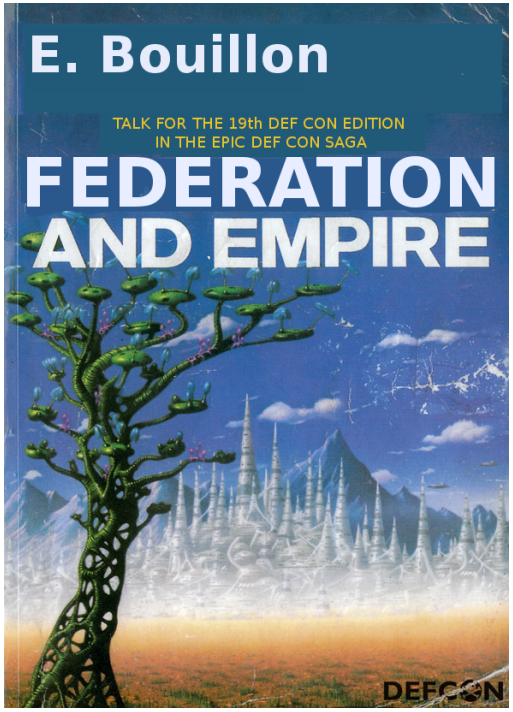
Federation & Empire

Emmanuel Bouillon
manu@veryopenid.net

DEF CON #19 - 7th August 2011



Prefatory notes

$ whoami

- Having fun in INFOSEC for a while
- SSTIC, PacSec, BlackHat EU, Hack.lu, #Days
- CVE-2010-{0283,2229,2914,2941,...}, CVE-2011-{0001,...}

Disclaimer

- This expresses my own views and does not involve my previous, current and future employers and thus for ten generations
- Presentation and code provided for educational purpose only

Prefatory notes

$ whoami

- Having fun in INFOSEC for a while
- SSTIC, PacSec, BlackHat EU, Hack.lu, #Days
- CVE-2010-{0283,2229,2914,2941,...}, CVE-2011-{0001,...}

Disclaimer

- This expresses my own views and does not involve my previous, current and future employers and thus for ten generations
- Presentation and code provided for educational purpose only

Outline

1. Prelude to Federation
   - Introduction
2. Forward the Federation
   - Where we come from
3. Federation
   - What you need to know
4. Federation and Empire
   - Sharpen your weapons
5. Federation's Edge
   - Design assessment
6. Federation and (down to) Earth
   - Conclusion

Outline

1. Prelude to Federation
   - Introduction
2. Forward the Federation
   - Where we come from
3. Federation
   - What you need to know
4. Federation and Empire
   - Sharpen your weapons
5. Federation's Edge
   - Design assessment
6. Federation and (down to) Earth
   - Conclusion

What is it about?

What it is not

This relates to

- SAML Token and Claims based IAM
- Low level, Pen-tester approach

Won't discuss

- Formal protocol/API comparison
- Consistent standards study

What is it about?

What it is not

This relates to

- SAML Token and Claims based IAM
- Low level, Pen-tester approach

Won't discuss

- Formal protocol/API comparison
- Consistent standards study

Why should you care?

- Pervasive
- Cloud
- Joining a federation usually has severe contractual, legal implications.
- It's coming your way!

Outline

1. Prelude to Federation
   - Introduction
2. Forward the Federation
   - Where we come from
3. Federation
   - What you need to know
4. Federation and Empire
   - Sharpen your weapons
5. Federation's Edge
   - Design assessment
6. Federation and (down to) Earth
   - Conclusion

The main problem to solve

- User and Administrator friendly cross organization boundaries SSO - here for web apps
  - Secure
  - Scalable
  - Manageable
  - Privacy / Anonymity
- Ideally compliant with the Laws of Identity [5]

Historical approaches

The good old time

- Account Replication
  - Manual
  - Automated
- WHAT?
  - Lose control of accounts, or
  - Have multiple passwords
- "Trust" relationships to be established with other realms / domains
  - All user information shared with federated partners
  - Firewalls need to be opened to allow trust
  - Bilateral $\Rightarrow n^2$ problem - no easy way to establish trust with multiple partners
- Privacy / anonymity
  - Anonymity Support for Kerberos [1]

Outline

1 Prelude to Federation
- Introduction

2 Forward the Federation
- Where we come from

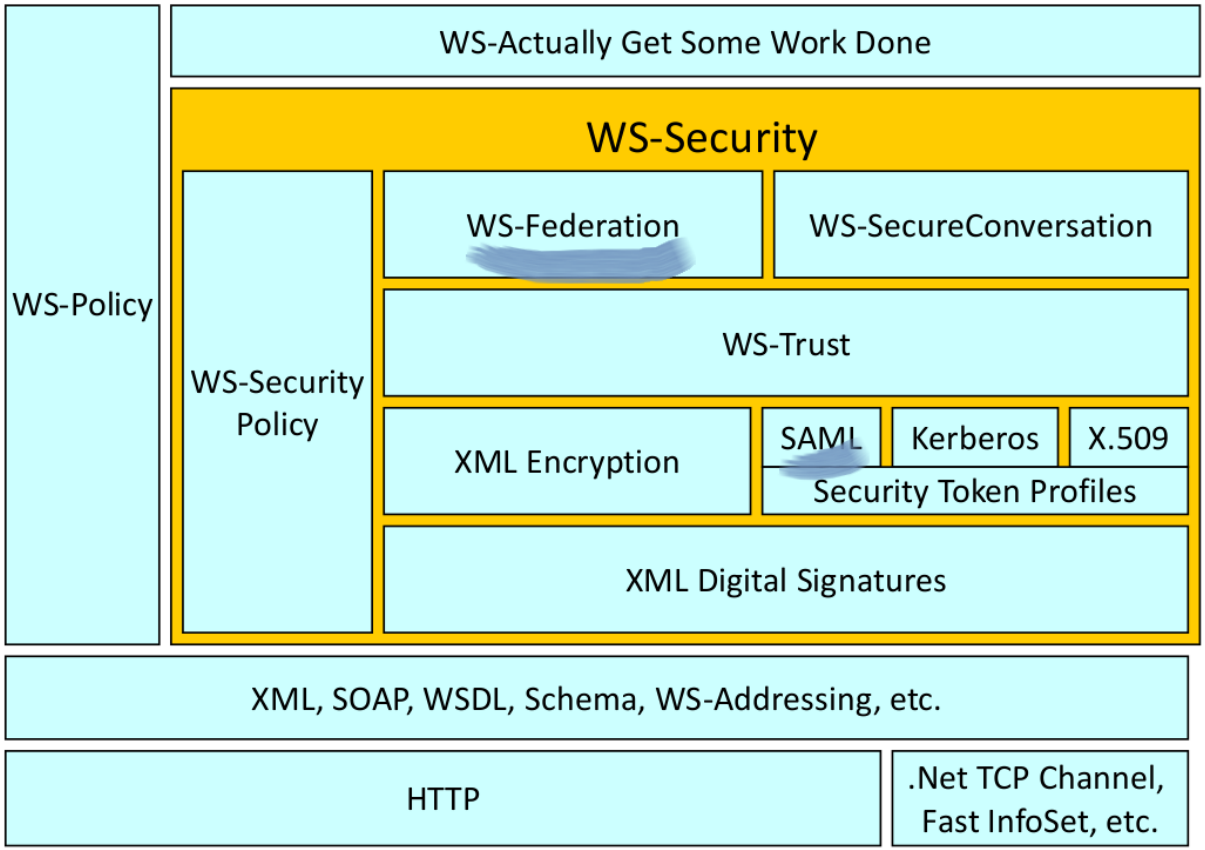
3 Federation
- What you need to know

4 Federation and Empire
- Sharpen your weapons

5 Federation's Edge
- Design assessment

6 Federation and (down to) Earth
- Conclusion

Federated identity with SAML 101



[8]

Federated identity with SAML 101

Security Assertion Markup Language [3]

- transfer of identity information
- between organizations
- that have an established trust relationship

SAML components

- SAML Assertions / Protocols / Bindings / Profiles
  - Web Browser SSO Profile
  - Identity Provider Discovery Profile

What are SAML Assertions?

- Signed XML document containing claims or attributes about a user
- Collected Claims = Identity
- Claims do not need to unambiguously identify user. Only relevant information (e.g. Age > 21, so can buy booze)

What it looks like

```
<Assertion ID="_e3534d1e-a301-462c-ad72-46fe56c995c8" IssueInstant="2010-11-23T12:14:18.382Z"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  <Issuer>..Token Issuer..</Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Can
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"></ds:
      <ds:Reference URI="#_e3534d1e-a301-462c-ad72-46fe56c995c8">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></d
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"></ds:DigestMetho
        <ds:DigestValue>C4uizWDjuFgPlRf9Eh8G6ssZsVByFp7rSf9Gd+butds=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>..Signature Value..</ds:SignatureValue>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>..Base64 Encoded Issuer Certificate..</ds:X509Certificate>
      </ds:X509Data>
    </KeyInfo>
  </ds:Signature>
  <Subject>
    <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
```

What it looks like

```
<Subject>
  <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
    <SubjectConfirmationData a:type="KeyInfoConfirmationDataType" xmlns:a="http://www.w3.org/
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <e:EncryptedKey xmlns:e="http://www.w3.org/2001/04/xmlenc#">
          <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
          </e:EncryptionMethod>
          <KeyInfo>
            <ds:X509Data xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:X509IssuerSerial>
                <ds:X509IssuerName>..Cert Issuer..</ds:X509IssuerName>
                <ds:X509SerialNumber>..Cert Ref..</ds:X509SerialNumber>
              </ds:X509IssuerSerial>
            </ds:X509Data>
          </KeyInfo>
          <e:CipherData>
            <e:CipherValue>..Encrypted Key..</e:CipherValue>
          </e:CipherData>
        </e:EncryptedKey>
      </KeyInfo>
    </SubjectConfirmationData>
  </SubjectConfirmation>
</Subject>
<Conditions NotBefore="2010-11-23T12:14:18.368Z" NotOnOrAfter="2010-11-23T13:14:18.368Z">
```

What it looks like

```
  </Subject>
  <Conditions NotBefore="2010-11-23T12:14:18.368Z" NotOnOrAfter="2010-11-23T13:14:18.368Z">
    <AudienceRestriction>
      <Audience>..Relying Party URI..</Audience>
    </AudienceRestriction>
  </Conditions>
  <AttributeStatement>
    <Attribute Name="http://schemas.xmlsoap.org/claims/UPN">
      <AttributeValue>
        ..Value from Directory..
      </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
      <AttributeValue>
        ..Value from Directory..
      </AttributeValue>
      <AttributeValue>
        ..Value from Directory..
      </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.xmlsoap.org/claims/EmailAddress">
      <AttributeValue>
        ..Value from Directory..
      </AttributeValue>
    </Attribute>
  </AttributeStatement>
  <AuthnStatement AuthnInstant="2010-11-23T12:14:18.315Z">
    <AuthnContext>
      <AuthnContextClassRef>urn:federation:authentication:windows</AuthnContextClassRef>
    </AuthnContext>
  </AuthnStatement>
</Assertion>
```

How is SAML used?

- Standards-based (so widely supported), including:
  - XML Encryption, XML Digital Signatures, X.509
- Relies on standard HTTP (so passes through firewalls and across Internet)
  - Local network (not just for Federation!)
  - Branch offices
  - Remote workers
  - But also supports federation (of which more, later)
- Supports SSO (no need to remember lots of passwords)
- Transparent to user (from web browser or compiled application) single click, and the magic happens!

How is SAML used?

- Standards-based (so widely supported), including:
  - XML Encryption, XML Digital Signatures, X.509
- Relies on standard HTTP (so passes through firewalls and across Internet)
  - Local network (not just for Federation!)
  - Branch offices
  - Remote workers
  - But also supports federation (of which more, later)
- Supports SSO (no need to remember lots of passwords)
- Transparent to user (from web browser or compiled application) single click, and the magic happens!

How is SAML used?

- Standards-based (so widely supported), including:
  - XML Encryption, XML Digital Signatures, X.509
- Relies on standard HTTP (so passes through firewalls and across Internet)
  - Local network (not just for Federation!)
  - Branch offices
  - Remote workers
  - But also supports federation (of which more, later)
- Supports SSO (no need to remember lots of passwords)
- Transparent to user (from web browser or compiled application) single click, and the magic happens!

How is SAML used?

- Standards-based (so widely supported), including:
  - XML Encryption, XML Digital Signatures, X.509
- Relies on standard HTTP (so passes through firewalls and across Internet)
  - Local network (not just for Federation!)
  - Branch offices
  - Remote workers
  - But also supports federation (of which more, later)
- Supports SSO (no need to remember lots of passwords)
- Transparent to user (from web browser or compiled application) single click, and the magic happens!

How is SAML used?

