X.509 certificates for AAI

How to avoid common pitfalls

SWITCH

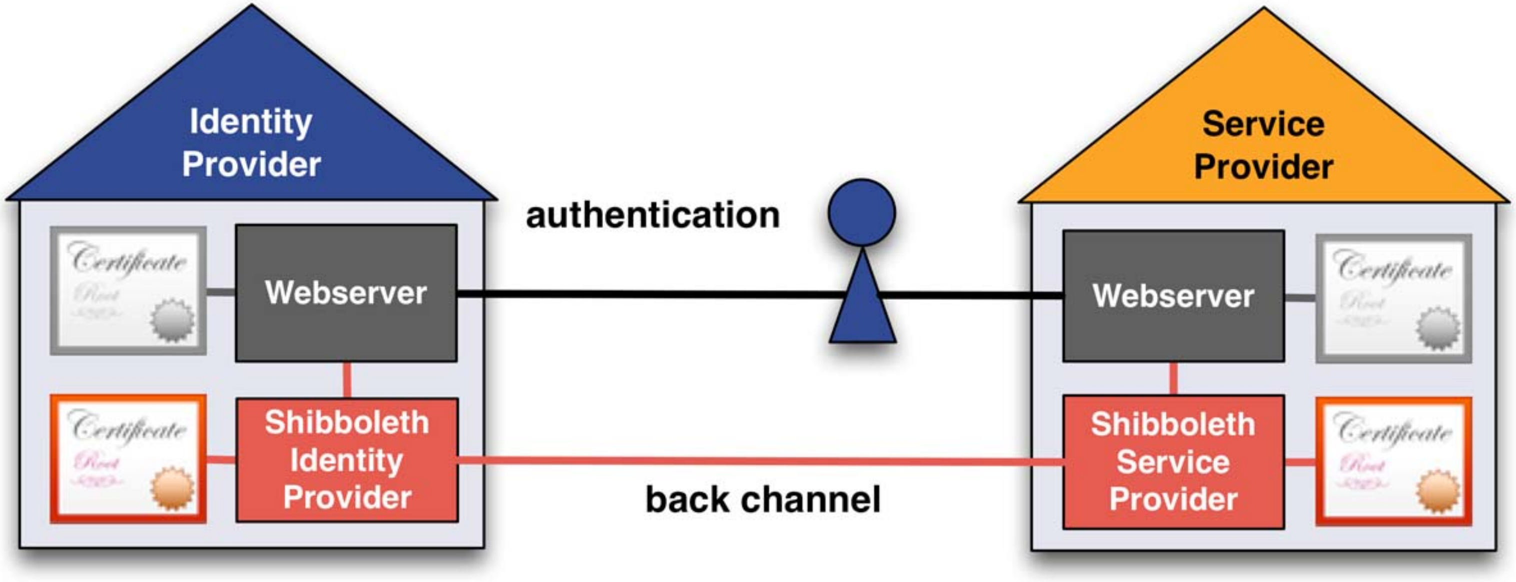
Serving Swiss Universities

Patrik Schnellmann
patrik.schnellmann@switch.ch

X.509 certificates for AAI

- Where AAI makes use of X.509 certificates
- Certificate chains
- CA root certificates as trust anchors

Where AAI uses X.509 certificates



- Protect user credentials
- Access to content on SP
- Attribute requests on back channel
- Sign / encrypt SAML assertions

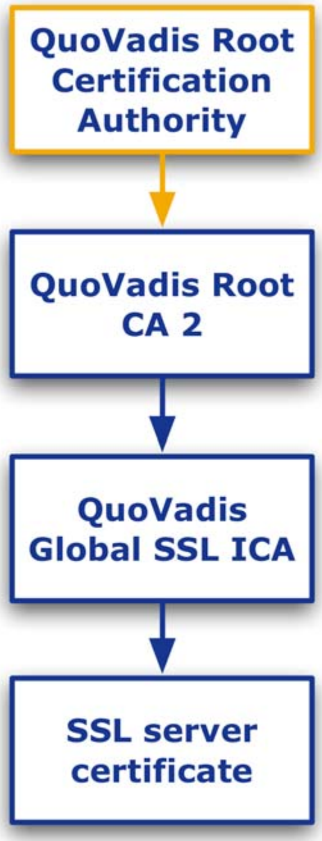
When it’s broken, you’re in trouble

Campagnolo 11s RECORD™ Chain

114 links

Chains of X.509 certificates

A beautiful chain in the PKI world:



QuoVadis Root Certification Authority

QuoVadis Root CA 2

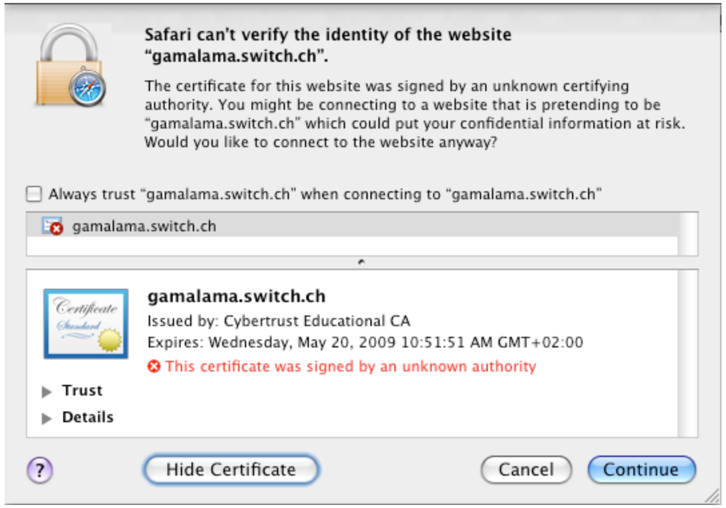
QuoVadis Global SSL ICA

SSL server certificate

Broken chains

Broken chains, the most frequent problem on Shibboleth Service Providers:

- Users get pop-ups, ...



Safari can't verify the identity of the website "gamalama.switch.ch".

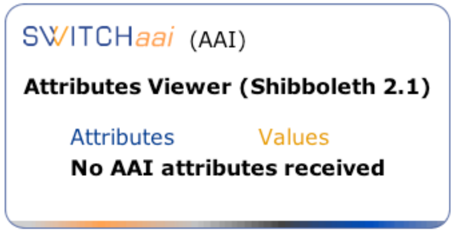
The certificate for this website was signed by an unknown certifying authority. You might be connecting to a website that is pretending to be "gamalama.switch.ch" which could put your confidential information at risk. Would you like to connect to the website anyway?

□ Always trust "gamalama.switch.ch" when connecting to "gamalama.switch.ch"

gamalama.switch.ch

gamalama.switch.ch
Issued by: Cybertrust Educational CA
Expires: Wednesday, May 20, 2009 10:51:51 AM GMT+02:00
This certificate was signed by an unknown authority

- ... but probably no attributes



SWITCHaai (AAI)

Attributes Viewer (Shibboleth 2.1)

Attributes	Values
No AAI attributes received	

Pick the right tool

Park Tool® Professional Tool Kit PK-63

Diagnose broken chains

Check if a server sends the full certificate chain:

```
openssl s_client -connect www.example.org:443 \
                          -showcerts < /dev/null
```

```
---
Certificate chain
0 s:/2.5.4.15=V1.0, Clause 5.(b)/serialNumber=CH-035.7.001.278-9/1.3.6.1.4.1.311.60.2.1.3=CH/
    1.3.6.1.4.1.311.60.2.1.2=Bern/C=CH/ST=Zuerich/L=Zuerich/O=SWITCH/CN=aai-logon.switch.ch
  i:/C=BM/O=QuoVadis Limited/OU=www.quovadisglobal.com/CN=QuoVadis Global SSL ICA
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
1 s:/C=BM/O=QuoVadis Limited/OU=www.quovadisglobal.com/CN=QuoVadis Global SSL ICA
  i:/C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
...
```

SWITCH also provides a web based tool to check certificate chains on:
https://tools.switch.ch/certchaintest/

The right tool

Park Tool® Chain Tool CT-3

Remedy broken chains

Apache httpd with mod_ssl

```
SSLCertificateChainFile    /etc/ssl/certs/chain.crt
SSLCertificateFile         /etc/ssl/certs/server.crt
SSLCertificateKeyFile      /etc/ssl/private/server.key
```

The directives point to PEM-encoded cert/key files.

Shibboleth

Concatenate PEM-encoded certificates in one file.

