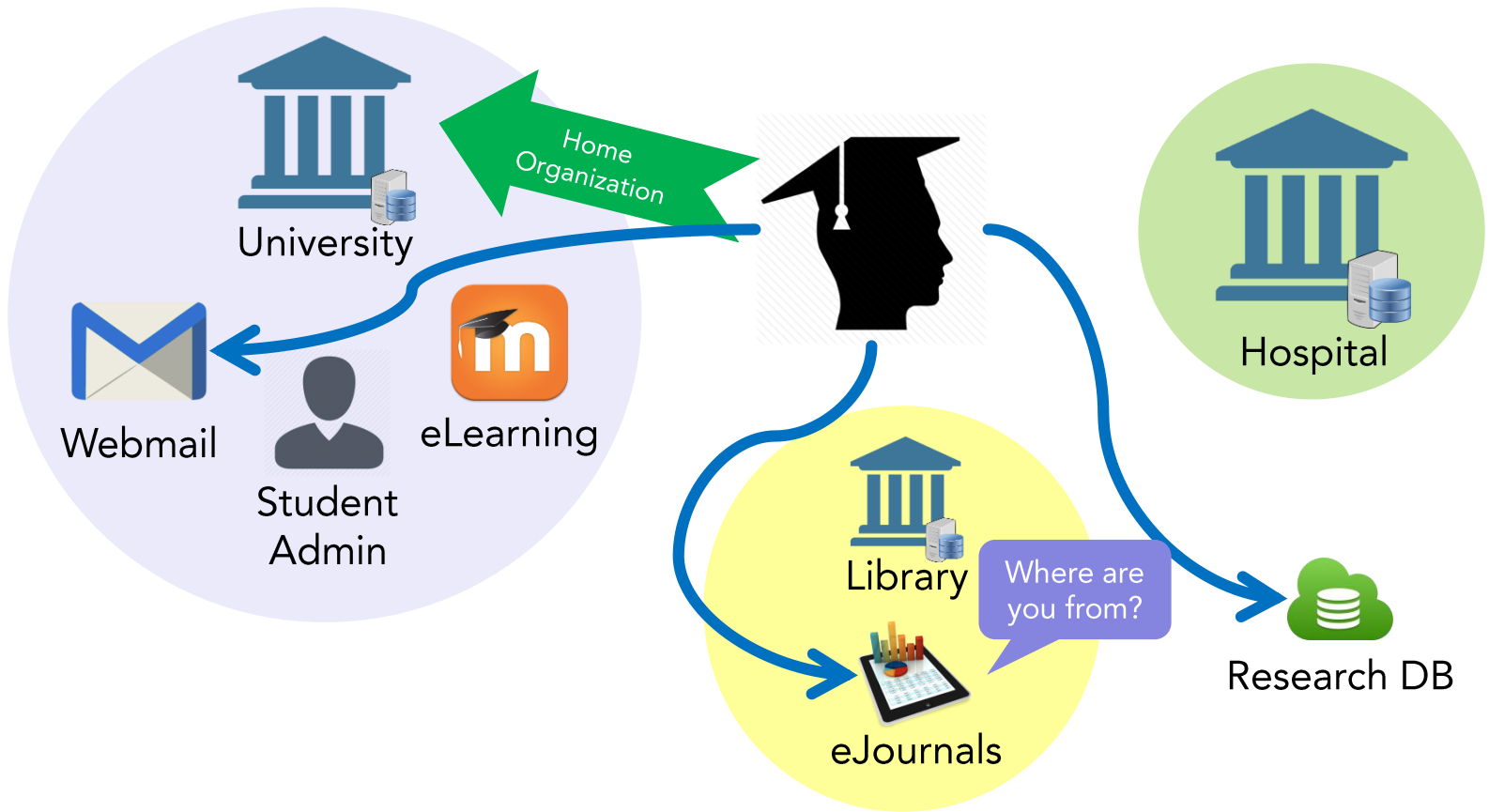
Service Providers (SP)