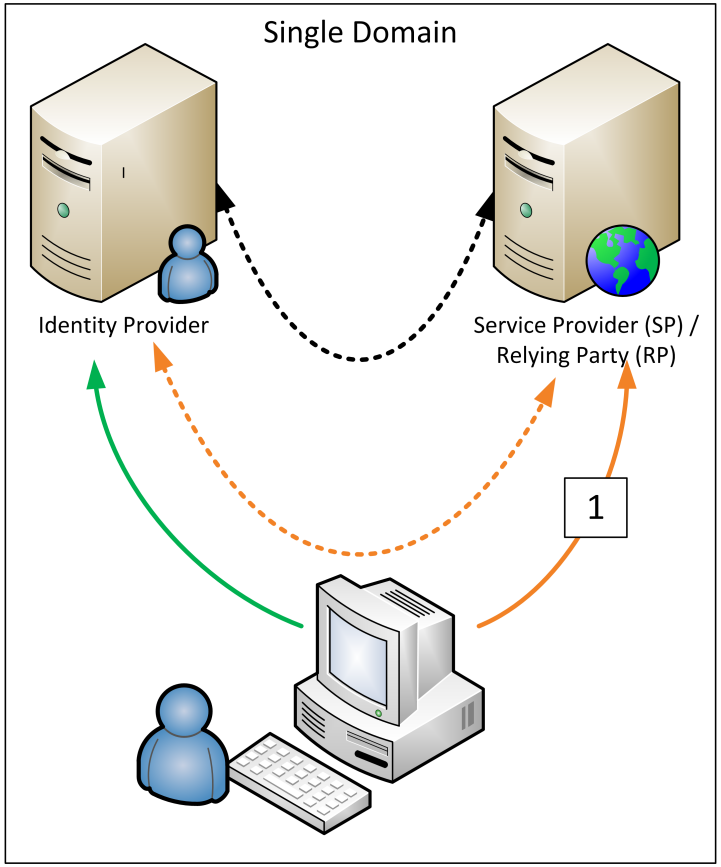
- Standards-based (so widely supported), including:
  - XML Encryption, XML Digital Signatures, X.509
- Relies on standard HTTP (so passes through firewalls and across Internet)
  - Local network (not just for Federation!)
  - Branch offices
  - Remote workers
  - But also supports federation (of which more, later)
- Supports SSO (no need to remember lots of passwords)
- Transparent to user (from web browser or compiled application) single click, and the magic happens!

How does it work?

1. User requests authentication to web application
2. Redirected (through HTTP GET) to IdP
3. Authenticates to IdP (either through Kerberos or Username/Password)
4. Redirected (through HTTP POST) back to web application, including security token
5. Happy User – no passwords to remember
   +
   Happy Administrator – much easier to manage

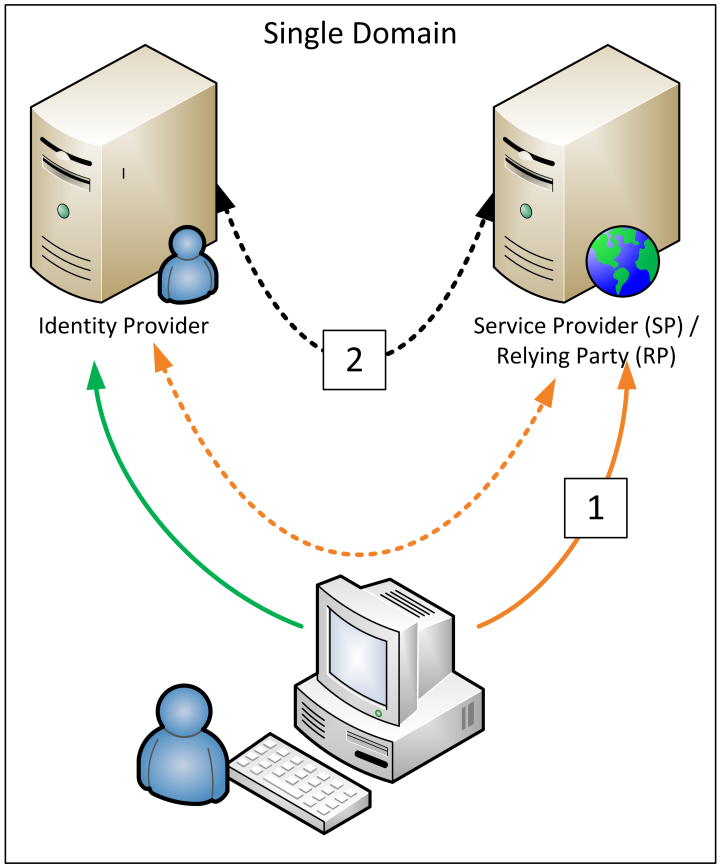
How does it work?

1. User requests authentication to web application



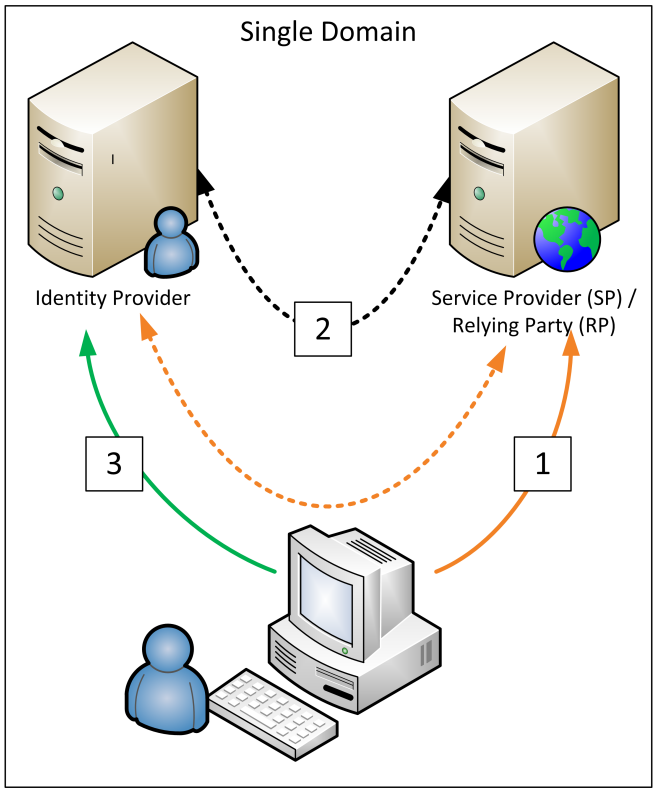
How does it work?

2. Redirected (through HTTP GET) to IdP



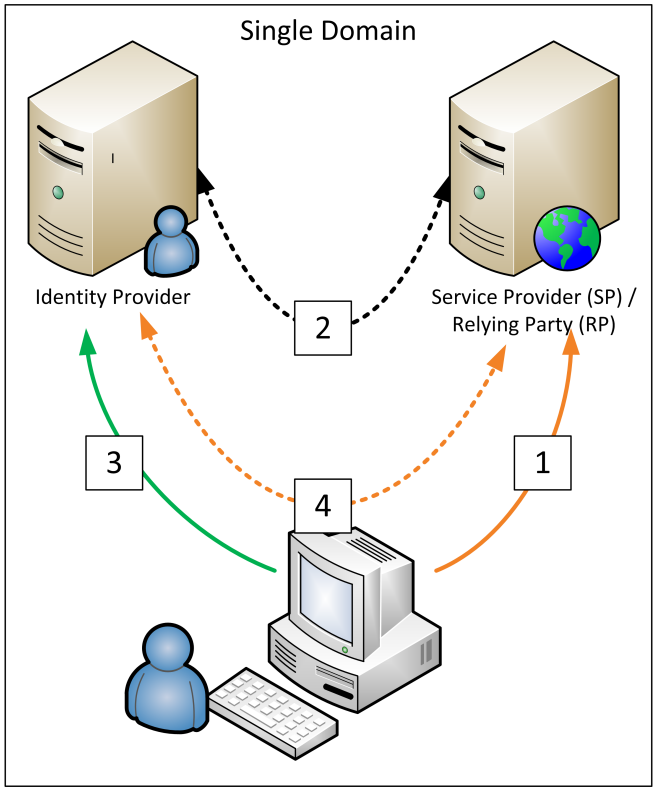
How does it work?

3. Authenticates to IdP (either through Kerberos or Username/Password)



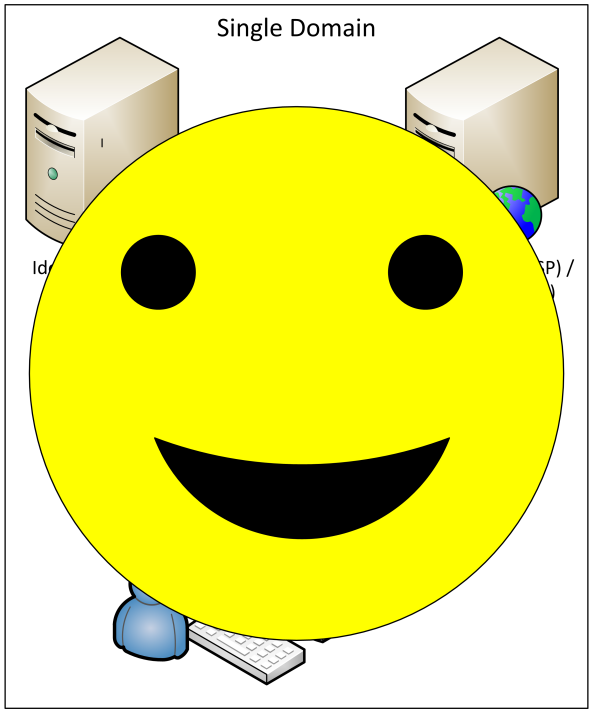
How does it work?

4. Redirected (through HTTP POST) back to web application, including security token



How does it work?

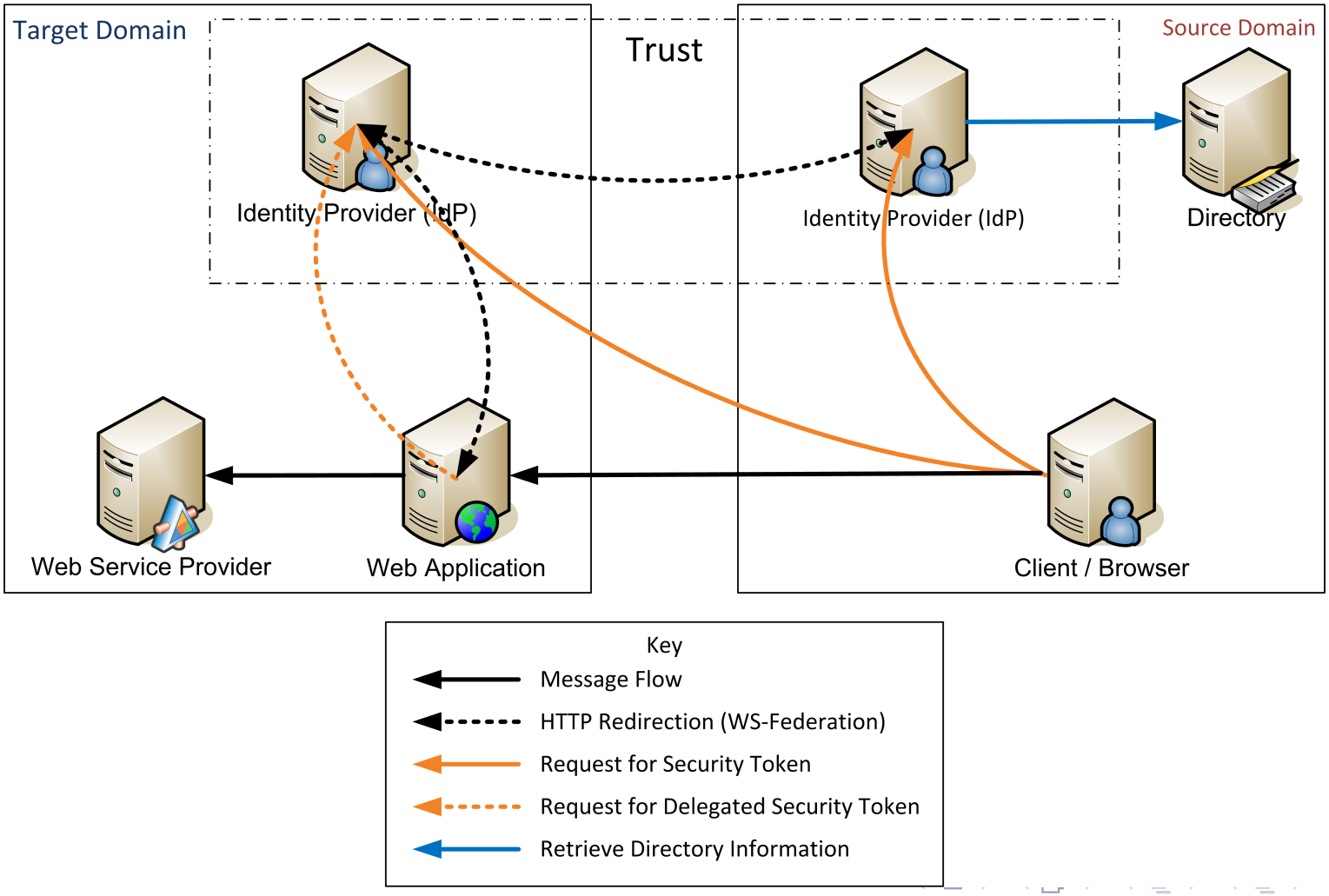
5. Happy User – no passwords to remember
   +
   Happy Administrator – much easier to manage



So what?