Other software

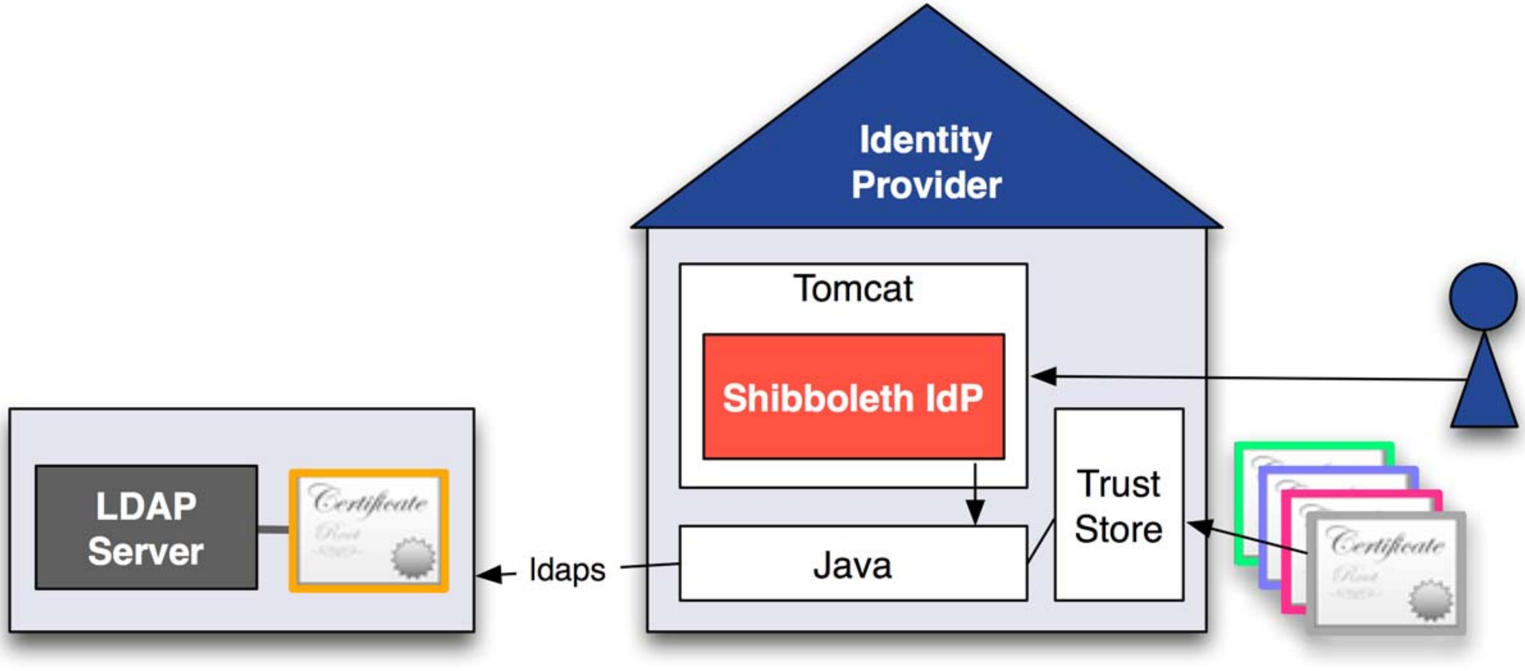
Refer to the manual

CA root certificates for trust stores

CAS webapp logs in the Tomcat logfile (catalina.out)

```
2008-09-30 17:55:12,821 INFO
  [org.jasig.cas.authentication.AuthenticationManagerImpl] -
  <AuthenticationHandler:
  org.jasig.cas.authentication.handler.support.JaasAuthenticationHa
  ndler failed to authenticate the user which provided the
  following credentials: username>
javax.security.auth.login.LoginException:
  javax.naming.CommunicationException: simple bind failed:
  ldap.switch.ch:636 [Root exception is
  javax.net.ssl.SSLHandshakeException:
  sun.security.validator.ValidatorException: PKIX path building
  failed:
  sun.security.provider.certpath.SunCertPathBuilderException:
  unable to find valid certification path to requested target]
```

CA root certificates for truststores, 2



CA root certificates for trust stores, 3

Trust store for Java / Tomcat:

JVM default

$JAVA_HOME/jre/lib/security/cacerts (password changeit)

Java system property setting

javax.net.ssl.trustStore

Tomcat connector setting

truststoreFile / truststorePass

Apache CA certificates for client authentication:

SSLCACertificateFile or
SSLCACertificatePath

Hassle-free security with X.509 certificates

Life would be much simpler without chains!