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



USE-CASES

SWITCH



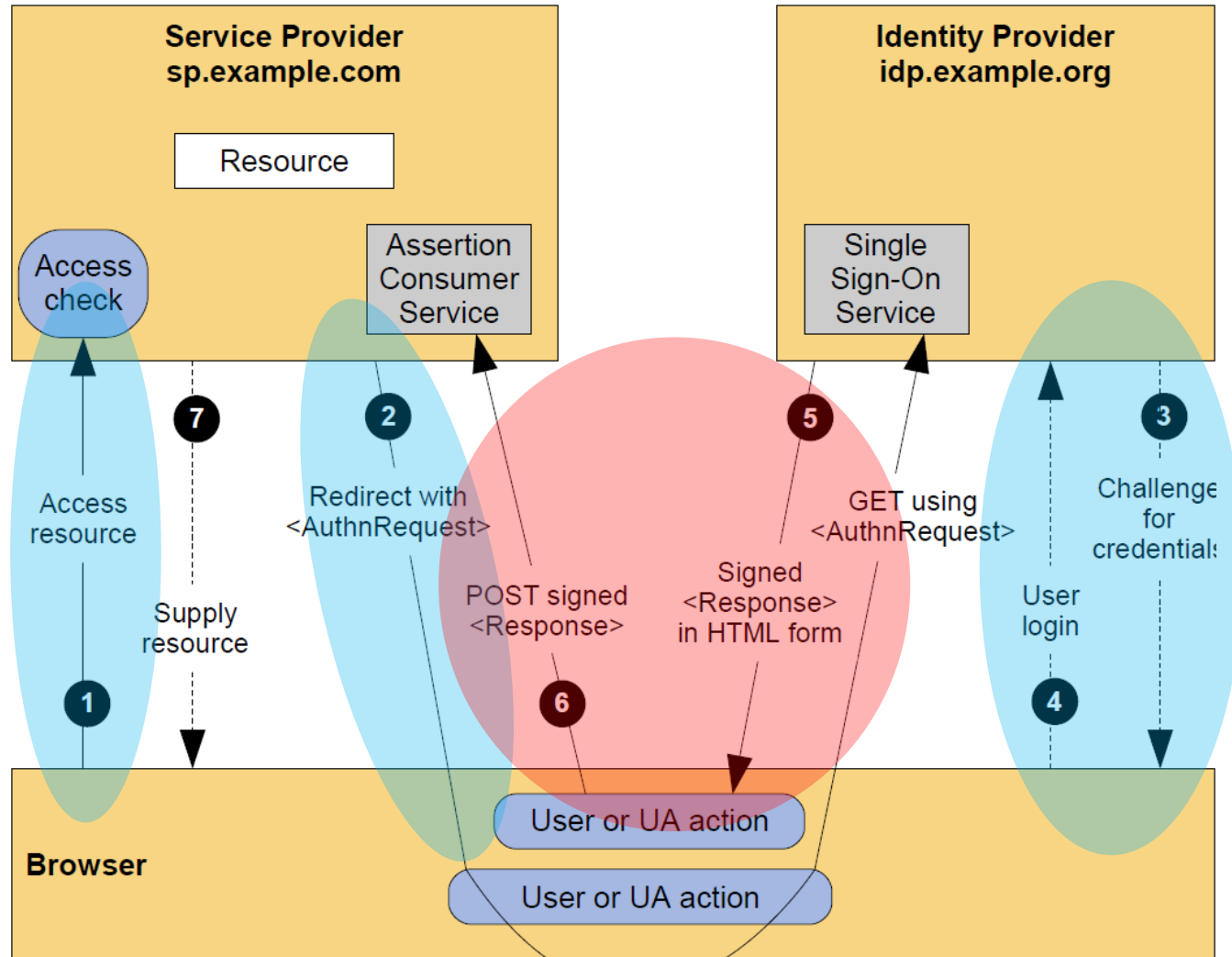
A vertical decorative strip on the left side of the slide features a close-up, slightly blurred image of a computer keyboard. A yellow metal padlock is placed over the keys, symbolizing security. The background of the slide is white with a horizontal dotted line near the top.