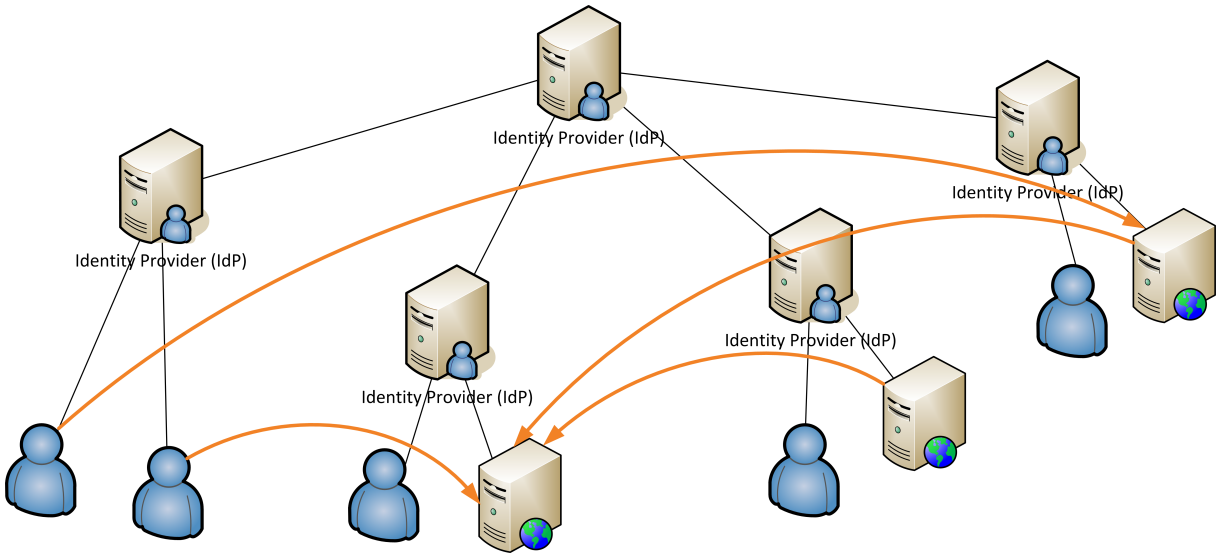
- In addition to SSO, also supports:
  - Federation – the sharing of identity between domains
  - Delegation – maintenance of identity to backend services
  - Distribution of Directory information to other applications, which gives us:
    - ABAC (Attribute Based Access Control) = RBAC +
- It is the support for Federation that makes the use of SAML suitable for the cloud, and it will become ubiquitous.

Federation


Target Domain
Trust
Source Domain
Identity Provider (IdP)
Identity Provider (IdP)
Directory
Web Service Provider
Web Application
Client / Browser
Key
Message Flow
HTTP Redirection (WS-Federation)
Request for Security Token
Request for Delegated Security Token
Retrieve Directory Information

Brokered Federation model

- Trust through a central Broker, establishes trust between many IdPs
- But:
  - How is the trust established?
  - Do we trust all of them?
  - How are standards to be maintained?



OASIS SAML V2.0 Technical Overview (draft 3 and 10)

[sic]

- [2] SAML use case n.1: *"Limitations of Browser cookies"*
- [3] Driver of SAML adoption n.1: *"Multi Domain SSO ... However, since browser cookies are never transmitted between DNS domains, ... SAML solves the MDSSO problem."*

True issue, legitimate will but...

Can also be read as: "SOP sucks, let's build a workaround!"

- Great potential for security issues
- Is it a fail or not?
- E.g. Can a bad guy steal cookies?
  - Be patient ;-)

OASIS SAML V2.0 Technical Overview (draft 3 and 10)

[sic]

- [2] SAML use case n.1: *"Limitations of Browser cookies"*
- [3] Driver of SAML adoption n.1: *"Multi Domain SSO ... However, since browser cookies are never transmitted between DNS domains, ... SAML solves the MDSSO problem."*

True issue, legitimate will but...

Can also be read as: "SOP sucks, let's build a workaround!"

- Great potential for security issues
- Is it a fail or not?
- E.g. Can a bad guy steal cookies?
  - Be patient ;-)

Implementations security

The Good, e.g:

- Token encryption
- Replay attacks usually addressed by default

The Bad, e.g:

- Unsigned LogOut Request accepted
- TargetAudience attribute not verified

The Ugly, e.g:

- Open redirection vulnerability
- Cookie stealing

Implementations security

The Good, e.g:

- Token encryption
- Replay attacks usually addressed by default

The Bad, e.g:

- Unsigned LogOut Request accepted
- TargetAudience attribute not verified

The Ugly, e.g:

- Open redirection vulnerability
- Cookie stealing

Implementations security

The Good, e.g:

- Token encryption
- Replay attacks usually addressed by default

The Bad, e.g:

- Unsigned LogOut Request accepted
- TargetAudience attribute not verified

The Ugly, e.g:

- Open redirection vulnerability
- Cookie stealing

Outline

1. Prelude to Federation
   - Introduction
2. Forward the Federation
   - Where we come from
3. Federation
   - What you need to know
4. Federation and Empire
   - Sharpen your weapons
5. Federation's Edge
   - Design assessment
6. Federation and (down to) Earth
   - Conclusion

Tools

Tool set usually made of a combination of

- Pro/Community edition of Commercial tools
- FOSS
- Custom scripts

Methodology

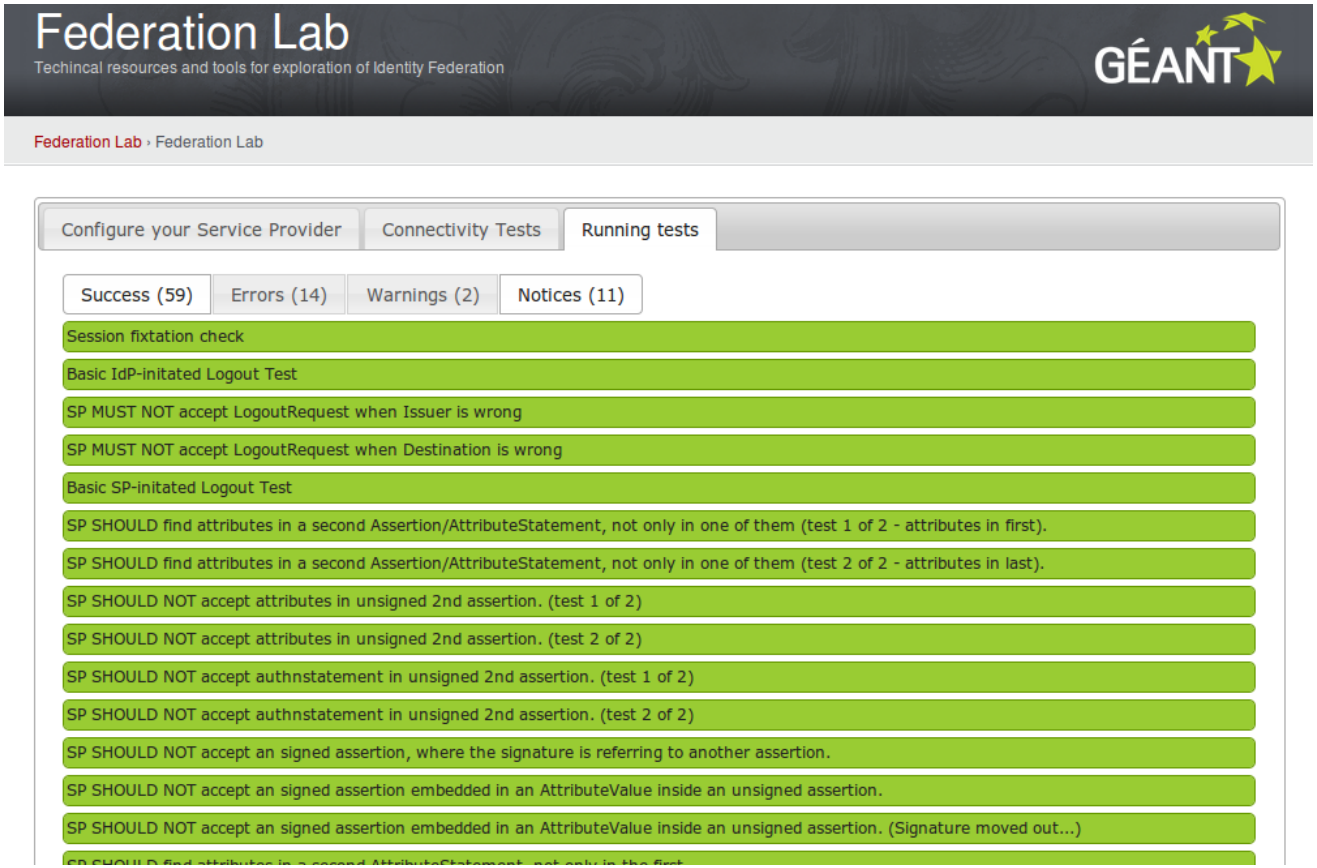
- Procedure (+/-) formal (generic or custom)
- Generally accepted best practices
- Habits, personal preferences
- Still many manual, ad-hoc, improvised steps

Exiting SAML oriented helpers

- UNINETT beta SAML tracer [11]
  - Firefox Plugin
  - A tool for viewing SAML messages sent through the browser during single sign-on and single logout
- Feide RnD SAML 2.0 Debugger [12]
  - Online application to encode/decode SAML message
- Federation Lab beta [13]
  - Online automated checks on SP implementation
- Manual approach
  - Burp decoder (truncated)
  - Python, ruby
    - `saml = Zlib::Inflate.new(-Zlib::MAX_WBITS).inflate(B...`
    - `encoded = CGI::escape(Base64::encode64(Zlib::Deflate...`

Fed Lab Service Provider test

Against an out of the box "Hello world" SP SimpleSAMLphp based



Fed Lab Service Provider test

Against an out of the box "Hello world" SP SimpleSAMLphp based

SAML 2.0 SP Demo Example

English | Bokmål | Nynorsk | Sámegiella | Dansk | Deutsch | Svenska | Suomeksi | Español | Français | Italiano | Nederlands | Luxembourgish | Czech | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語

SAML 2.0 SP Demo Example

Hi, this is the status page of simpleSAMLphp. Here you can see if your session is timed out, how long it lasts until it times out and all the attributes that is attached to your session.

Your attributes

urn:oid:1.3.6.1.4.1.5923.1.1.1.6 andreas@uninett.no

SP MUST accept an LogoutRequest with two sesionindexes (first valid) (sent in separate session, no session-cookies)

SP MUST accept an LogoutRequest with two sesionindexes (second valid) (sent in separate session, no session-cookies)

SP MUST NOT accept LogoutRequest when NameID content is wrong

SP MUST NOT accept LogoutRequest when NameID@Format is wrong

SP MUST NOT accept LogoutRequest when NameID@SPNameQualifier is wrong

SP MUST NOT logout user when invalid SessionIndex is sent

SP MUST NOT accept unsigned LogoutRequest

SP MUST NOT accept a replayed Response. An identical Response/Assertion used a second time. [Profiles]: 4.1.4.5 POST-Specific Processing Rules (test 2 of 2: unsolicited response)

All endpoints in SP metadata SHOULD be HTTPS (not http) (saml2int)

SP should nnot accept a Response with a SubjectConfirmationData elements with a incorrect @Address attribute

SP should not accept a Response with a AuthnStatement missing

AuthnRequest:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" I
  <saml:Issuer>http://www.veryopenid.net/simplesaml/module.php/saml/sp/metadata.php/default-sp</saml:Issuer>
  <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" AllowCreate="true"/>
</samlp:AuthnRequest>
```

Adapt your toolset

"Don't be a tool" [15] but...

- Properly using the right tools often makes the difference
- Time constraint

Two reasons

- Allow "traditional" assessment of Web applications and Services protected by SAML tokens
- Configurations of such architectures is crucial yet complex and error prone, so we need tools to assess these configurations criteria are effective

Decoding / encoding

[15] "Things humans arent good at"

- Decoding / encoding on the fly

Gain of automation

- Easy semantic understanding
- Allows relevant request mangling
- Changes scanner from dumb to smart fuzzer
- Thwarts anti-reply safeguards (e.g. unique random nonce)
- Updates timestamps (long scans can unfold)

Pre & Post processing

- Same approach as [20] for WCF Binary SOAP
- Proxy chaining
  - Preprocessing (decoding requests / encoding responses)
  - Scanning (Fuzz, mangle, do stuff...)
  - Postprocessing (encoding requests / decoding responses)

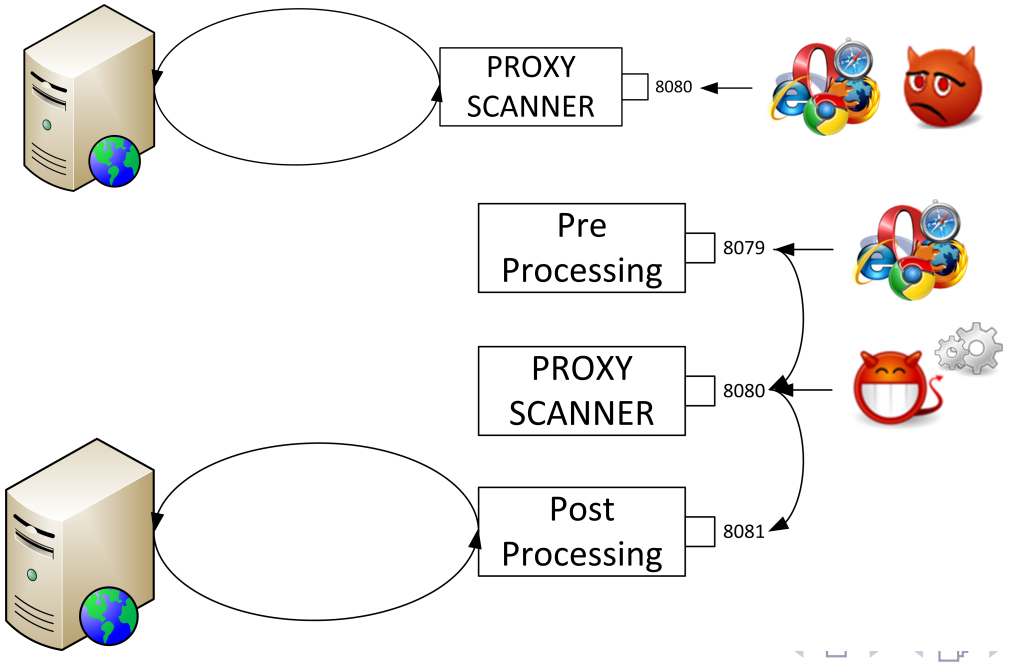


Illustration with Burp Pro Suite

- Burp Pro Suite [14] Extender
  - Java API to extend Burp Suite functionalities
  - Particularly suitable for Pre & Post processing
  - Bindings for Python and Ruby (Buby [17])
- Buby
  - Ruby based framework to extend Burp Suite
  - Tutorial: [18]
  - Hook either $evt\_proxy\_message$ or $evt\_http\_message$
- POC
  - Buby modules and sample code at `http://code.google.com/p/buby-saml`
  - `buby -r SAML_preprocessing -e ReqTamperer`
  - `buby -r SAML_postprocessing -e ReqTamperer`

Preprocessing proxy - Original request

burp intruder repeater window about

target | proxy | spider | scanner | intruder | repeater | sequencer | decoder | comparer | options | alerts

intercept | options | history

Filter: hiding CSS, image and general binary content

#	host	method	URL	params	mod	status	length	MIME ty...	extensi...	title	comment	SSL	
37	https://www.veryopen...	GET	/simplesaml/module.php/core/authenticate.php			200	4000	HTML	php	Test authenti...		✓	81.20
38	https://www.veryopen...	GET	/simplesaml/module.php/core/authenticate.p...	✓		302	2752	HTML	php	Redirect		✓	81.20
39	https://www.veryopen...	GET	/simplesaml/module.php/saml/disco.php?entit...	✓		200	17643	HTML	php	Select your id...		✓	81.20
40	https://www.veryopen...	GET	/simplesaml/module.php/saml/disco.php?entit...	✓		302	2292	HTML	php	Redirect		✓	81.20
41	https://www.veryopen...	GET	/simplesaml/module.php/saml/sp/discoresp.p...	✓		302	3050	HTML	php	Redirect		✓	81.20
42	https://openidp.feide....	GET	/simplesaml/saml2/idp/SSOService.php?SAMLR...	✓	✓	302	2500	HTML	php	Redirect		✓	158.3
43	https://openidp.feide....	GET	/simplesaml/module.php/core/loginuserpass....	✓		200	12015	HTML	php	Enter your us...		✓	158.3
46	https://openidp.feide....	POST	/simplesaml/module.php/core/loginuserpass....	✓		200	12777	HTML	php	POST data		✓	158.3
47	https://www.veryopen...	POST	/simplesaml/module.php/saml/sp/saml2-acs.p...	✓	✓							✓	81.20

original request | edited request

raw | params | headers | hex

SAMLResponse=PHNhbWxwOlJlc3BvbnNlIHhtbG5zOnNhbWxwPSJ1cm46b2FzaXM6bmFtZXM6dGM6UOFNTDoyLjA6cHJvdG9jb2wiIHhtbG5zOnNhbWw9InVybjpvYXNpczpuYW1l
czpOYzpTQU1MOjIuMDphc3NlcnRpb24iIE1EPSJwZng2NGF1OTc4OS1hM2EwLWEOMzEtOGJiNi0wOGYOYmQ1OGI5YTIiIFZlcnNpb249IjIuMCIgSXNzdWVJbnNOYW5OPSIyMDExL
TA3LTE2VDA5OjEO0jQ1WiIgRGVzdGluYXRpb249ImhOdHBzOi8vd3d3LnZlcnlvcGVuaWQubmVOL3NpbXBsZXNhbWwvbW9kdWxlLnBocC9zYW1sL3NwL3NhbWwyLWFjcy5waHAvZG
VmYXVsdC1zcCIgSW5SZXNwb25zZVRvPSJfMDk0OWM2ODM3ZGVkYjcxNzAyYjIwZTQ5MTQwODZmMzE4NTBmZjk2ODNmIj48c2FtbDpJc3N1ZXI%2BaHR0cHM6Ly9vcGVuaWRwLmZla
WRlLm5vPC9zYW1sOklzc3Vlcj48ZHM6U2lnbmFOdXJlIHhtbG5zOmRzPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjIj4KICA8ZHM6U2lnbmVkSW5mbz48ZHM6Q2
Fub25pY2FsaXphdGlvbkl1dGhvZCBBbGdvcm1OaG09ImhOdHA6Ly93d3cudzMub3JnLzIwMDAvMDkveG1sZHNpZyNyc2Etc2hhMSIvPgogIDxkczpSZWZlcmVuY2UgVVJJPSIjcGZ4NjRhZTk3ODktYTNhMC1hNDMxLThiYjYt
MDhmNGJkNThiOWEyIj48ZHM6VHJhbnNmb3Jtcz48ZHM6VHJhbnNmb3Jt IEFsZ29yaXRobTOiaHR0cDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnI2VudmVsb3B1ZC1zaWduY
XR1cmUiLz48ZHM6VHJhbnNmb3JtIEFsZ29yaXRobTOiaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC94bWwtZXhjLWMxNG4jIi8%2BPC9kczpUcmFuc2Zvcm1zPjxkczpEaWd1c3RN
ZXRob2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjc2hhMSIvPjxkczpEaWd1c3RWYWx1ZT5HOUpYRE9GZGtMZDZRQ1hCUnZ6a3JsTEdTUDQ9P
C9kczpEaWd1c3RWYWx1ZT48L2RzOlJ1ZmVyZW5jZT48L2RzOlNpZ251ZE1uZm8%2BPGRzOlNpZ25hdHVyZVZhbHV1PnF5KOErTnVOcWOwcWFyMOFrQkpUL3VJSGJneXpXM2haY1RW
R1VmZUVlcOVRSGNJT2pXdVJmZXc2OUJsSmJESWpiNC9FcOpFcVFPOE9jNmNhUzEwdzNYWVhqSOpmRGFFajQwWEVUclBjcmJGKORsRmc1ZXIvcmdyS3NLSzJzN31DaWY4Rk1zYOJEd
itqTVhHRFFhOWJPN21EZDYrREtOTDYvW1VObVB4TzA2Zz08L2RzOlNpZ25hdHVyZVZhbHV1Pgo8ZHM6S2V5SW5mbz48ZHM6WDUwOURhdGE%2BPGRzOlg1MD1DZXJOaWZpY2FOZT5N
SU1DaXpDQOFmUUNDUUNZOHRLYU1jMEJNakFOQmdrcWhraUc5dzBCQVFVRkFEQOJpVEVMTUFrROExVUVCaE1DVGs4eEVqQVFCZO5WQkFnVENWUnliMjVrYUdWcGJURVFNQTRHQTFVR
UNoTUhWVTVKVGtWVVZERU9NQXdHQTFVRUN4TUZSbVZwWkdVeEdUQVhCZO5WQkFNVEVHOXdaVzVwWkhBdVptVnBaR1V1Ym04eEtUQW5CZ2txaGtpRz13MEJDUUVXR21GdVpISmxZWE
l1YzI5c1ltVnlaMEIxYm1sdVpYUjBMbTV2TUIOWERUQTRNRFV3TORBNU1qSTBPRm9YRFRNMU1Ea3lNekE1TWpJME9Gb3dnWWt4Q3pBSkJnT1ZCQV1UQWs1UE1SSXdFQV1EV1FRSUV
3bFVjbTl1WkdobGFXMHhFREFPQmdOVkJBb1RCMVZPU1U1R1ZGUXhEakFNQmdOVkJBc1RCVVpsYVdSbE1Sa3dGdllEV1FRREV4QnZjR1Z1YVdSdOxtWmxhV1JsTGO1dk1Ta3dKd1lK
S29aSWh2YO5BUWtCRmhwaGJtUnlaVOZ6TG5OdmJHSmxjbWRBZFc1cGJtVjBkQzV1YnpDQm56QU5CZ2txaGtpRz13MEJBUUVGQUFPQmpRQXdnWWtDZ1lFQXQ4akxvcUkxV1RseEFaM
mF4aURJVGhXYOFPWGR1OEtrV1VXYU4vU29vTz1PMFFRNOtSVWpTROtOOUpLNjVBR1JEWFFrV1BBdTRIbG5PNG5vWWxGUOxuWX1EeEk2NkxDcjcxeDRsZOZKanFMZUF2Qi9HcUJxRm
ZJWjNZSy9OcmhuVXFGd1p1NjNuTHJaamNVWnhOYVBqTO9TU1NEYVhwdjFrYjVrM2pPaVNHRUNBdOVBQVRBTkJna3Foa21HOXcwQkFRVUZBQU9CZ1FCUV1qNGNBYWZXYV1makJVMnp
pMUVsd1NOSWFKNW55cC9zLzhCOFNBUEsyVDc5TWNNeWNjUDN3U1cxMOxIa21NMWp3S2UzQUNGWEJ2cUdRTjBJYmNINDlodTBGS2hZRkOvR1BESmNJSEZCc215TUJYQ2hweWU5dkJh
VE5FQkNOVTNLamp5RzBoU1QybUFROWgrYmtQbU92bEVvL2FIMHhSNjhaOWh3NFBGMTN3PTO8L2RzOlg1MD1DZXJOaWZpY2FOZT48L2RzOlg1MD1EYXRhPjwvZHM6S2V5SW5mbz48L
2RzOlNpZ25hdHVyZT48c2FtbHA6U3RhdHVzPjxzYW1scDpTdGFOdXNDb2R1IFZhbHV1PSJ1cm46b2FzaXM6bmFtZXM6dGM6UOFNTDoyLjA6c3RhdHVzOlN1Y2N1c3MiLz48L3NhbW
xwOlNOYXR1cz48c2FtbDpBc3N1cnRpb24geG1sbnM6eHNpPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxL1hNTFNjaGVtYS1pbnNOYW5jZSIgeG1sbnM6eHM9ImhOdHA6Ly93d3cudzM
ub3JnLzIwMDEvWE1MU2NoZW1hIiBJRDOicGZ4OTdlZjAyMDctMGM1MyO5ZDBiLTUxMTItZjExNGFhZDllOGIzIiBWZXJzaW9uPSIyLjAiIE1zc3V1SW5zdGFudDOiMjAxMSOwNyOx
N1QwOToxNDoONVoiPjxzYW1sOklzc3Vlcj5odHRwczovL29wZW5pZHAuZmVpZGUubm88L3NhbWw6SXNzdWVyPjxkczpTaWduYXR1cmUgeG1sbnM6ZHM9ImhOdHA6Ly93d3cudzMub
3JnLzIwMDAvMDkveG1sZHNpZyMiPgogIDxkczpTaWduZWRJbmZvPjxkczpDYW5vbmlqYWxpemFOaW9uTWVOaG9kIEFsZ29yaXRobTOiaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC
94bWwtZXhjLWMxNG4jIi8%2BCiAgICA8ZHM6U2lnbmFOdXJlTWVOaG9kIEFsZ29yaXRobTOiaHR0cDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnI3JzYS1zaGExIi8%2BCiA

+ < > 0 matches

Preprocessing proxy - Edited request

burp intruder repeater window about

target | proxy | spider | scanner | intruder | repeater | sequencer | decoder | comparer | options | alerts

intercept | options | history

Filter: hiding CSS, image and general binary content

#	host	method	URL	params	mod	status	length	MIME ty...	extensi...	title	comment	SSL	
37	https://www.veryopen...	GET	/simplesaml/module.php/core/authenticate.php			200	4000	HTML	php	Test authenti...		✓	81.20
38	https://www.veryopen...	GET	/simplesaml/module.php/core/authenticate.p...	✓		302	2752	HTML	php	Redirect		✓	81.20
39	https://www.veryopen...	GET	/simplesaml/module.php/saml/disco.php?entit...	✓		200	17643	HTML	php	Select your id...		✓	81.20
40	https://www.veryopen...	GET	/simplesaml/module.php/saml/disco.php?entit...	✓		302	2292	HTML	php	Redirect		✓	81.20
41	https://www.veryopen...	GET	/simplesaml/module.php/saml/sp/discoresp.p...	✓		302	3050	HTML	php	Redirect		✓	81.20
42	https://openidp.feide....	GET	/simplesaml/saml2/idp/SSOService.php?SAMLR...	✓	✓	302	2500	HTML	php	Redirect		✓	158.3
43	https://openidp.feide....	GET	/simplesaml/module.php/core/loginuserpass....	✓		200	12015	HTML	php	Enter your us...		✓	158.3
46	https://openidp.feide....	POST	/simplesaml/module.php/core/loginuserpass....	✓		200	12777	HTML	php	POST data		✓	158.3
47	https://www.veryopen...	POST	/simplesaml/module.php/saml/sp/saml2-acs.p...	✓	✓							✓	81.20

original request | edited request

raw | params | headers | hex


```
SAMLResponse=__SAMLResponse__SEPARATOR_A__<samlp:Response xmlns:samlp='urn:oasis:names:tc:SAML:2.0:protocol'
xmlns:saml='urn:oasis:names:tc:SAML:2.0:assertion' ID='pfx64ae9789-a3a0-a431-8bb6-08f4bd58b9a2' Version='2.0'
IssueInstant='2011-07-16T09:14:45Z' Destination='https://www.veryopenid.net/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp'
InResponseTo='_0949c6837dedb71702b20e4914086f31850ff9683f'>
  <saml:Issuer>https://openidp.feide.no</saml:Issuer>
  <ds:Signature xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm='http://www.w3.org/2001/10/xml-exc-c14n#'/>
      <ds:SignatureMethod Algorithm='http://www.w3.org/2000/09/xmldsig#rsa-sha1'/>
      <ds:Reference URI='#pfx64ae9789-a3a0-a431-8bb6-08f4bd58b9a2'>
        <ds:Transforms>
          <ds:Transform Algorithm='http://www.w3.org/2000/09/xmldsig#enveloped-signature'/>
          <ds:Transform Algorithm='http://www.w3.org/2001/10/xml-exc-c14n#'/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm='http://www.w3.org/2000/09/xmldsig#sha1'/>
        <ds:DigestValue>G9JXDOFdkLd6QBXBRvzkr1LGSP4=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>

qy+A+NuNqmOqar3AkBJT/uIHbgyzW3hZbTVFUfeEesEQHcIOjWuRfew69B1JbDIjb4/EsJEqQO8Oc6caS1Ow3XYXjKJfDaEj4OXETrPcrbF+D1Fg5er/rgrKsKK2s7yCif8FMscBD
v+jMXGDQa9bO7mDd6+DKNL6/ZUNmPxOO6g=
    </ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>