SAML 2.0 FUNDAMENTALS

Web Browser SSO Profile



SP-Initiated SSO with Redirect and POST Bindings

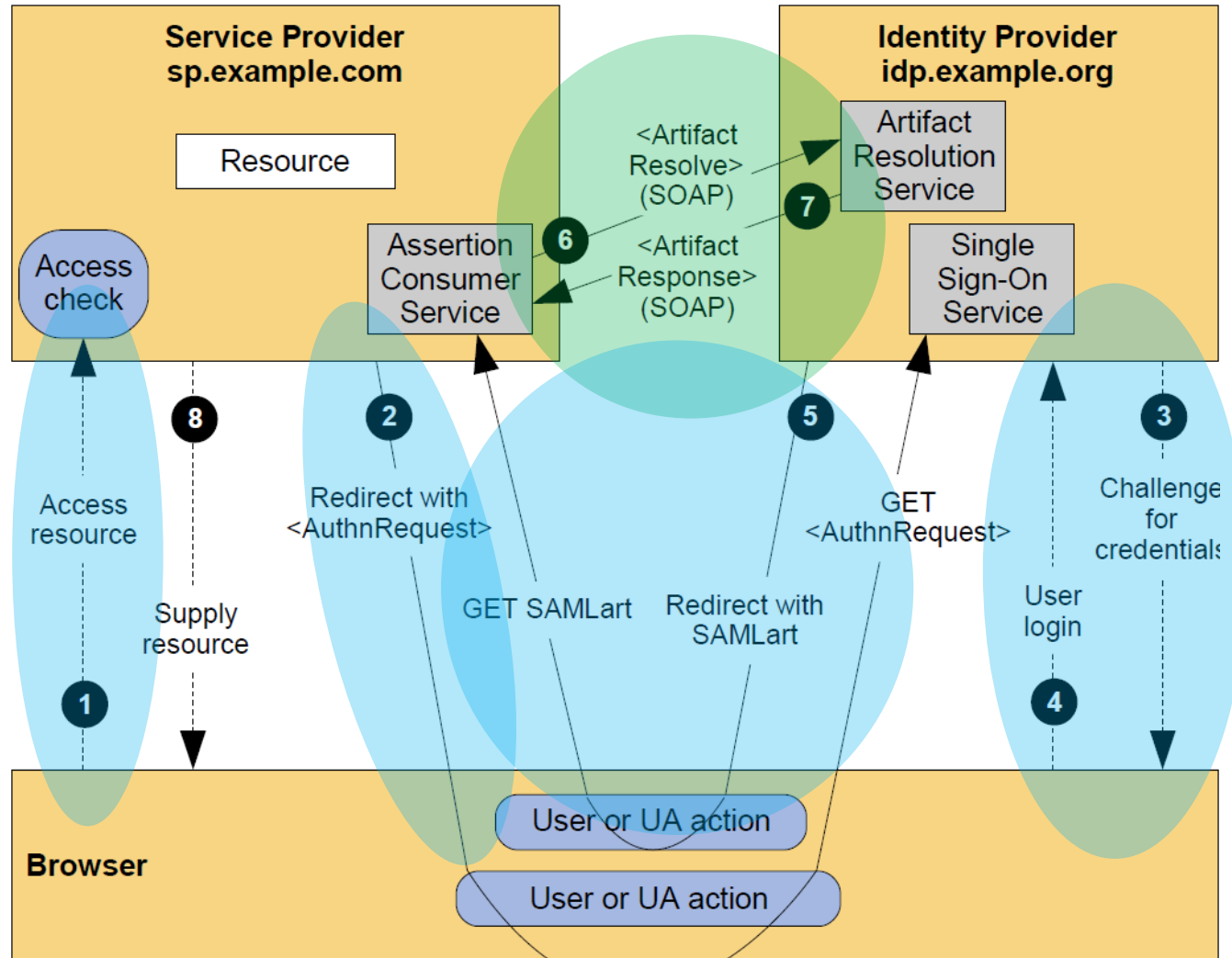


SSO-SP-redir-POST

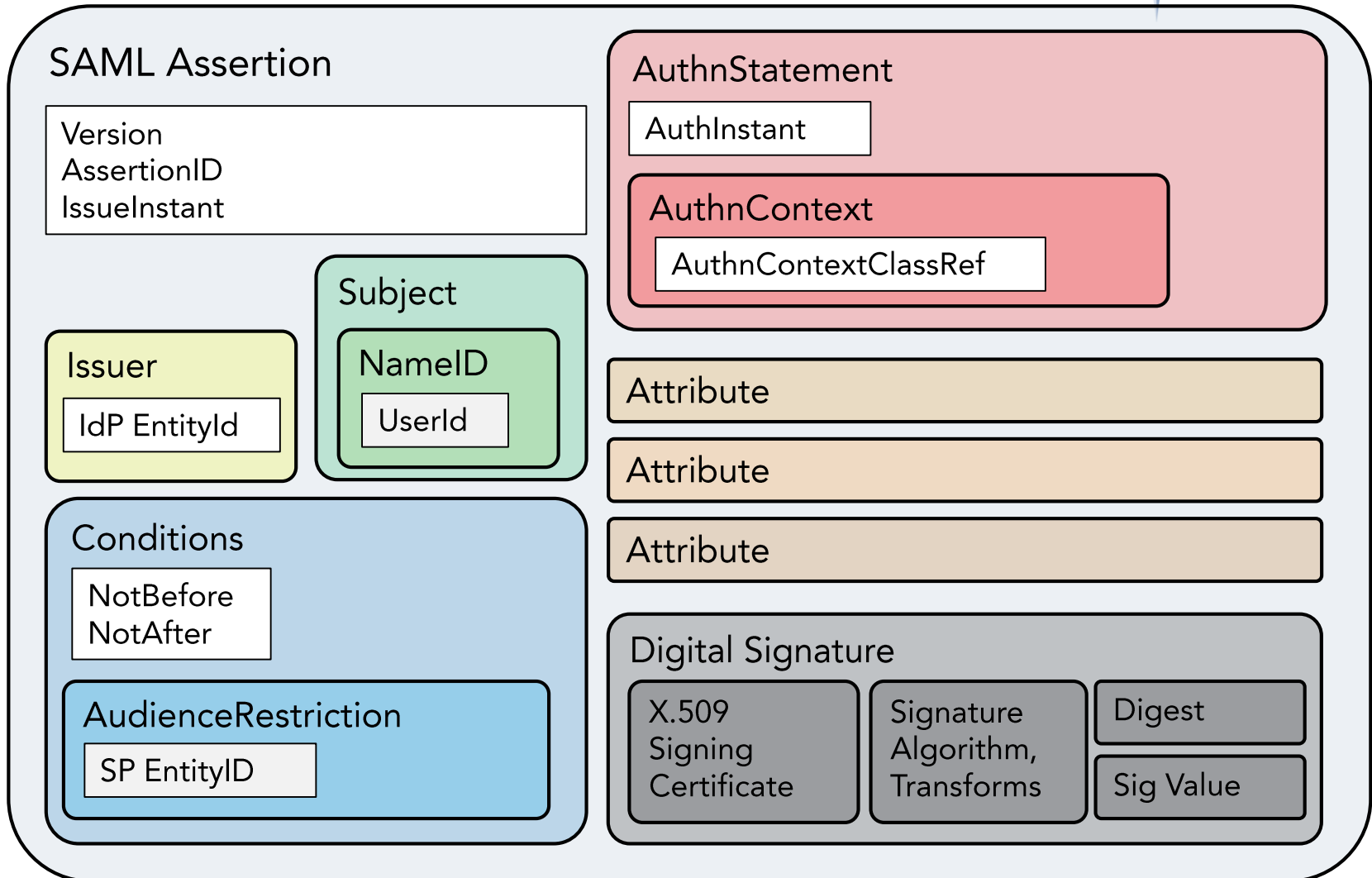
Web Browser SSO Profile (Artifact)