MIICizCCAfQCCQCY8tKaMcOBMjANBgkqhkiG9wOBAQUFADCBiTELMAkGA1UEBhMCTk8xEjAQBgNVBAgTCVRyb25kaGVpbTEQMA4GA1UEChMHVU5JTkVUVDEOMAwGA1UECxMFRmVpZ
```


+ < > 0 matches

Central Burp instance - Intruder

burp intruder repeater window about

target | proxy | spider | scanner | intruder | repeater | sequencer | decoder | comparer | options | alerts

1 | 2

target | positions | payloads | options

attack type sniper

4 payload positions — length: 10239

```
        <saml:SubjectConfirmationData NotOnOrAfter='2011-07-16T09:19:45Z'
Recipient='https://www.veryopenid.net/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp'
InResponseTo='_0949c6837dedb71702b20e4914086f31850ff9683f'/>
      </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore='§2011-07-16T09:14:15Z§' NotOnOrAfter='§2011-07-16T09:19:45Z§'>
      <saml:AudienceRestriction>
        <saml:Audience>
          https://www.veryopenid.net/simplesaml/module.php/saml/sp/metadata.php/default-sp
        </saml:Audience>
      </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant='2011-07-16T09:14:45Z' SessionNotOnOrAfter='2011-07-16T17:14:45Z'
SessionIndex='_d72a50c89dca85d6c686c739e2ac6dfc67440fae7b'>
      <saml:AuthnContext>
        <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>
      </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
      <saml:Attribute Name='uid' NameFormat='urn:oasis:names:tc:SAML:2.0:attrname-format:uri'>
        <saml:AttributeValue xsi:type='xs:string'>§lebouille71§</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name='givenName' NameFormat='urn:oasis:names:tc:SAML:2.0:attrname-format:uri'>
        <saml:AttributeValue xsi:type='xs:string'>le</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name='sn' NameFormat='urn:oasis:names:tc:SAML:2.0:attrname-format:uri'>
        <saml:AttributeValue xsi:type='xs:string'>bouille</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name='cn' NameFormat='urn:oasis:names:tc:SAML:2.0:attrname-format:uri'>
        <saml:AttributeValue xsi:type='xs:string'>le bouille</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name='mail' NameFormat='urn:oasis:names:tc:SAML:2.0:attrname-format:uri'>
        <saml:AttributeValue xsi:type='xs:string'>lebouille71@gmail.com</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name='eduPersonPrincipalName' NameFormat='urn:oasis:names:tc:SAML:2.0:attrname-format:uri'>
        <saml:AttributeValue xsi:type='xs:string'>lebouille71@rnd.feide.no</saml:AttributeValue>
```

add § | clear § | auto § | refresh | clear

+ | < | > — 0 matches

Postprocessing proxy - Original request

burp intruder repeater window about

target | proxy | spider | scanner | intruder | repeater | sequencer | decoder | comparer | options | alerts

intercept | options | history

Filter: hiding CSS, image and general binary content

#	host	method	URL	params	mod	status	length	MIME ty...	extensi...	title	comment	SSL	
81	http://simplesamlphp....	GET	/favicon.ico			404	4235	HTML	ico	SimpleSAMLphp			158.3
82	http://simplesamlphp....	GET	/favicon.ico			404	4235	HTML	ico	SimpleSAMLphp			158.3
83	https://www.veryopen...	GET	/simplesaml/module.php/core/frontpage_welc...			200	5863	HTML	php	simpleSAMLp...		✓	81.20
84	https://www.veryopen...	GET	/simplesaml/module.php/core/frontpage_auth...			200	5322	HTML	php	simpleSAMLp...		✓	81.20
85	https://www.veryopen...	GET	/simplesaml/module.php/core/authenticate.php			200	4000	HTML	php	Test authenti...		✓	81.20
86	https://www.veryopen...	GET	/simplesaml/module.php/core/authenticate.p...	✓		302	2752	HTML	php	Redirect		✓	81.20
87	https://www.veryopen...	GET	/simplesaml/module.php/saml/disco.php?entit...	✓		200	17643	HTML	php	Select your id...		✓	81.20

original request | edited request | response

raw | params | headers | hex


```
SAMLResponse=__SAMLResponse__SEPARATOR_A__<samlp:Response xmlns:samlp='urn:oasis:names:tc:SAML:2.0:protocol'
xmlns:saml='urn:oasis:names:tc:SAML:2.0:assertion' ID='pfx64ae9789-a3a0-a431-8bb6-08f4bd58b9a2' Version='2.0'
IssueInstant='2011-07-16T09:14:45Z' Destination='https://www.veryopenid.net/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp'
InResponseTo='_0949c6837dedb71702b20e4914086f31850ff9683f'>
  <saml:Issuer>https://openidp.feide.no</saml:Issuer>
  <ds:Signature xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm='http://www.w3.org/2001/10/xml-exc-c14n#'/>
      <ds:SignatureMethod Algorithm='http://www.w3.org/2000/09/xmldsig#rsa-sha1'/>
      <ds:Reference URI='#pfx64ae9789-a3a0-a431-8bb6-08f4bd58b9a2'>
        <ds:Transforms>
          <ds:Transform Algorithm='http://www.w3.org/2000/09/xmldsig#enveloped-signature'/>
          <ds:Transform Algorithm='http://www.w3.org/2001/10/xml-exc-c14n#'/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm='http://www.w3.org/2000/09/xmldsig#sha1'/>
        <ds:DigestValue>G9JXDOFdkLd6QBXBRvzkr1LGSP4=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>

qy+A+NuNqmOqar3AkBJT/uIHbgyzW3hZbTVFUfeEesEQHcIOjWuRfew69B1JbDIjb4/EsJEqQO8Oc6caS1Ow3XYXjKJfDaEj4OXETrPcrbF+D1Fg5er/rgrKsKK2s7yCif8FMscBD
v+jMXGDQa9bO7mDd6+DKNL6/ZUNmPxOO6g=
    </ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>

MIICizCCAfQCCQCY8tKaMcOBMjANBgkqhkiG9wOBAQUFADCBiTELMAkGA1UEBhMCTk8xEjAQBgNVBAgTCVRyb25kaGVpbTEQMA4GA1UEChMHVU5JTkVUVDEOMAwGA1UECxMFRmVpZ
GUxGTAXBgNVBAMTEG9wZW5pZHAuZmVpZGUubm8xKTAnBgkqhkiG9wOBCQEWGmFuZHJlYXMuc29sYmVyZOB1bmluZXROLm5vMB4XDTA4MDUwODA5MjIOOFoXDTM1MDkyMzA5MjIOOF
owgYkxCzAJBgNVBAYTAk5PMRIwEAYDVQQIEwlUcm9uZGhlaWOxEDAOBgNVBAoTB1VOSU5FVFQxDjAMBgNVBAsTBUZlaWR1MRkwFwYDVQQDExBvcGVuaWRwLmZlaWR1Lm5vMSkwJwY
JKoZIhvcNAOkBFhpbbmRvZWFzLnNvbGJlcmdAdW5pbmVOdC5ubzCBnzANBgkqhkiG9wOBAOEFAAOBjOAwgYkCgYEAt8jLoqI1VT1xAZ2axiDIThWcAOXdu8KkVUWaN/Soo090007
```


+ < > 0 matches

Postprocessing proxy - Edited request

burp intruder repeater window about

target | proxy | spider | scanner | intruder | repeater | sequencer | decoder | comparer | options | alerts

intercept | options | history

Filter: hiding CSS, image and general binary content

#	host	method	URL	params	mod	status	length	MIME ty...	extensi...	title	comment	SSL	
81	http://simplesamlphp....	GET	/favicon.ico			404	4235	HTML	ico	SimpleSAMLphp			158.3
82	http://simplesamlphp....	GET	/favicon.ico			404	4235	HTML	ico	SimpleSAMLphp			158.3
83	https://www.veryopen...	GET	/simplesaml/module.php/core/frontpage_welc...			200	5863	HTML	php	simpleSAMLp...		✓	81.20
84	https://www.veryopen...	GET	/simplesaml/module.php/core/frontpage_auth...			200	5322	HTML	php	simpleSAMLp...		✓	81.20
85	https://www.veryopen...	GET	/simplesaml/module.php/core/authenticate.php			200	4000	HTML	php	Test authenti...		✓	81.20
86	https://www.veryopen...	GET	/simplesaml/module.php/core/authenticate.p...	✓		302	2752	HTML	php	Redirect		✓	81.20
87	https://www.veryopen...	GET	/simplesaml/module.php/saml/disco.php?entit...	✓		200	17643	HTML	php	Select your id...		✓	81.20

original request | edited request | response

raw | params | headers | hex

SAMLResponse=PHNhbWxwOlJlc3BvbnNlIHhtbG5zOnNhbWxwPSdlcm46b2FzaXM6bmFtZXM6%OAdGM6UOFNTDoyLjA6cHJvdG9jb2wnIHhtbG5zOnNhbWw9J3Vybjpv YXNpczpu%
OAYW1lczpOYzpTQU1MOjIuMDphc3NlcnRpb24nIE1EPSdwZng2NGF1OTc4OS1h%OAM2EwLWEOMzEtOGJiNiOwOGYOYmQ1OGI5YTInIFZlcnNpb249JzIuMCcgSXNz%OAdWVJbnNOY
W50PScyMDExLTA3LTE2VDA5OjEOOjQ1WicgRGVzdG1uYXRpb249%OAJ2hOdHBzOi8vd3d3LnZlcnlvcGVuaWQubmVOL3NpbXBsZXNhbWwvbW9kdWx1%OALnBocC9zYW1sL3NwL3Nh
bWwyLWFjcy5waHAvZGVmYXVsdC1zcCcgSW5SZXNw%OAb25zZVRvPSdfMDk0OWM2ODM3ZGVkYjcxNzAyYjIwZTQ5MTQwODZmMzE4NTBm%OAZjk2ODNmJz4KICA8c2FtbDpJc3N1ZXI
%2BaHROcHM6Ly9vcGVuaWRwLmZlaWR1%OALm5vPC9zYW1sOklzc3Vlcj4KICA8ZHM6U2lnbmFOdXJlIHhtbG5zOmRzPSdo%OAdHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRz
aWcjJz4KICAgIDxkczpT%OAaWduZWRJbmZvPgogICAgICA8ZHM6Q2Fub25pY2FsaXphdGlvbk1ldGhvZCBB%OAbGdvcm1OaG09J2hOdHA6Ly93d3cudzMub3JnLzIwMDEvMTAveG1
sLWV4Yy1j%OAMTRuIycvPgogICAgICA8ZHM6U2lnbmFOdXJlTWV0aG9kIEFsZ29yaXRobTOn%OAaHROcDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnI3JzYS1zaGExJy8%2B
%OACiAgICAgIDxkczpSZWZlcmVuY2UgVVJJPScjcGZ4NjRhZTk3ODktYTNhMC1h%OANDMxLThiYjYtMDhmNGJkNThiOWEyJz4KICAgICAgICA8ZHM6VHJhbnNmb3Jt%OAcz4KICAg
ICAgICAgIDxkczpUcmFuc2Zvcm0gQWxnb3JpdGhtPSdodHRwOi8v%OAd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjZW52ZWxvcGVkLXNpZ25hdHVy%OAZScvPgogICAgICAgICA
gPGRzOlRyYW5zZm9ybSBBbGdvcm1OaG09J2hOdHA6%OALy93d3cudzMub3JnLzIwMDEvMTAveG1sLWV4Yy1jMTRuIycvPgogICAgICAg%OAIDwvZHM6VHJhbnNmb3Jtcz4KICAgIC
AgICA8ZHM6RG1nZXNOTWVOaG9kIEFs%OAZ29yaXRobTOnaHROcDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnI3No%OAYTEnLz4KICAgICAgICA8ZHM6RG1nZXNOVmFsdWU%2
BRzlKWERPRmRrTGQ2UUJY%OAQ1J2emtybExHU1AOPTwvZHM6RG1nZXNOVmFsdWU%2BCiAgICAgIDwvZHM6UmVm%OAZXJlbmN1PgogICAgPC9kczpTaWduZWRJbmZvPgogICAgPGRz
OlNpZ25hdHVy%OAZVZhbHV1PgogICAgICBxeStBK051TnFtMHFhcjNBaOJKVC91SUhiZ3l6VzNo%OAWmJUVkZVZmVFZXNFUUhjSU9qV3VSZmV3Nj1CbEpiRE1qYjQvRXNKRXFRTzh
P%OAYzZjYVMxMHczWF1YaktKZkRhRWoOMFhFVHJQY3JiRitEbEZnNWVyL3Jnckt z%OASOsyczd5Q2lmOEZNc2NCRHYrak1YRORRYT1iTzdtRGQ2KORLTkw2L1pVTm1Q%OAeE8wNmc
9CiAgICA8L2RzOlNpZ25hdHVyZVZhbHV1PgogICAgPGRzOktleU1u%OAZm8%2BCiAgICAgIDxkczpYNTA5RGFOYT4KICAgICAgICA8ZHM6WDUwOUN1cnRp%OAZmljYXR1PgogICAg
ICAgICAgTU1JQ216QONBZ1FDQ1FDWThOS2FNYzBCTWpB%OATkJna3Foa21HOXcwQkFRVUZBRENCaVRFTE1BaOdBMVVFQmhNQ1RrOHhFakFR%OAQmdOVkJBZ1RDV1J5YjI1a2FHVnB
iVEVRTUEORO ExVUVDaE1IV1U1S1RrV1VW%OAREVPTUF3ROExVUVDeE1GUm1WcFpHVXhHVEFYQmdOVkJBTVRFRzl3Wlc1cFpI%OAQXVabVZwWkdVdWJtOHhLVEFuQmdrcWhraUc5dz
BCQ1FFVOdtRnVaSEpsWVhN%OAdWMyOXNZbVZ5WjBCMWJtbHVaWFIwTGO1dk1CNFhEVEEOTURVdO9EQTVNakkw%OATOZvWERUTTFNRGt5TXpBNU1qSTBPRm93Z1lreEN6QUpCZO5WQ
kFZVEFrNVBN%OAUkl3RUFZRFZRUU1Fd2xVY2O5dVpHaGxhVzB4RURBTOJnT1ZCQW9UQjFWT1NV%OANUZWR1F4RGpBTUJnT1ZCQXNUQ1VabGFXUmxNUmt3RndZRFZRUURFeEJ2YOdW
%OAdWFXUndMbVpsYVdSbExtNXZNU2t3SndZSktvWklodmNOQVFrQkZocGhibVJ5%OAW1dGekxuTnZiROpsY21kQWRXNXBibVYwZEM1dWJ6QOJuekFOQmdrcWhraUc5%OAdzBCQVFF
RkFBTOJqUUF3Z1lrQ2dZRUFOOGpMb3FJMVZUbHhBWjJheG1ESVRo%OAV2NBT1hkdThLa1ZVV2FOL1NvbO85TzBRUTdLU1VqUOdLTj1KSzY1QUZSRFhR%OAa1dQQXUOSGxuTzRub11