SP-Initiated SSO with POST/Artifact Bindings



SSO-SP-POST-art

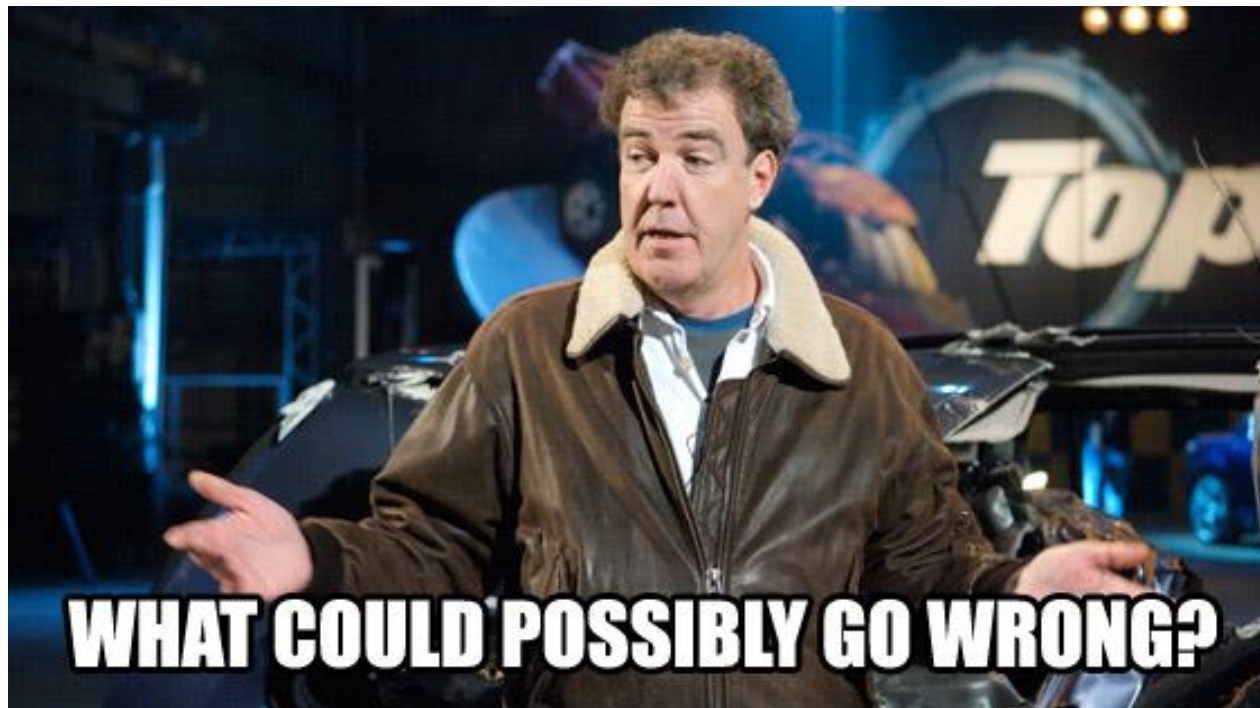


A vertical decorative strip on the left side of the slide. It features a close-up of a yellow padlock on a silver metal shackle, resting on a light blue computer keyboard. The background of the strip is a blurred, light blue and white pattern.

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 Απριλίου 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.

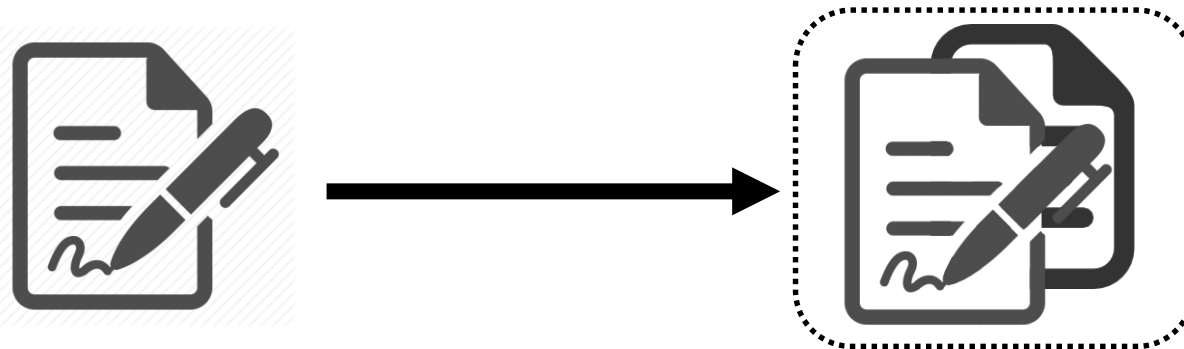
<http://www.economyofmechanism.com/office365-authbypass.html>

- ◆ Signature Exclusion (simply delete Signature)

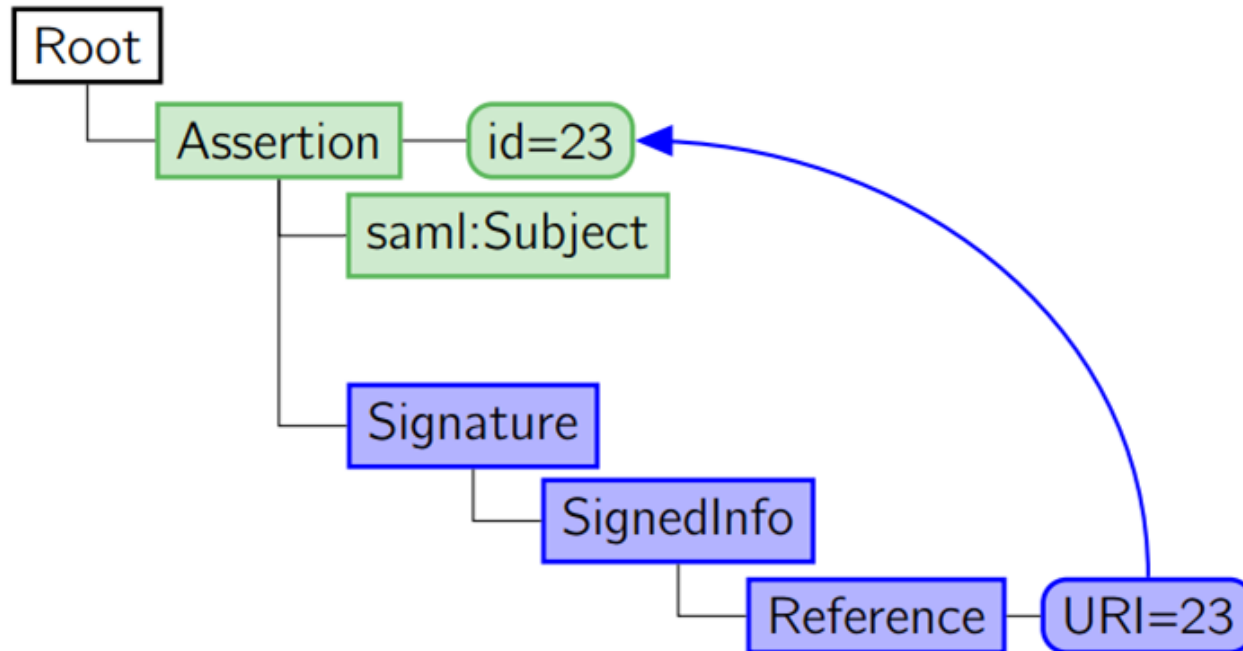


- ◆ XML Signature Wrapping

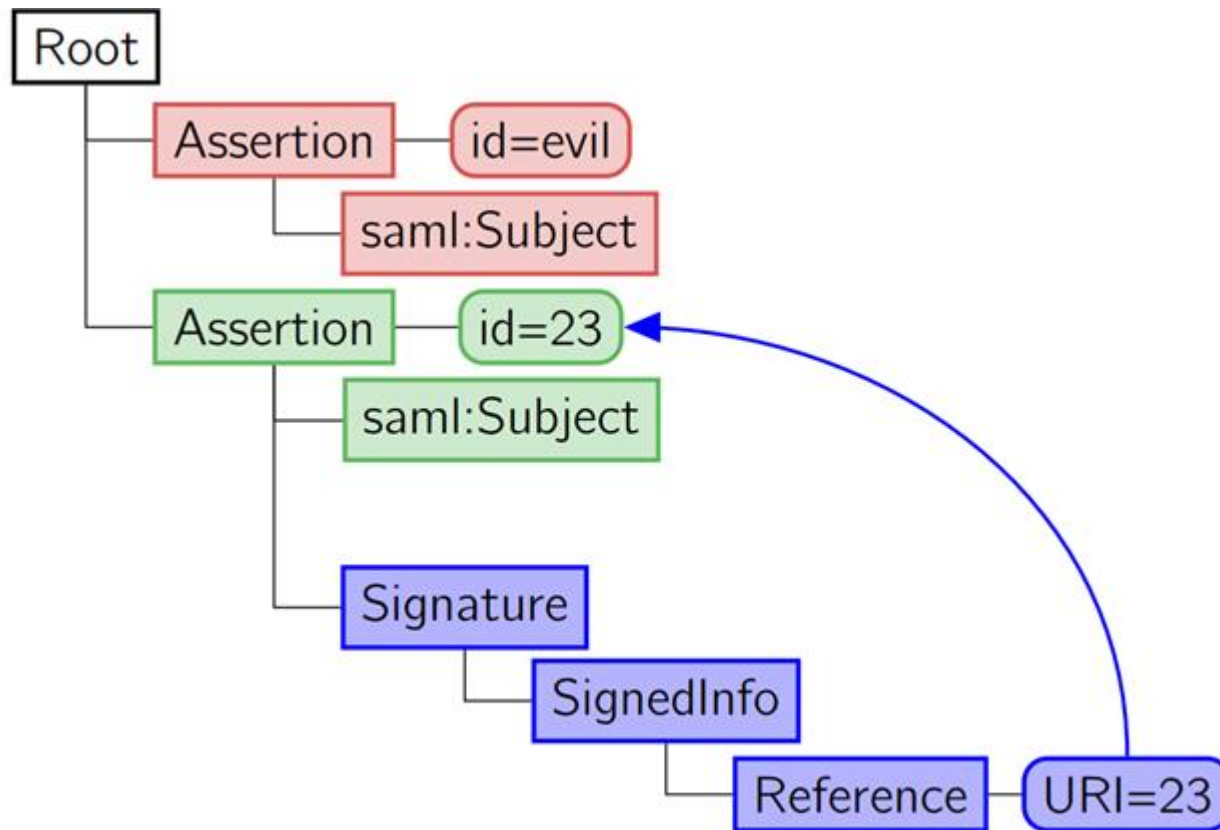
- ◆ Paper «On Breaking SAML: Be Whoever You Want to Be», 2012



◆ Normal Message



◆ Manipulated Message (XSW)



Precondition: Certificate is embedded in the message

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



Found in June 2015 by Compass Security

Using SAML POST-Binding

Validated the signature with the embedded certificate

Embedded certificate not correctly compared to local one (IdP certificate)

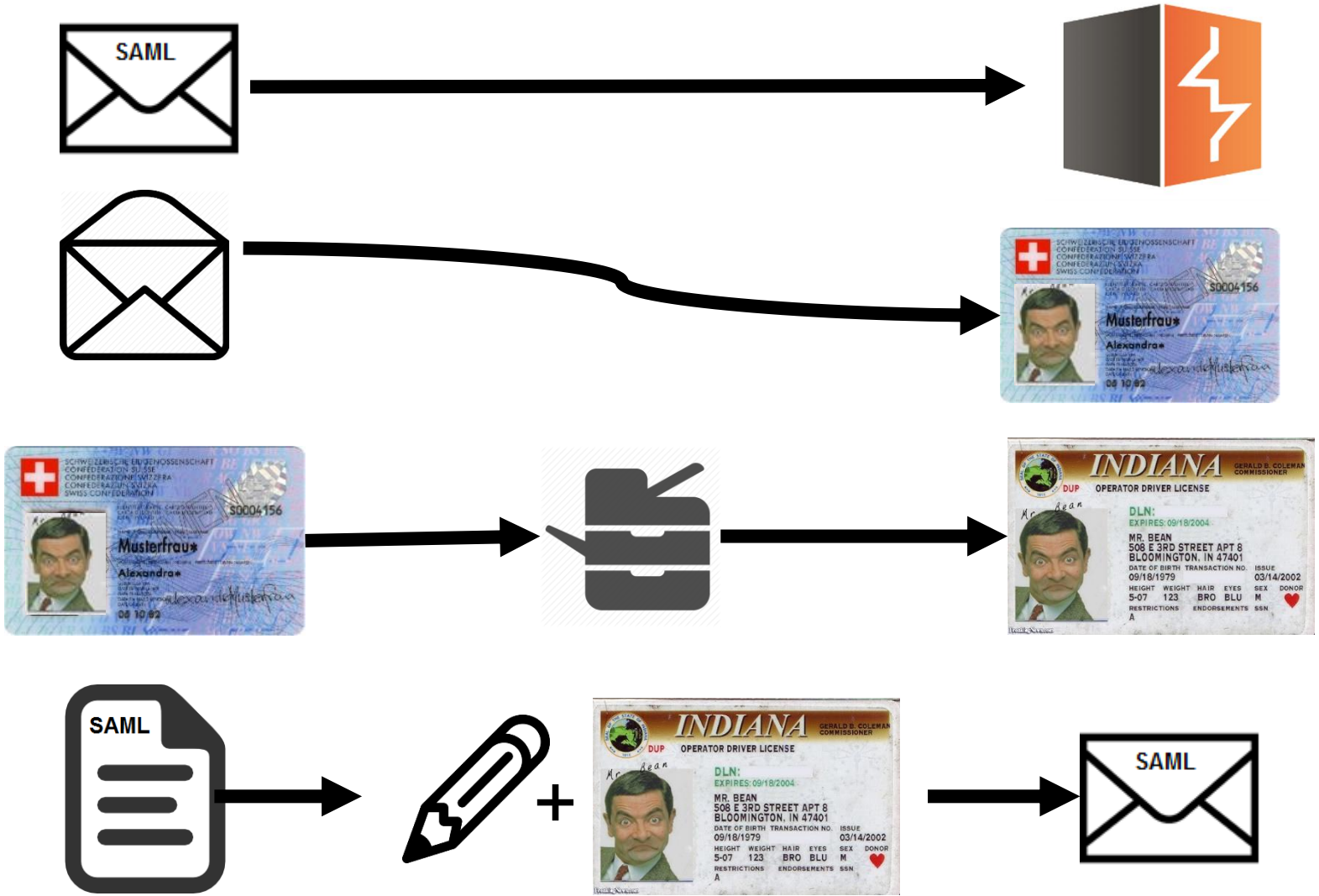
Sign assertion with arbitrary content by using self generated key material



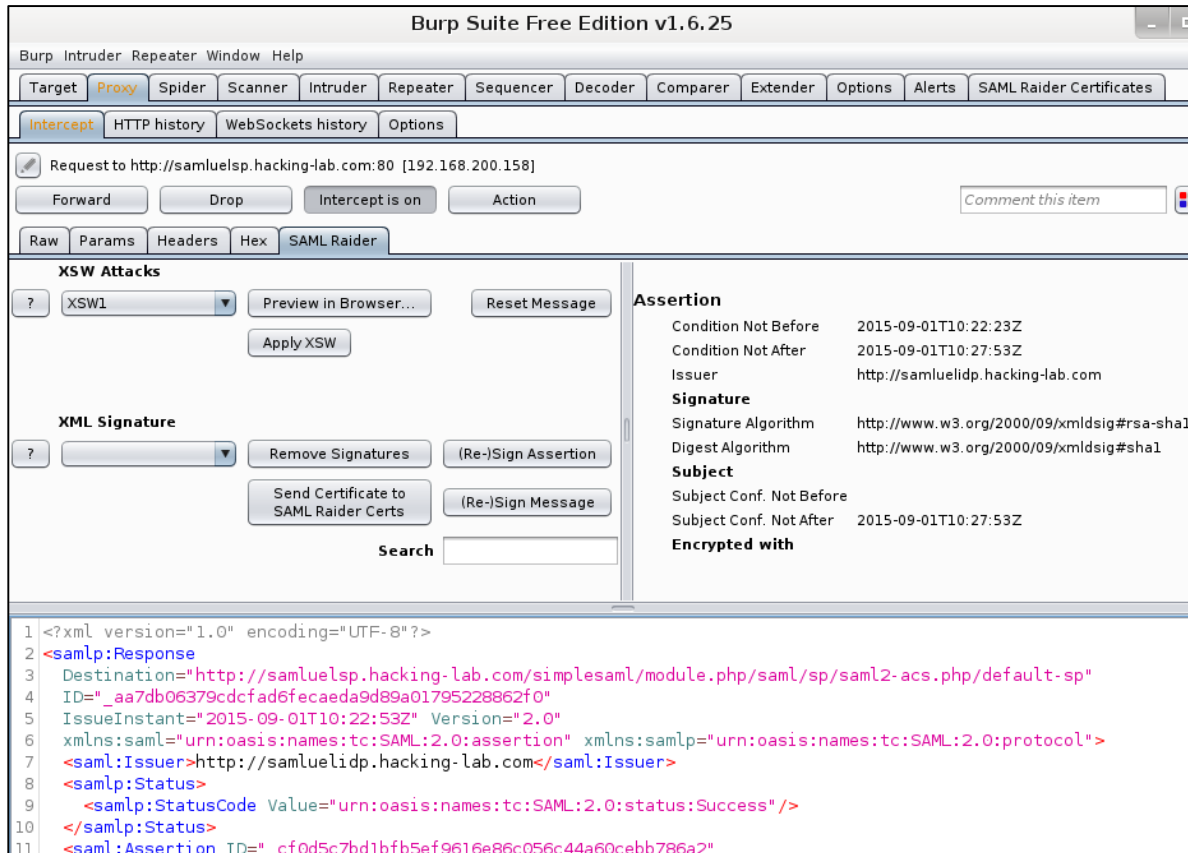
The screenshot shows a web interface for a mailing list archive. On the left is a navigation menu for 'SECLISTS.ORG' with categories like 'Nmap Security Scanner', 'Security Lists', and 'Security Tools'. The main content area displays an email from Antoine Neuenschwander with the subject 'SAML SP Authentication Bypass'. The email body contains a security advisory header with fields for Product, Vendor, CVD ID, Subject, Risk, Effect, and Authors.

```
#####  
#  
# COMPASS SECURITY ADVISORY  
# http://www.csnc.ch/en/downloads/advisories.html  
#  
#####  
# Product:  
# Vendor:  
# CVD ID:  
# 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



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 Comment this item

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="_aa7db06379cdcfad6fecaeda9d89a01795228862f0"
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 (IdP sends assertion directly to SP)
 - ✦ 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
- ✦ Testing: Test your Implementation (with SAMLRaider ;-))

Questions?



Links:

Bachelor Thesis:

<https://eprints.hsr.ch/464/>

SAMLRaider on Github:

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

SAMLRaider in BApp Store:

<https://portswigger.net/bappstore/>