sR1NMb115RHhJNjZMQ3I3MXgObGdGSmpxTGVBdkIv%OAR3FCcUZmSVozWUsvTnJob1VxRndadTYzbkxyWmpjVVp4TmFQak9PU1JTRGFY%OAcHYxa2I1azNqT21TROVDQXdFQUFUQU
5CZ2txaGtpRz13MEJBUVVGQUFPQmdR%OAQ1FZajRjQWFmV2FZZmpCVTJ6aTFFbHdTdE1hSjVueXAvcy84QjhTQVBLM1Q3%OAOU1jTX1jY1Azd1NXMTNMSGttTTFqdOt1MOFDR1hCd
nFHUU4wSWJjSDQ5aHUw%OARktoWUZNLOdQREpjSUhGQnNpeU1CWENocH11OXZCYVRORUJDdFUzS2pqeUcw%OAaFJUMm1BUT1oK2JrUG1PdmxFby9hSDB4UjY4Wjlodz RQRjEzdz09
CiAgICAg%OAICAgPC9kczpYNTA5Q2VydG1maWNhdGU%2BCiAgICAgIDwvZHM6WDUwOURhdGE%2B%OACiAgICA8L2RzOktleU1uZm8%2BCiAgPC9kczpTaWduYXR1cmU%2BCiAgPHN
hbWxw%OAO1NOYXR1cz4KICA8c2FtbDpBc3N1cnRpb24geG1sbnM6eHNpPSdodHRw%OAOi8vd3d3LnczLm9yZy8yMDAxL1hNTFNjaGVtYS1pbnNOYW5jZScgeG1sbnM6%OAeHM9J2hOdHA6Ly
93d3cudzMub3JnLzIwMDEvWE1MU2NoZW1hJyBJRDOncGZ4%OAOTdlZjAyMDctMGM1MyO5ZDBiLTUxMTItZjExNGFhZD11OGIzJyBWZXJzaW9u%OAPScyLjAnIE1zc3V1SW5zdGFud
DOnMjAxMSOwNyOxN1QwOToxNDoONVonPgog%OAICAgPHNhbWw6SXNzdWVyPmhOdHBzOi8vb3Blbmlkc5mZW1kZS5ubzwvc2Ft%OAbDpJc3N1ZXI%2BCiAgICA8ZHM6U2lnbmFOdX
J1IHhtbG5zOmRzPSdodHRwOi8v%OAd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjZ24KICAgICAgPGRzOlNpZ251%OAZE1uZm8%2BCiAgICAgICAgICAgPGRzOkNhbm9uaWNhbG16YXR
nb25NZXRob2QgOWxn%OAb3JndGhtPSdodHRwOi8vd3d3LnczLm9vZv8vMDAxLzEwL3htbC1leGMtYzEO%OAbiMnLz4KICAgICAgICA8ZHM6U2lnbmFOdXJ1TWV0aG9kIEFsZ29vaX

+ < > 0 matches

Example of vulnerabilities

- Open redirection [21]
  - $\simeq$ `http://www.vulnerable.com/?redirect=http://www.attacker.com`
  - Not critical
  - Built in the standards?
- Cookie theft
  - Works even if the victim has not chosen the "Remember" option
  - Demo: Make the SP leaking $idpdisco\_saml\_lastidp$ cookie, even if cookie $idpdisco\_saml\_remember = 0$
    - If you visit his site, a bad guy can inconspicuously discover your IdP = what is your originating organization

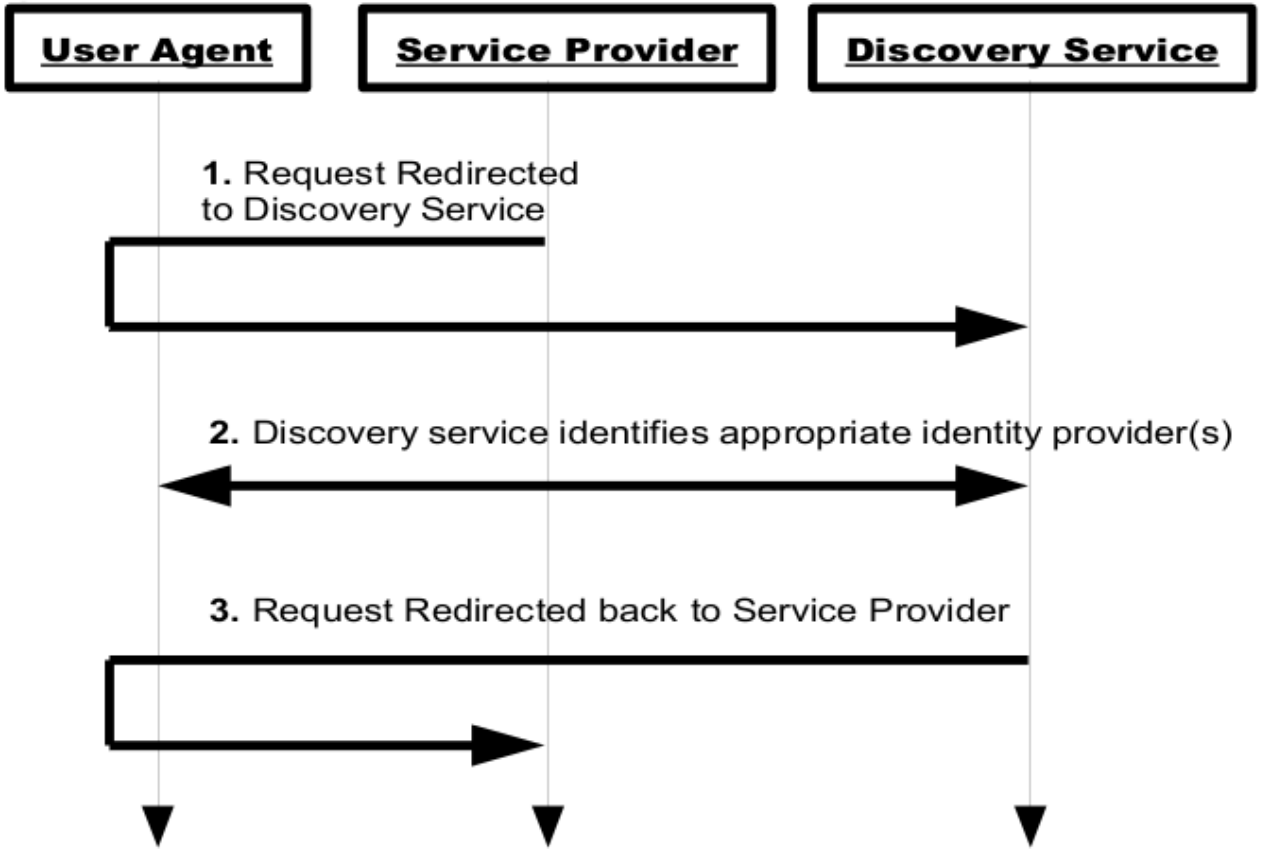
Demo: SimpleSAMLPHP open redirect

When an open redirect leads to cookie theft

- Leveraging an existing live, open to everyone test environment
- Feide [19]: Norwegian academic Federation
- on a dummy account

Back to the OASIS standard

Identity Provider Discovery Service Protocol and Profile [22]



Identity Provider Discovery Service Protocol and Profile [21]

[sic]

- *"This protocol has the potential for creating additional opportunities for phishing..."*
- Proposed workaround: use of SP metadata
- *"To mitigate this threat, metadata* **can** *be used to limit the sites authorized to use a discovery service"*
- *"A discovery service* **SHOULD** *require that the service providers making use of it supply metadata"*

- Developers don't have to implement it to be compliant [23]

Identity Provider Discovery Service Protocol and Profile [21]

[sic]

- *"This protocol has the potential for creating additional opportunities for phishing..."*
- Proposed workaround: use of SP metadata
- *"To mitigate this threat, metadata* **can** *be used to limit the sites authorized to use a discovery service"*
- *"A discovery service* **SHOULD** *require that the service providers making use of it supply metadata"*

- Developers don't have to implement it to be compliant [23]

Outline

1. Prelude to Federation
   - Introduction
2. Forward the Federation
   - Where we come from
3. Federation
   - What you need to know
4. Federation and Empire
   - Sharpen your weapons
5. Federation's Edge
   - Design assessment
6. Federation and (down to) Earth
   - Conclusion

New risks?

Previous boundaries become more and more notional

- Network flows
  - Attack surface
  - Management interface
- Users community
  - Insider?
- Data flows

Cost/Benefit not doing it?

- Security policy comparison / enforcement

Considerations on deployment architectures

Typical situations

- Web Browser SSO Profile
- SP-Initiated SSO
- Redirect/POST Bindings

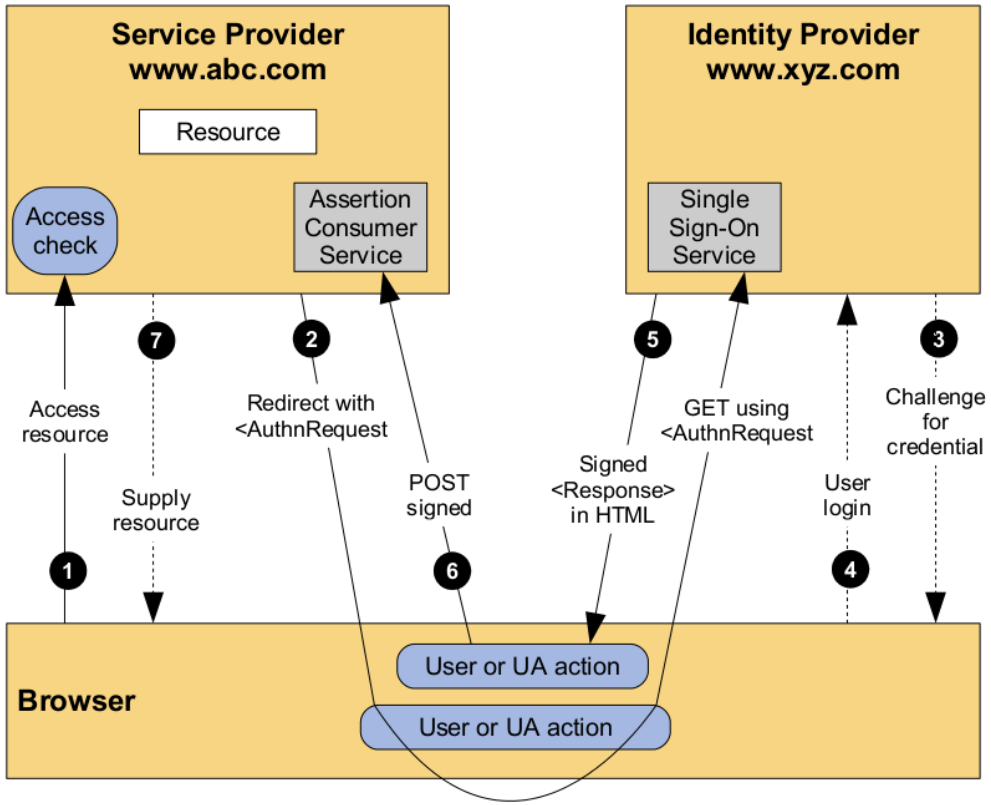
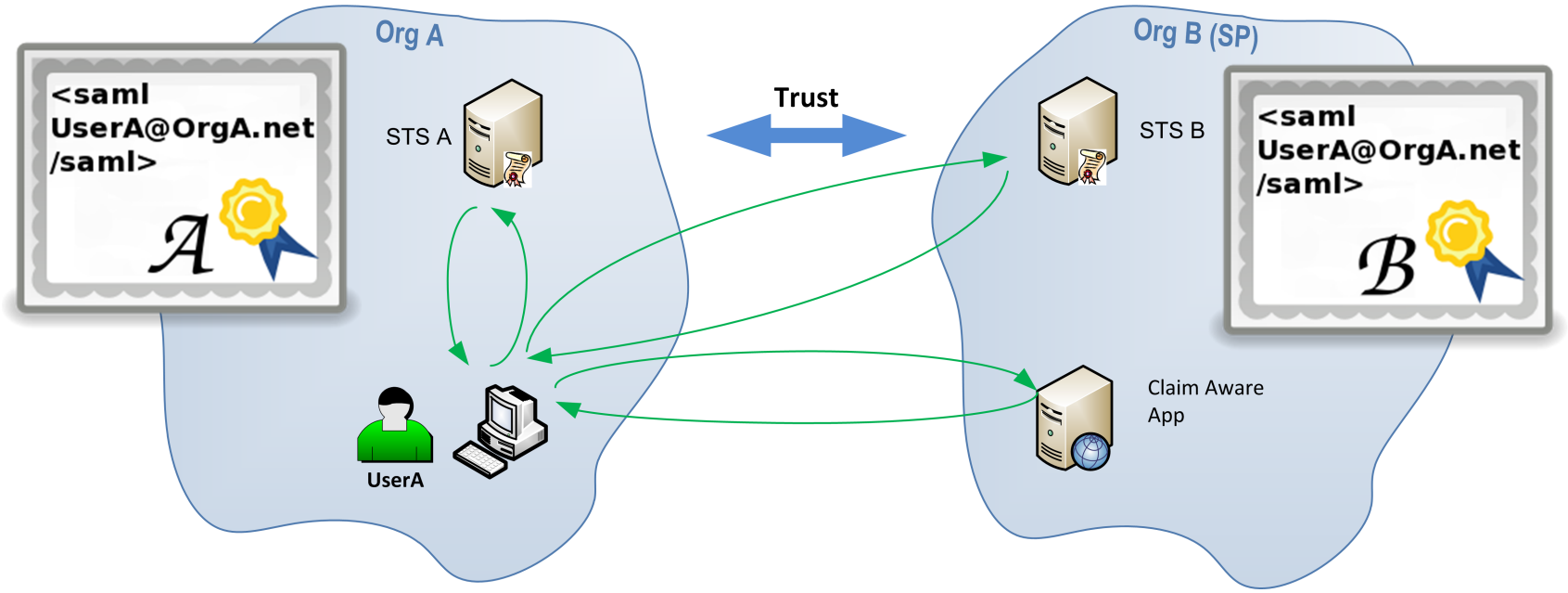


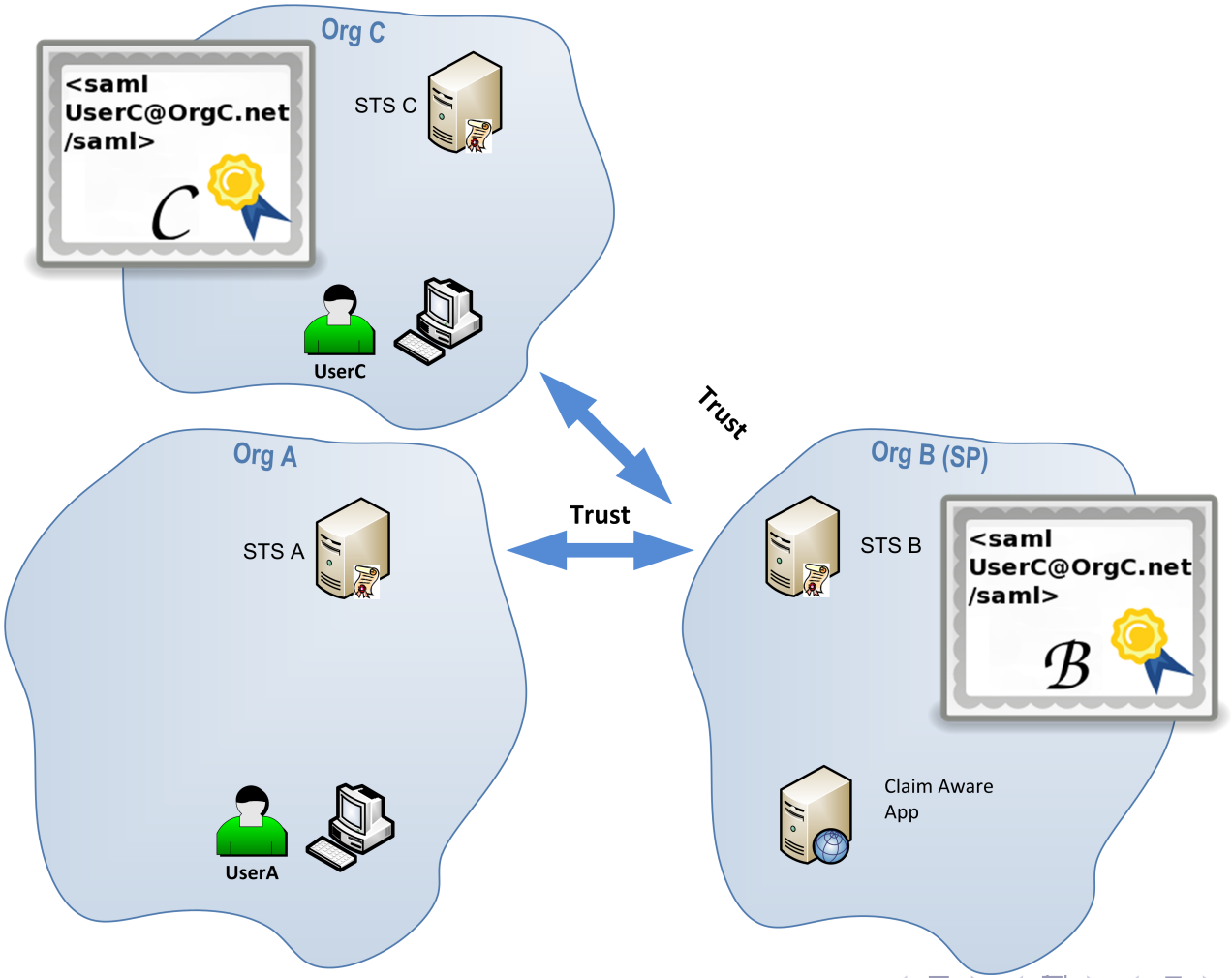
Figure 15 of [3]

Similar flows orchestrated in federated environment

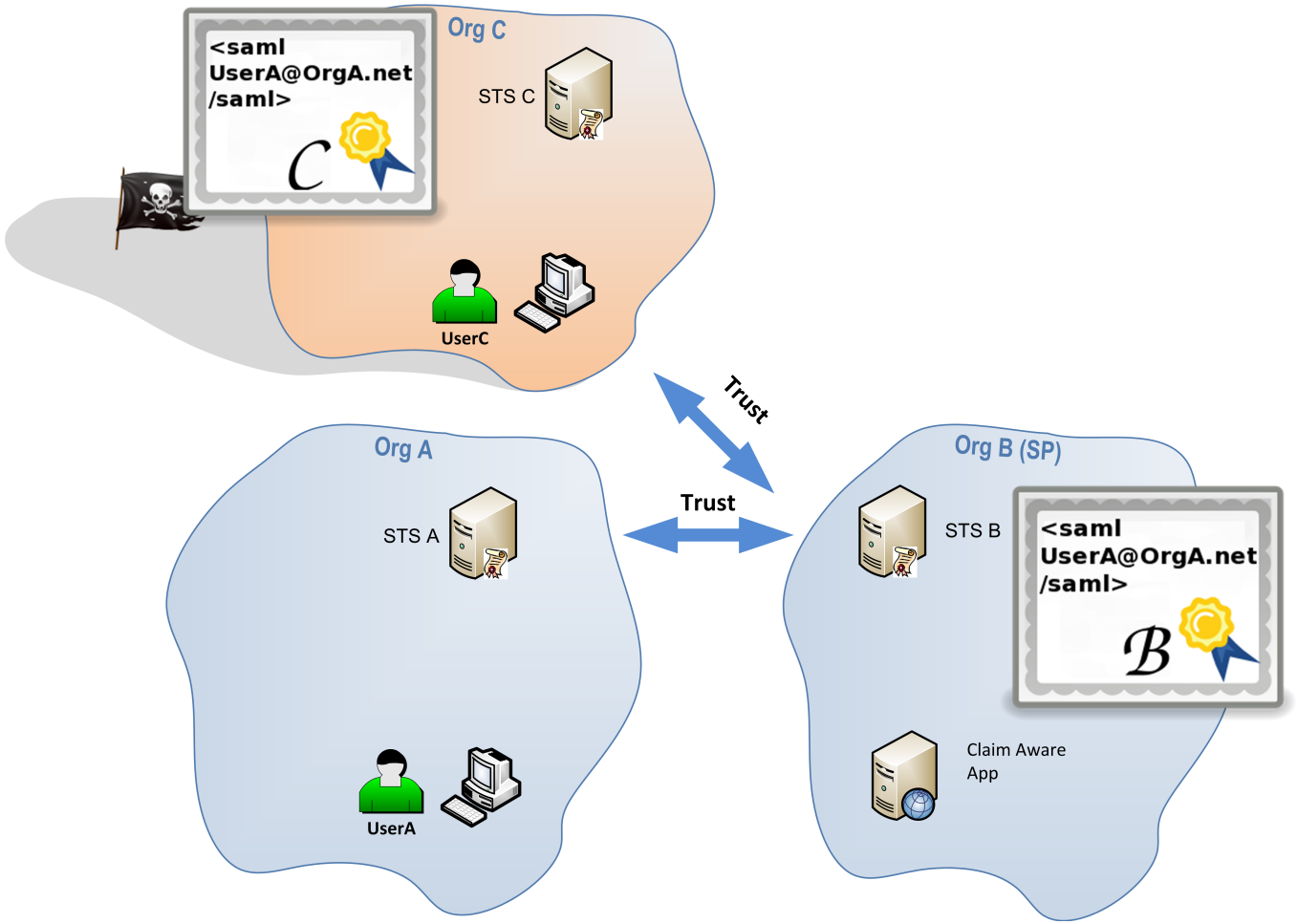
simple federation scenario [24]



Similar flows orchestrated in federated environment



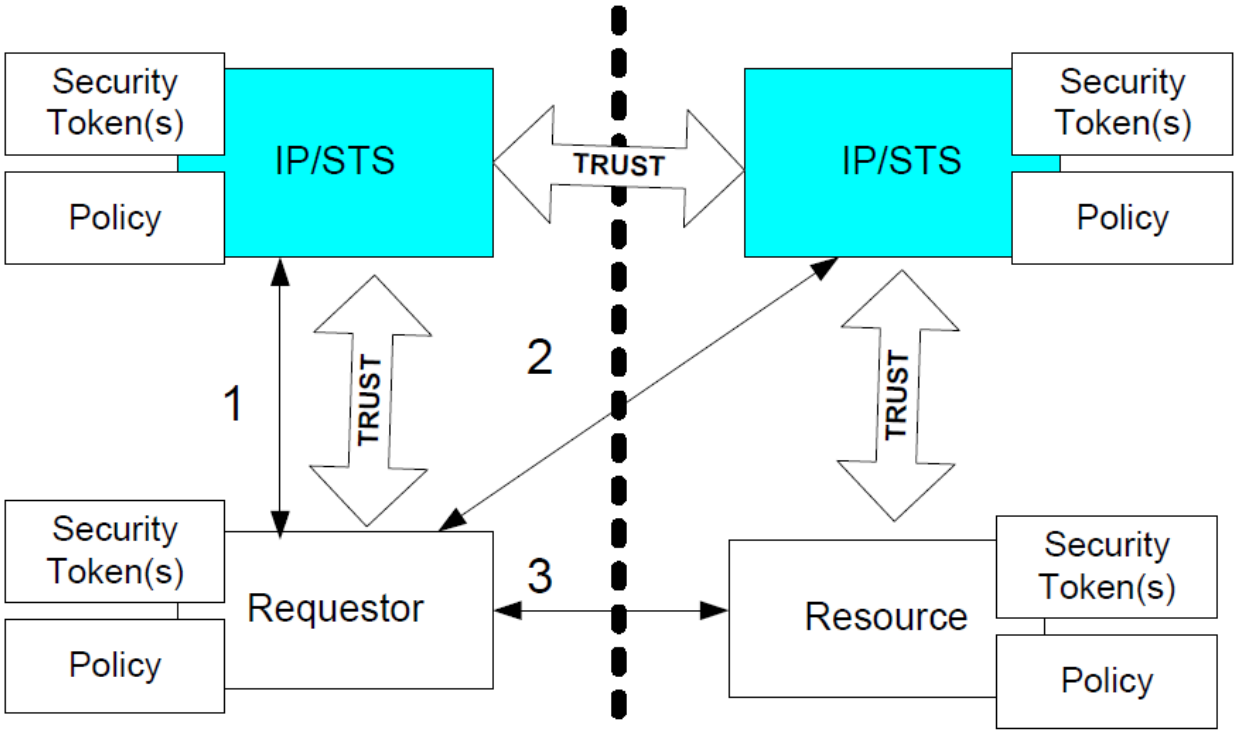
What if OrgC signs a claim for userA@orgA.net?



Considerations on deployment architectures

Trust topology

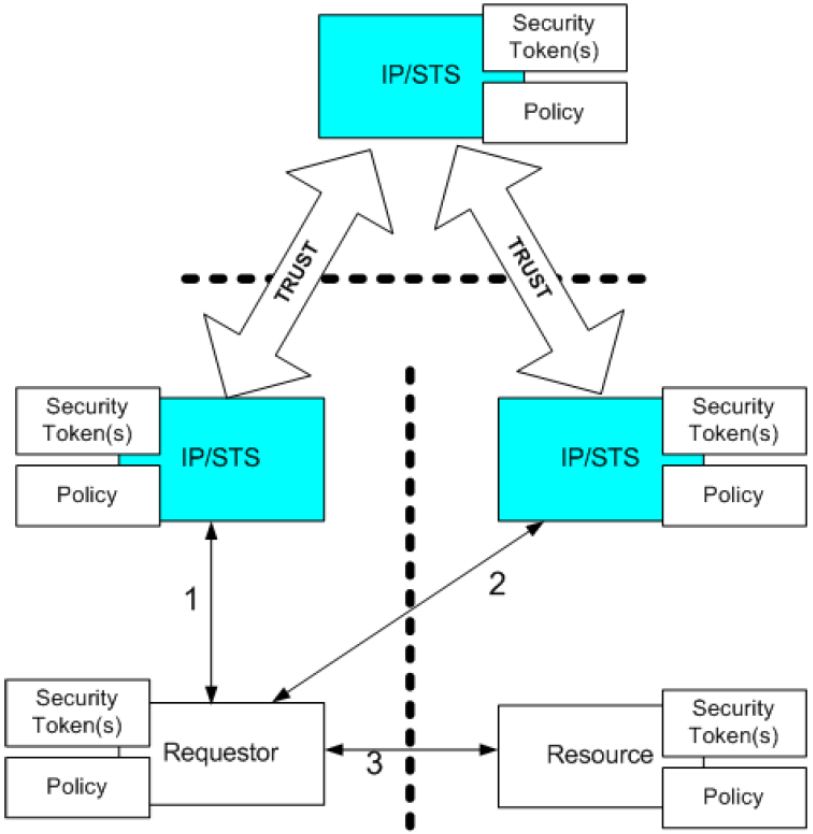
- Previous example follows a direct trust topology



Considerations on deployment architectures

Trust topology

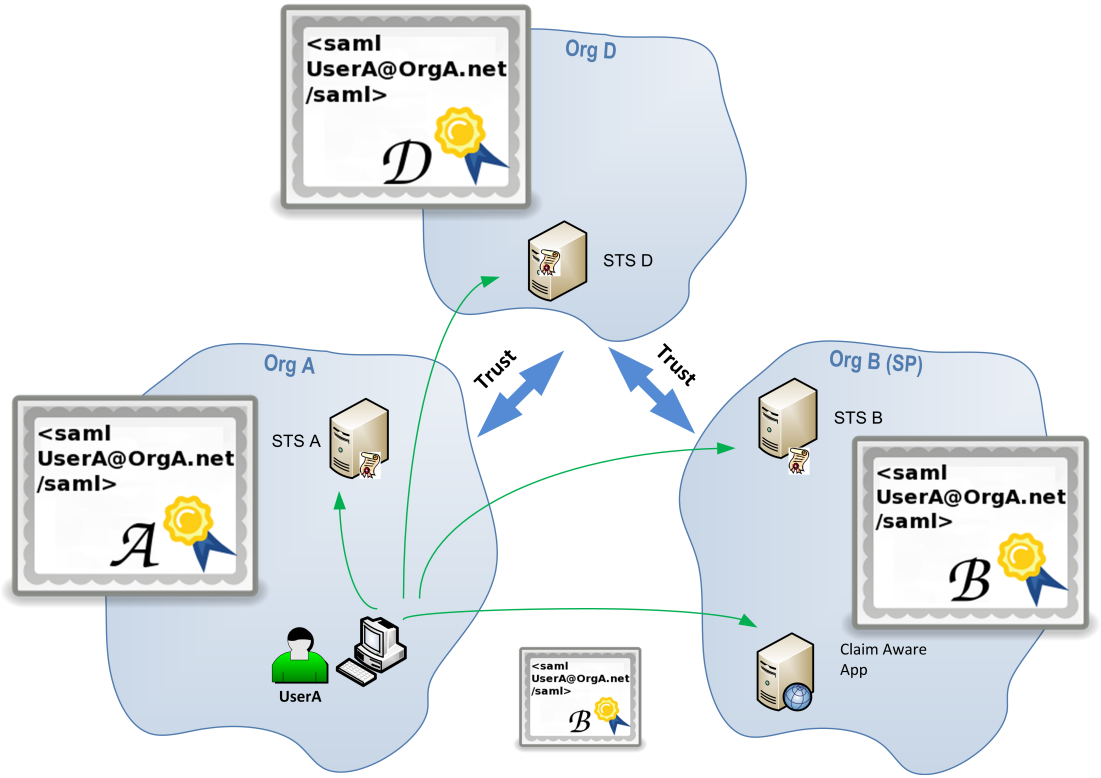
- More complex exist including indirect trust topology



Considerations on deployment architectures

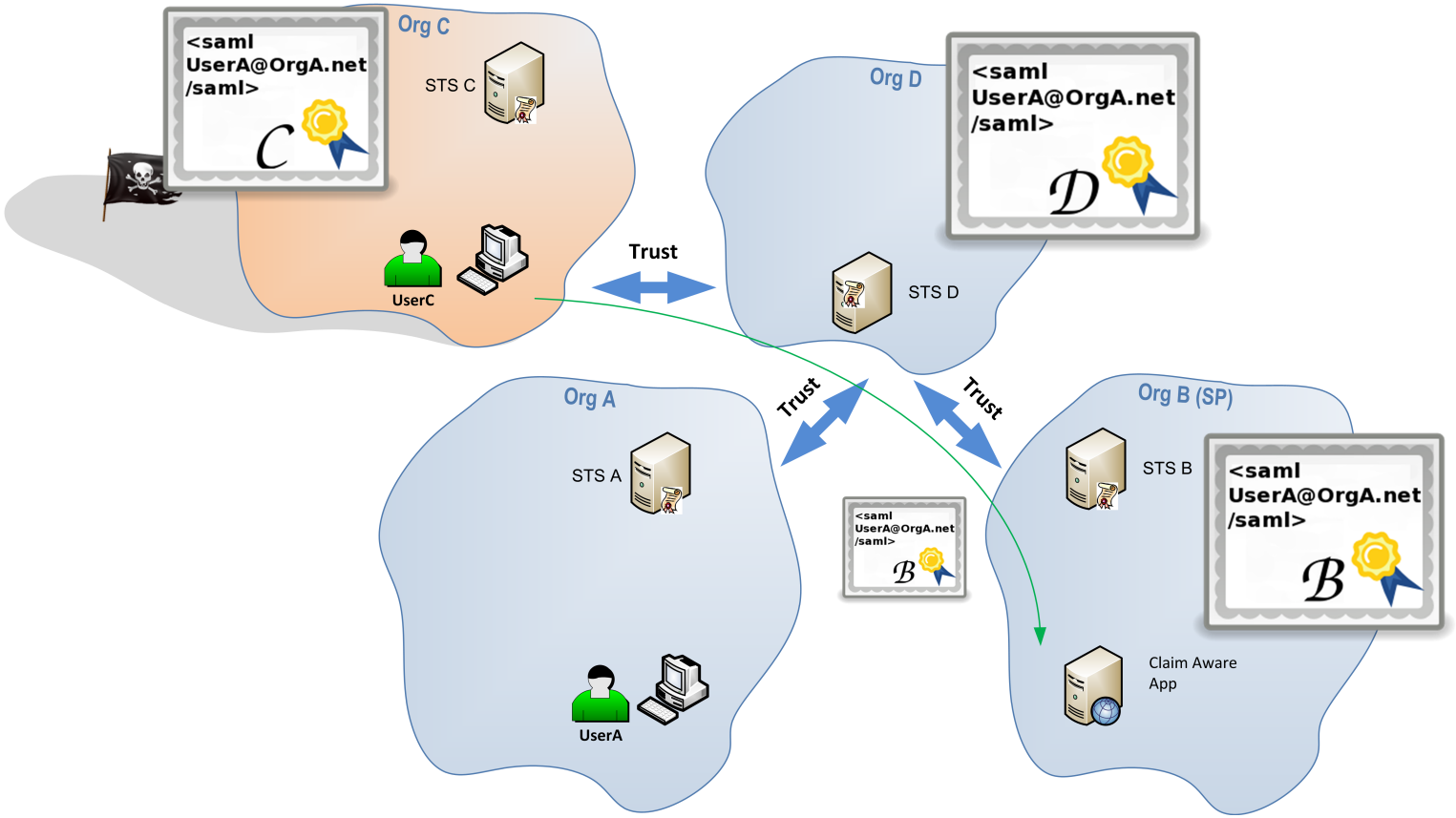
Trust topology

- More complex exist including indirect trust topology



What if OrgC signs a claim for userA@orgA.net?

SAML claims laundering



SAML claims laundering

- Questions usually unasked and even less answered:
  - What about a malicious/compromised IdP in the federation?
    - Can a malicious IdP impersonate another domain users?
    - Are there safeguards in place?
    - Do I own or delegate these safeguards?
  - What about a malicious/compromised SP in the federation?
- Control the loss of control
  - Whose liability
  - Other parties obligation (accountability)

Outline

1. Prelude to Federation
   - Introduction
2. Forward the Federation
   - Where we come from
3. Federation
   - What you need to know
4. Federation and Empire
   - Sharpen your weapons
5. Federation's Edge
   - Design assessment
6. Federation and (down to) Earth
   - Conclusion

Conclusion

Take-aways

- Knowledge and tool to keep on powning SAML protected Web app
- Proven assumption: Standards can be read as an attempt to circumvent SOP
  - Process and tools to get there
- Important design security considerations
  - Without taking care, "Insecurity by design" is more than likely
  - E.g. Cross domain SSO with AD trust relationships
    - A compromised domain cannot impersonate other domains users
  - With SAML based cross domain SSO, by default, it will

Conclusion

- This apply to other form of federation with very few adaptation
- Developers, marketers ahead of security guys in this area. Yet default settings are not secure. The "make it working" approach might lead to insecure deployment. We need to catch up to avoid big deployment security failure (with probably thorny legal issues)
  - Get acquainted with protocols to properly assess designs and deployments
  - Adapt our tool set because bad guys will
- Incidentally some of these issues would also be solved more easily with a standardized solution as opposed to custom based checks by diligent administrators

Thanks for your attention

- Acknowledgment
  - Isaac Asimov
  - Rui Fiske for his great help and extensive knowledge on SAML
- Q & possibly A
- Buby modules and sample code at `http://code.google.com/p/buby-saml`

manu@veryopenid.net

References I

[1] Anonymity Support for Kerberos - draft-ietf-krb-wg-anon-04 - Kerberos extension

[2] Security Assertion Markup Language (SAML) 2.0 Technical Overview (draft 3) - OASIS - http://www.oasis-open.org/committees/download.php/11511/sstc-saml-tech-overview-2.0-draft-03.pdf

[3] Security Assertion Markup Language (SAML) 2.0 Technical Overview (draft 10) - OASIS - http://www.oasis-open.org/committees/download.php/20645/sstc-saml-tech-overview-2%200-draft-10.pdf

[4] D. Hardt - Identity 2.0 - OSCON 2005 Keynote - http://identity20.com/media/OSCON2005/

[5] K. Cameron - The Laws of Identity - http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

[6] R. Anderson - Can We Fix the Security Economics of Federated Authentication? - http://www.cl.cam.ac.uk/~rja14/Papers/sefa-pr11.pdf

References II

[7] C. Soghoian - Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1421553

[8] B. Hill - Attacking XML Security - Black Hat Briefings USA 2007 - http://www.isecpartners.com/files/iSEC_HILL_AttackingXMLSecurity_bh07.pdf

[9] Myth Breaker - The Best Open Source Web Application Vulnerability Scanner - http://sectooladdict.blogspot.com/2011/01/myth-breaker-best-open-source-web.html

[10] Web Application Scanner Benchmark (v1.0) http://sectooladdict.blogspot.com/2010/12/web-application-scanner-benchmark.html

[11] UNINETT releases public beta of SAML tracer - https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/

[12] Feide RnD SAML 2.0 Debugger - https://rnd.feide.no/software/saml_2_0_debugger/

References III

[13] Federation Lab beta - https://fed-lab.org/

[14] Burp Suite - http://portswigger.net

[15] J. Haddix, J. Parish - ToorCon 12 - http://www.securityaegis.com/burp_preso.pdf

[16] J. Haddix, J. Parish - Bsides Chicago 2011 - http://www.securityaegis.com/wp-content/uploads/2011/04/bsides_final.ppt

[17] Buby's homepage - http://emonti.github.com/buby

[18] Buby tutorial - K. Johnson - http://carnal0wnage.attackresearch.com/2011/05/buby-script-basics-part-1.html

[19] Feide - http://www.feide.no

[20] WCF Binary Soap Plug-In for Burp - Gotham Digital Science - http://www.gdssecurity.com/l/b/2009/11/19/wcf-binary-soap-plug-in-for-burp/

[21] OWASP Open Redirect - https://www.owasp.org/index.php/Open_redirect

References IV

[22] Identity Provider Discovery Service Protocol and Profile - OASIS - http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf

[23] Support metadata DiscoveryResponse for discovery service - SimpleSAMLphp issue 363 - http://code.google.com/p/simplesamlphp/issues/detail?id=363

[24] Web Services Federation Language (WS-Federation) Version 1.2 - OASIS - http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf