

SFU

SIMON FRASER UNIVERSITY
THINKING OF THE WORLD



Authorizing REST Services with CAS

No Rest for the Not Ticketed

Jasig Conference May 2011



Monday, June 6, 2011



About Me

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011

- Jeremy Rosenberg
Developer in IT services since 2004
Identity management strategy
Java Developer



About Me

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD



About SFU

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011

- One University - Three campuses



Simon Fraser
1776 -1862



About SFU

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

- One University - Three campuses
 - Burnaby



Simon Fraser
1776 -1862



About SFU

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

- One University - Three campuses
 - Burnaby
 - Surrey
 - Vancouver
- 32,000 students
- 900 faculty



Simon Fraser
1776 -1862



About SFU

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

- One University - Three campuses
 - Burnaby
 - Surrey
 - Vancouver
- 32,000 students
- 900 faculty
- 1600 staff
- 100,000 alumni



Simon Fraser
1776 -1862



About SFU

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD



About This Presentation

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011

- Disclaimer



About This Presentation

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011

- Disclaimer
- Definitions



About This Presentation

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011

- Disclaimer
- Definitions
- Backstory



About This Presentation

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

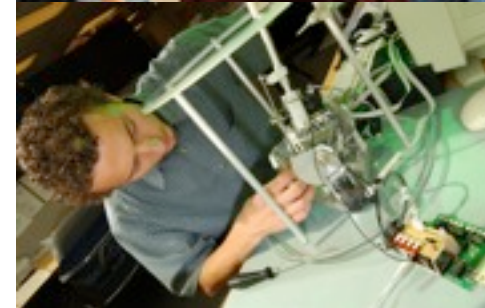
Monday, June 6, 2011

- Disclaimer
- Definitions
- Backstory
- Walkthroughs



About This Presentation

- Disclaimer
- Definitions
- Backstory
- Walkthroughs
 - SOAP



About This Presentation

- Disclaimer
- Definitions
- Backstory
- Walkthroughs
 - SOAP
 - REST



About This Presentation

- Disclaimer
- Definitions
- Backstory
- Walkthroughs
 - SOAP
 - REST
- Questions



About This Presentation

Disclaimer

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011

I'm not Ray:

Disclaimer

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011

I'm not Ray:



Disclaimer

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011

Definitions

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Web Service:

Definitions

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011

Web Service:

- An API to a remote procedure

Definitions

Web Service:

- An API to a remote procedure
- Typically accessed over HTTP

Definitions

Web Service:

- An API to a remote procedure
- Typically accessed over HTTP
- Machine-to-machine communications

Definitions

Web Service:

- An API to a remote procedure
- Typically accessed over HTTP
- Machine-to-machine communications
- Allows data source to be loosely coupled to applications

Definitions

Web Service:

- An API to a remote procedure
- Typically accessed over HTTP
- Machine-to-machine communications
- Allows data source to be loosely coupled to applications
- Makes systems reusable

Definitions

Web Service:

- An API to a remote procedure
- Typically accessed over HTTP
- Machine-to-machine communications
- Allows data source to be loosely coupled to applications
- Makes systems reusable
- Very popular with Twitter, Facebook, Amazon, etc

Definitions

Definitions - SOAP vs REST

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

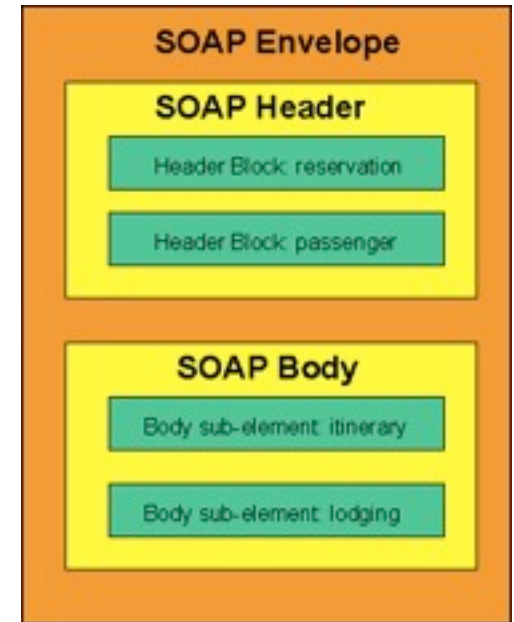
Monday, June 6, 2011

SOAP:

Definitions - SOAP vs REST

SOAP:

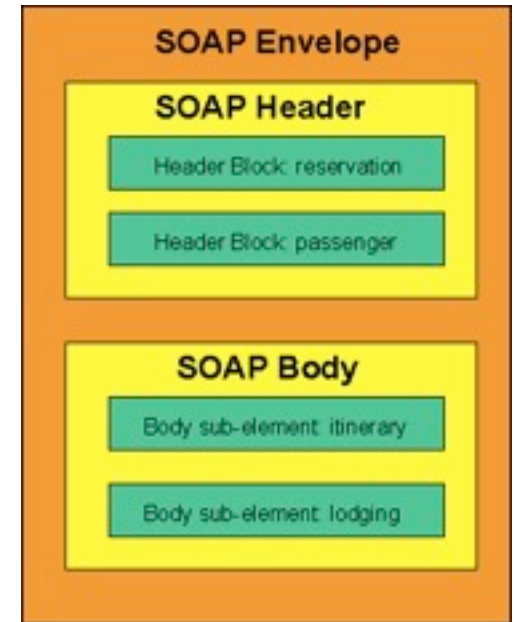
- XML Message passing protocol



Definitions - SOAP vs REST

SOAP:

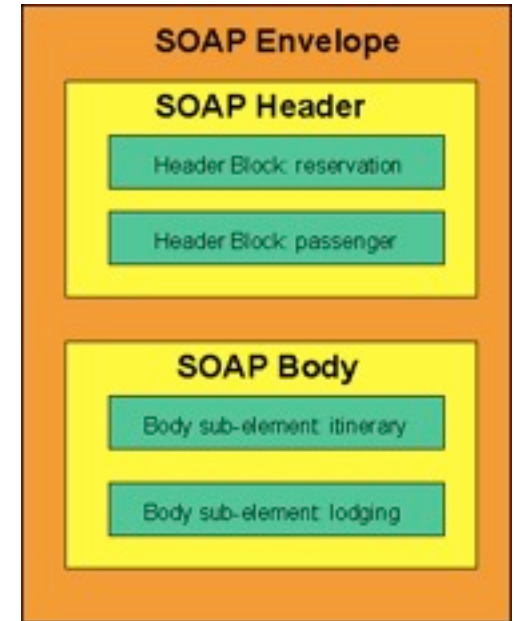
- XML Message passing protocol
- Numerous 'WS-' standards



Definitions - SOAP vs REST

SOAP:

- XML Message passing protocol
- Numerous 'WS-' standards
- Associated with "Big" Web Services
 - Most vendor SOA solutions use SOAP



Definitions - SOAP vs REST

Definitions - SOAP vs REST

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011

REST:

- URL-addressable objects

Definitions - SOAP vs REST

REST:

- URL-addressable objects
 - <http://maps.google.com/maps/api/geocode/xml?address=Memorial+University,+NL,+CA>

Definitions - SOAP vs REST

REST:

- URL-addressable objects
 - “<http://maps.google.com/maps/api/geocode/xml?address=Memorial+University,+NL,+CA>”
- Accessed and manipulated with standard HTTP GET/POST/PUT/DELETE

Definitions - SOAP vs REST

REST:

- URL-addressable objects
 - <http://maps.google.com/maps/api/geocode/xml?address=Memorial+University,+NL,+CA>
- Accessed and manipulated with standard HTTP GET/POST/PUT/DELETE
- Lightweight client requirements

Definitions - SOAP vs REST

REST:

- URL-addressable objects
 - “<http://maps.google.com/maps/api/geocode/xml?address=Memorial+University,+NL,+CA>”
- Accessed and manipulated with standard HTTP GET/POST/PUT/DELETE
- Lightweight client requirements
- Stateless (every request is self-contained)

Definitions - SOAP vs REST

REST:

- URL-addressable objects
 - <http://maps.google.com/maps/api/geocode/xml?address=Memorial+University,+NL,+CA>
- Accessed and manipulated with standard HTTP GET/POST/PUT/DELETE
- Lightweight client requirements
- Stateless (every request is self-contained)
- WS- standards are less mature

Definitions - SOAP vs REST

XML Gateway - What it does

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011

- Parses all Inbound ***and*** outbound XML messages

XML Gateway - What it does

- Parses all Inbound ***and*** outbound XML messages
- Inspection ***and*** modification of XML messages

XML Gateway - What it does

- Parses all Inbound **and** outbound XML messages
- Inspection **and** modification of XML messages
 - Replace “Username” value in inbound XML message with value extracted from client certificate
 - Prevent spoofing

XML Gateway - What it does

- Parses all Inbound **and** outbound XML messages
- Inspection **and** modification of XML messages
 - Replace “Username” value in inbound XML message with value extracted from client certificate
 - Prevent spoofing
 - Blank-out Student Number value in outbound XML messages
 - Prevent accidental leakage of confidential info

XML Gateway - What it does

SOAP Security - Cowboy Style

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011



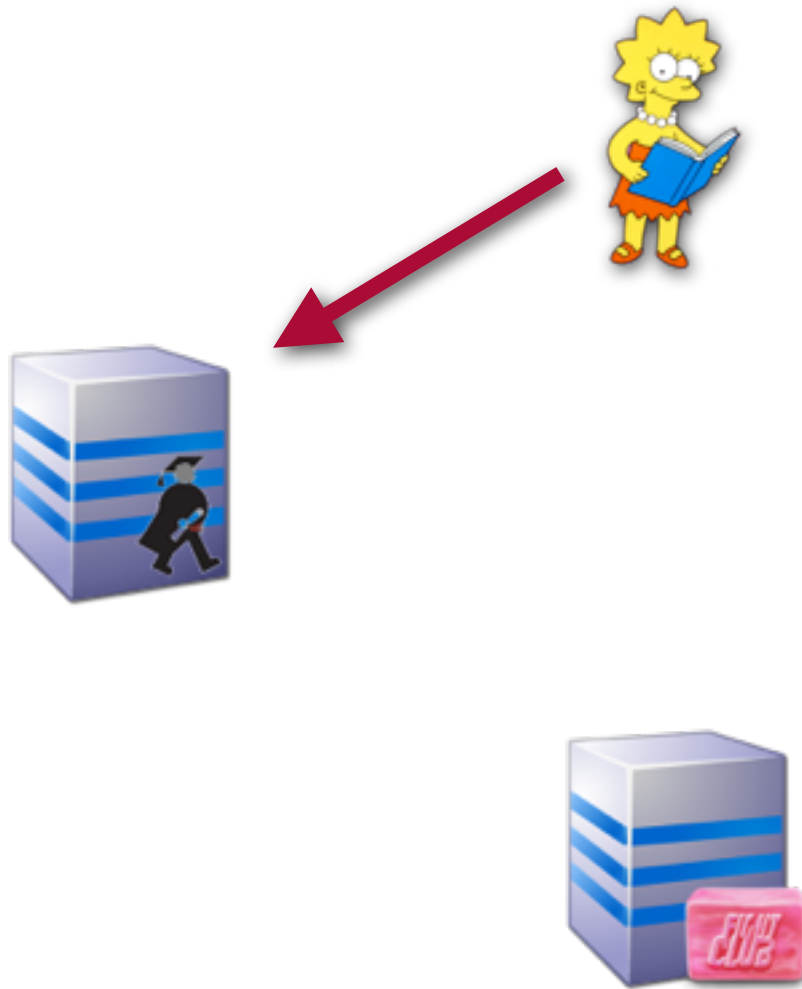
SOAP Security - Cowboy Style

IT Services - Jeremy Rosenberg

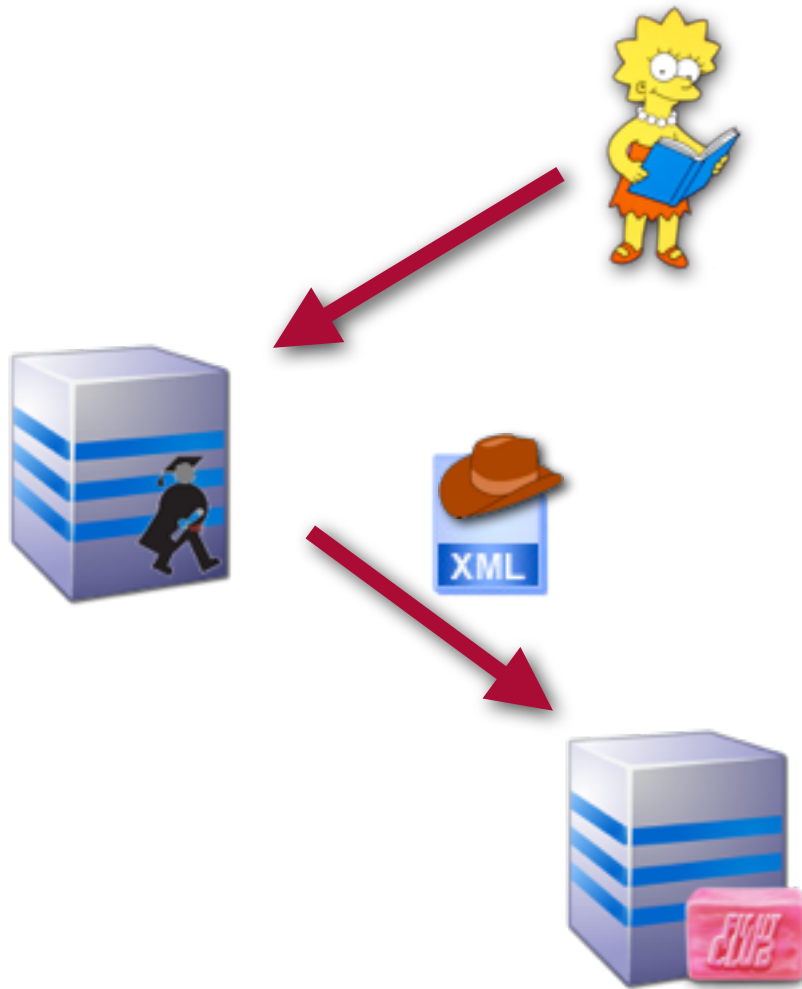


SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

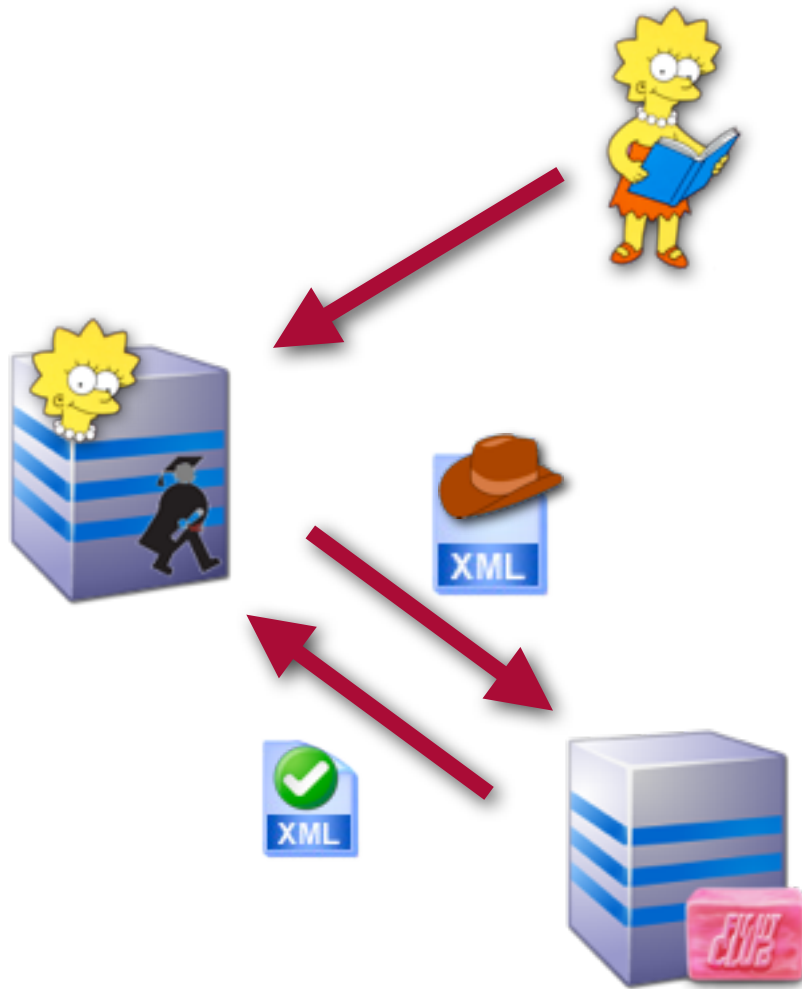
Monday, June 6, 2011



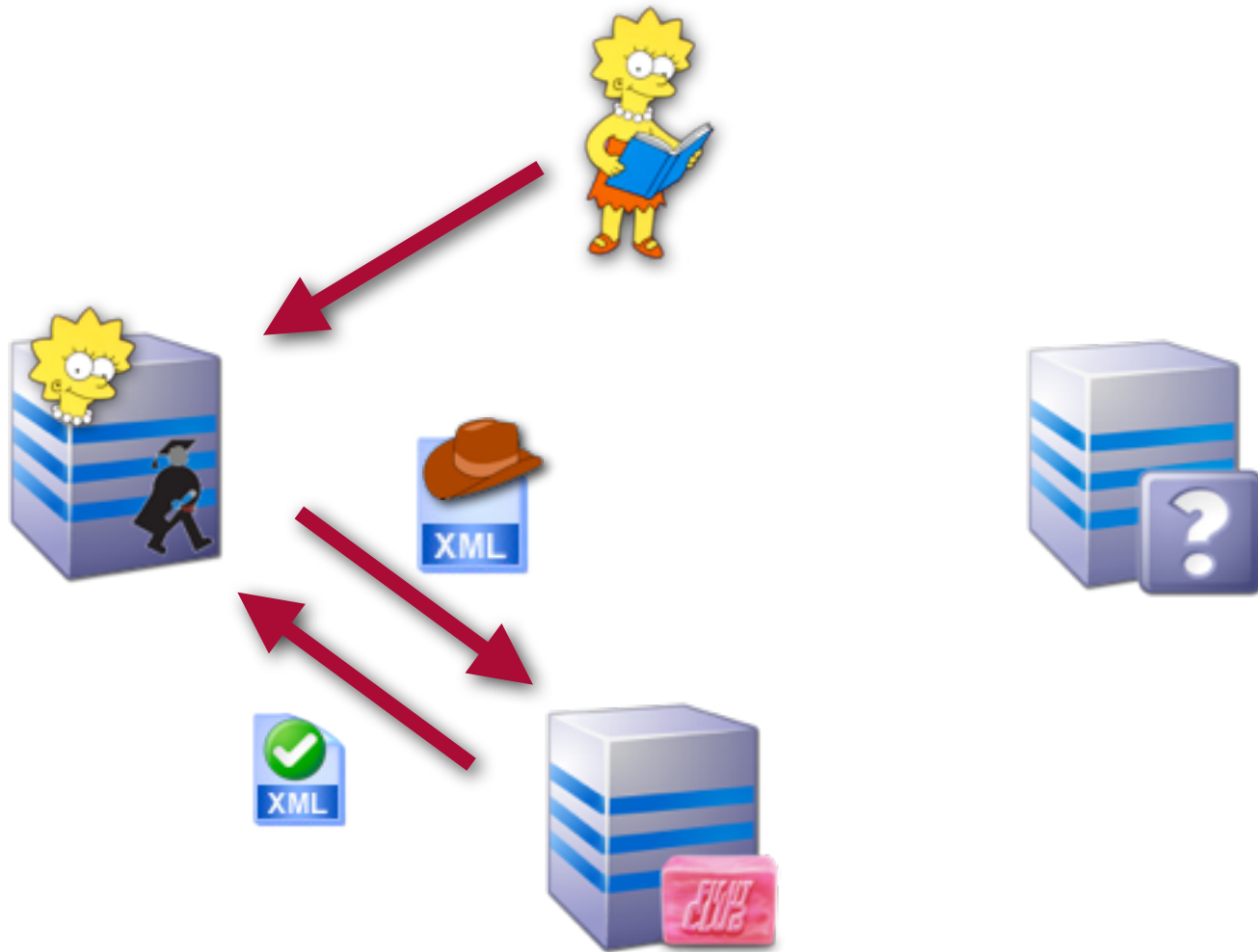
SOAP Security - Cowboy Style



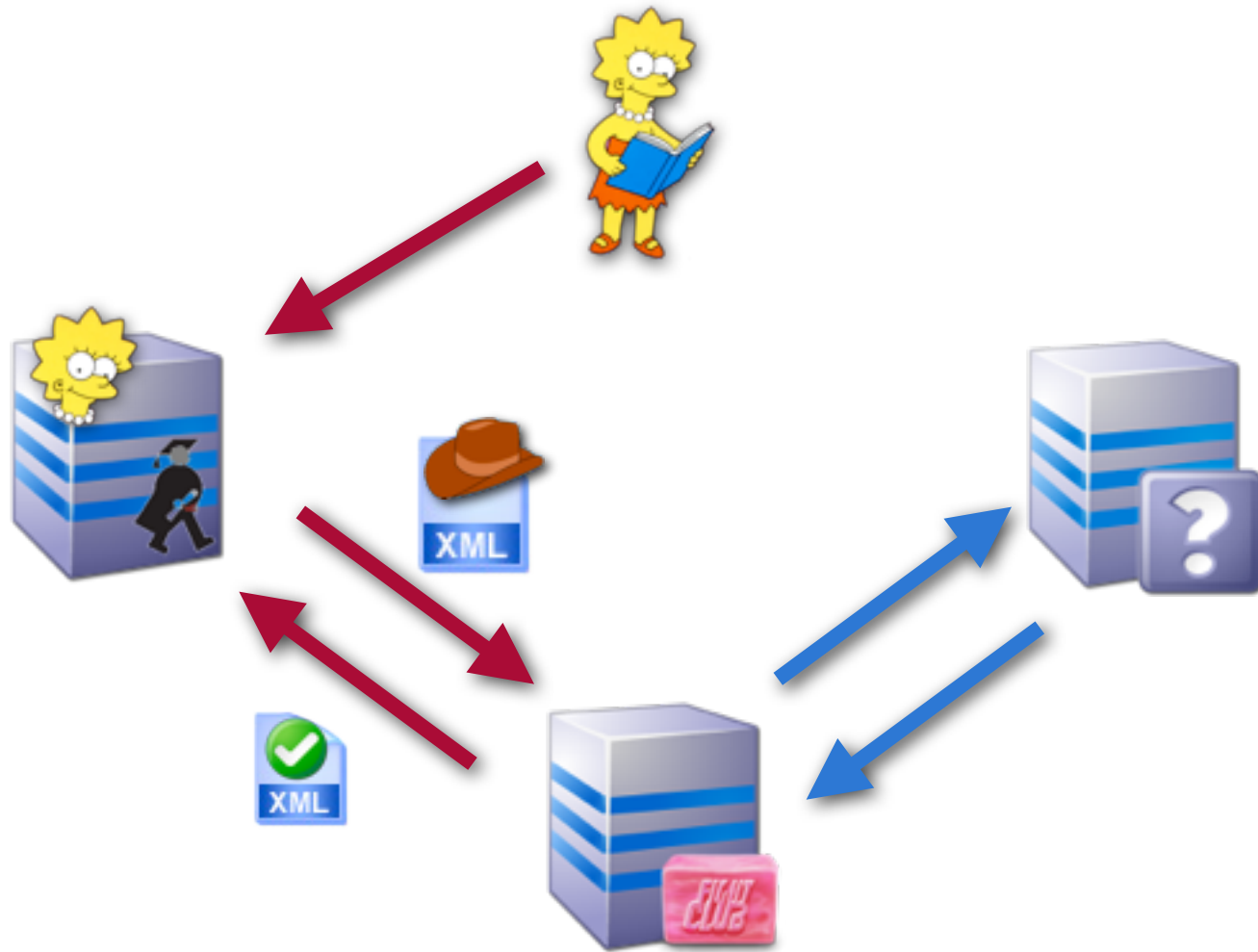
SOAP Security - Cowboy Style



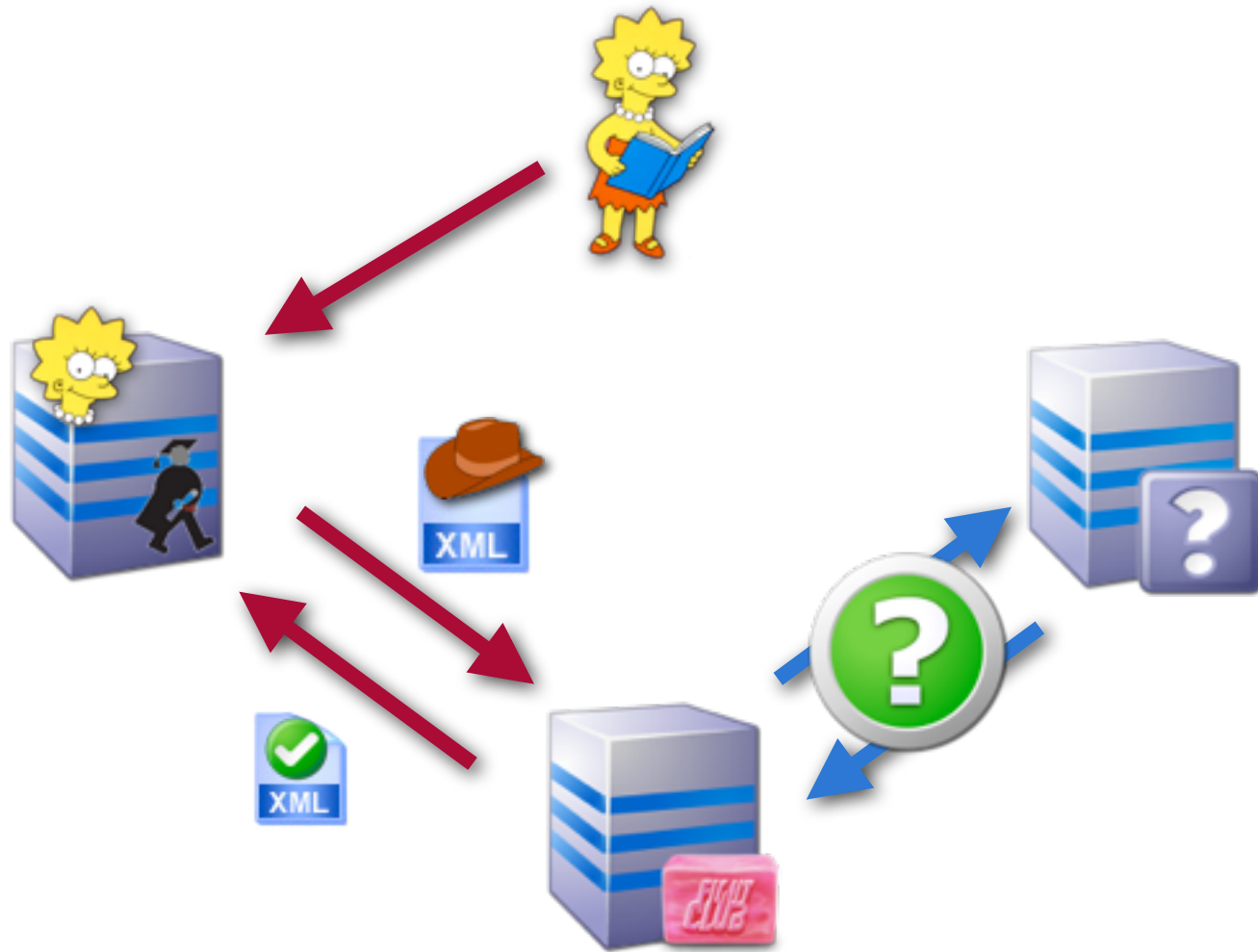
SOAP Security - Cowboy Style



SOAP Security - Cowboy Style



SOAP Security - Cowboy Style



SOAP Security - Cowboy Style

SOAP Security - Best Practices

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011



SOAP Security - Best Practices

IT Services - Jeremy Rosenberg

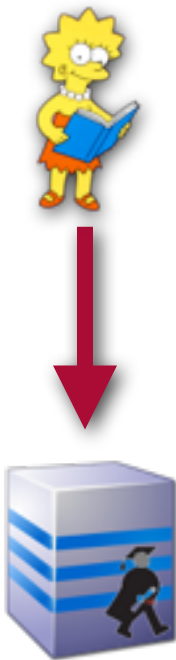


SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

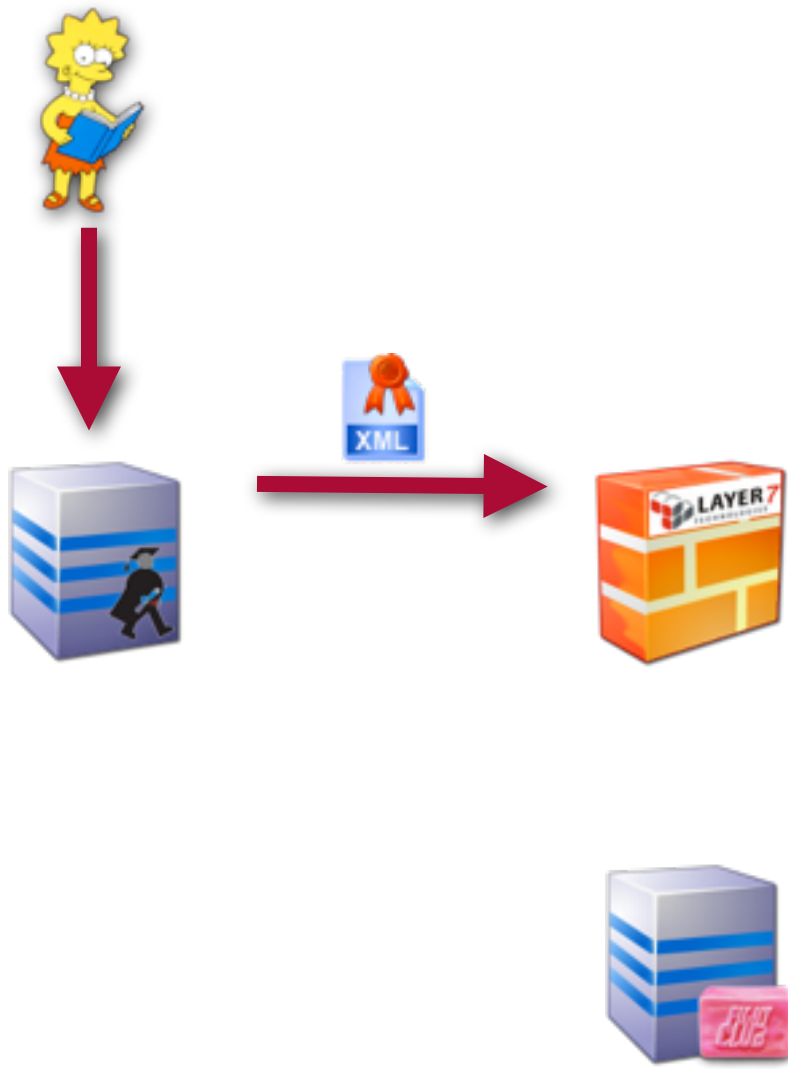
Monday, June 6, 2011



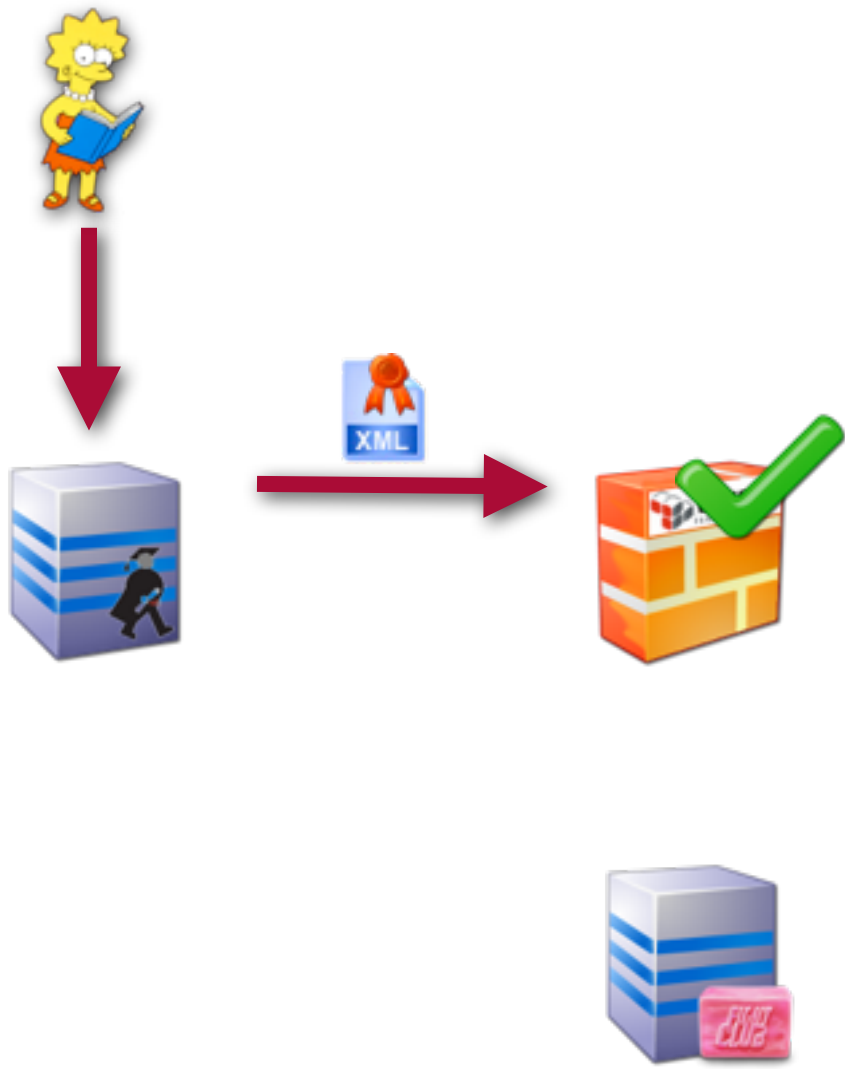
SOAP Security - Best Practices



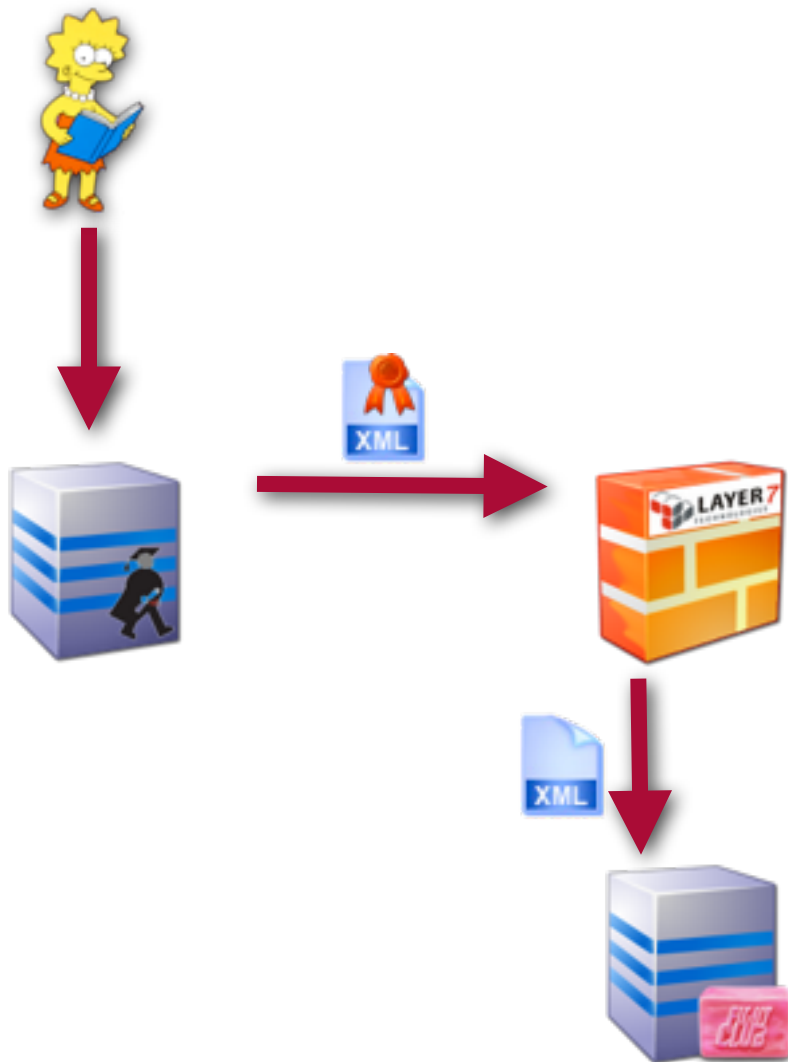
SOAP Security - Best Practices



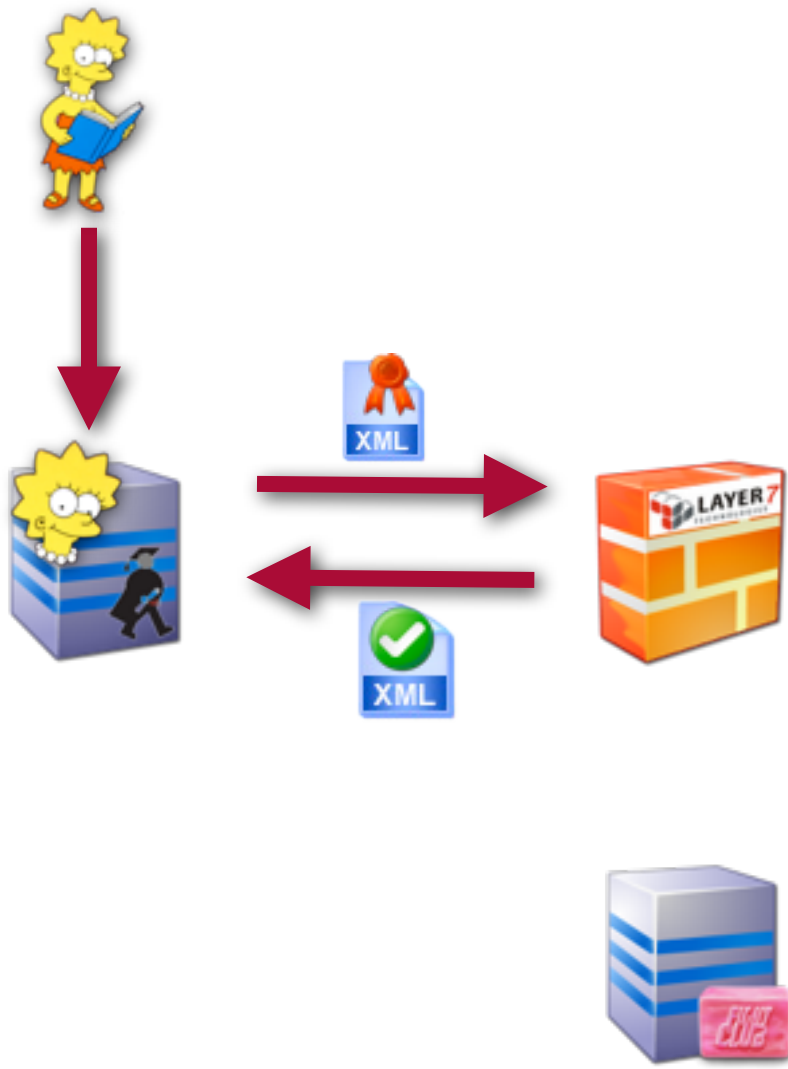
SOAP Security - Best Practices



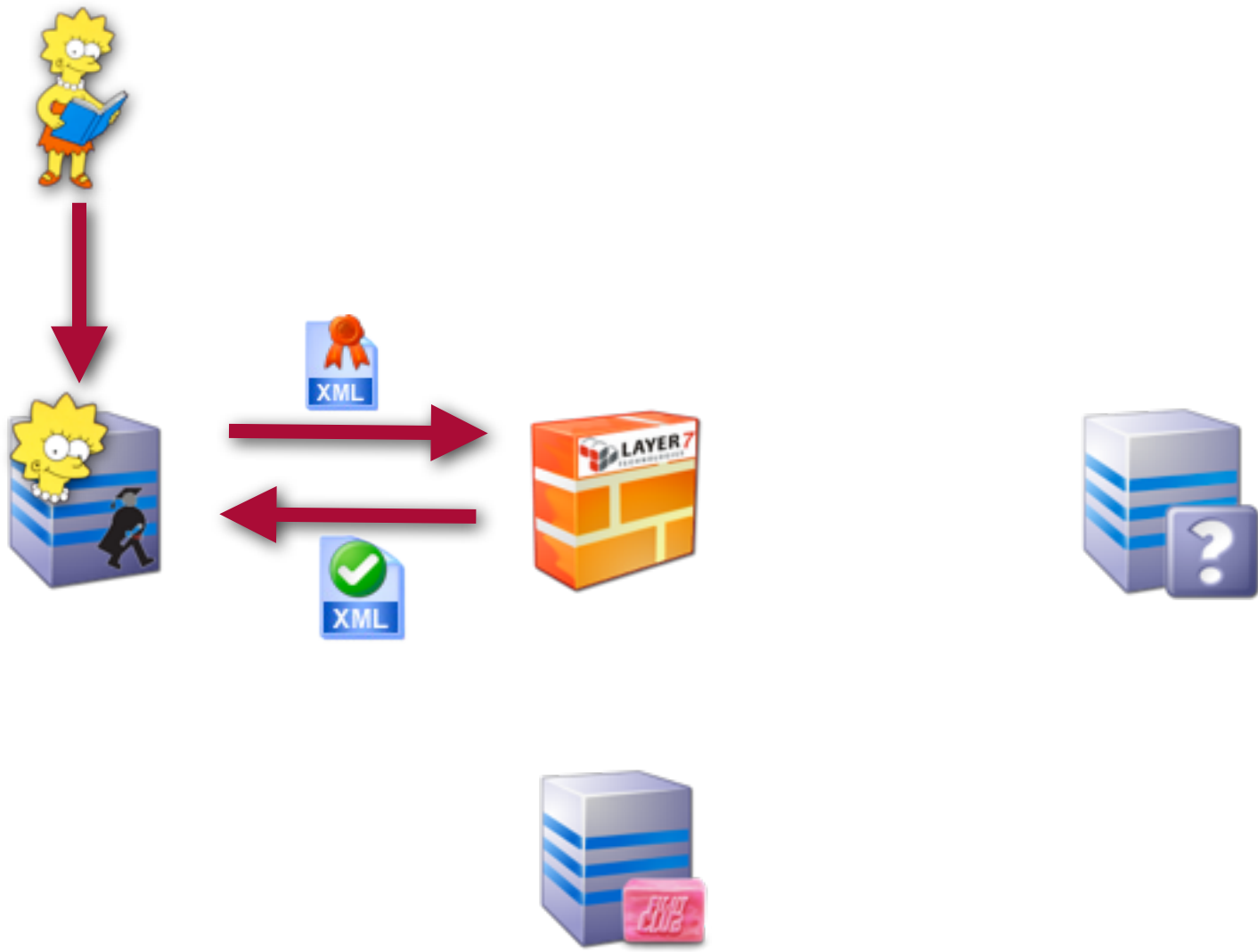
SOAP Security - Best Practices



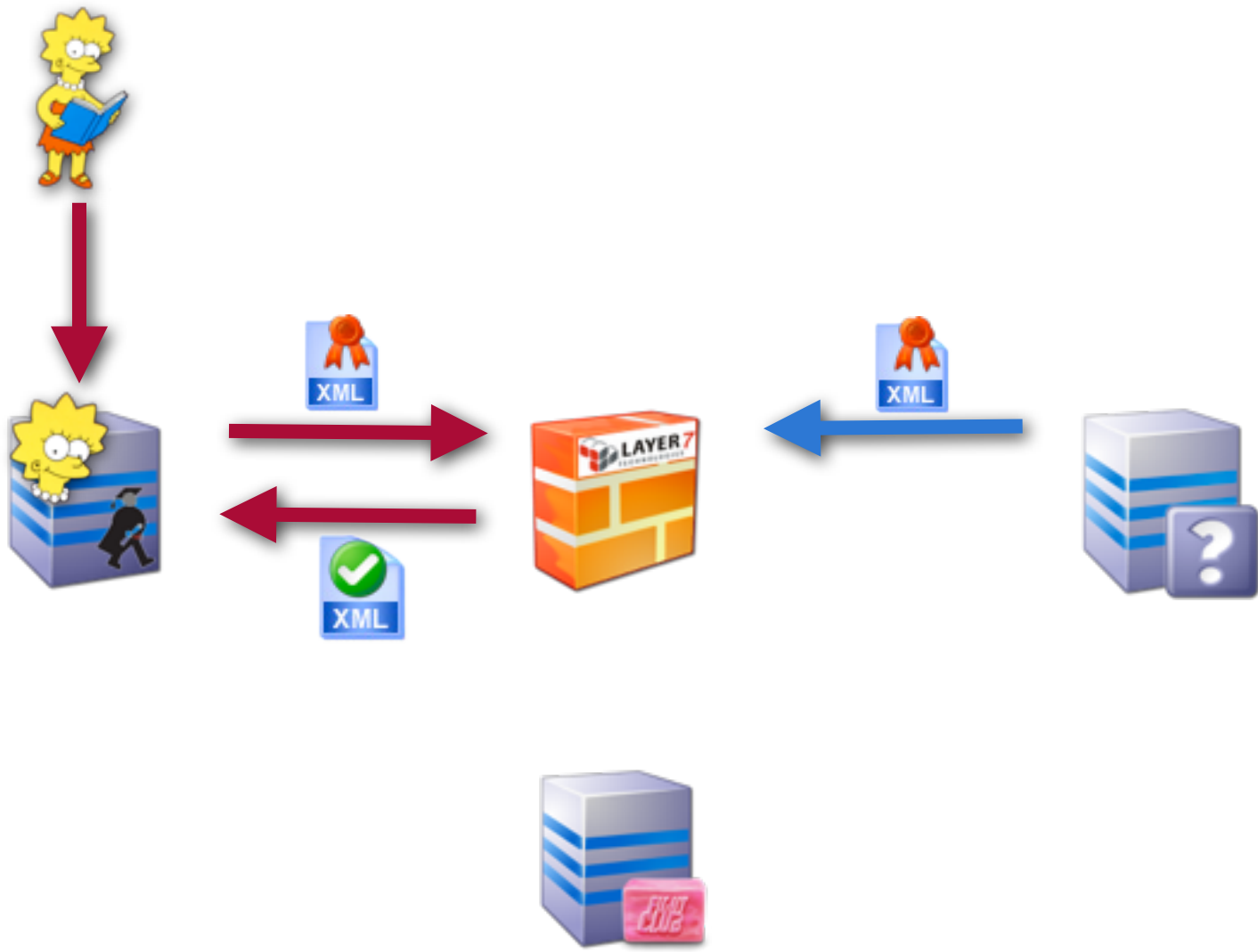
SOAP Security - Best Practices



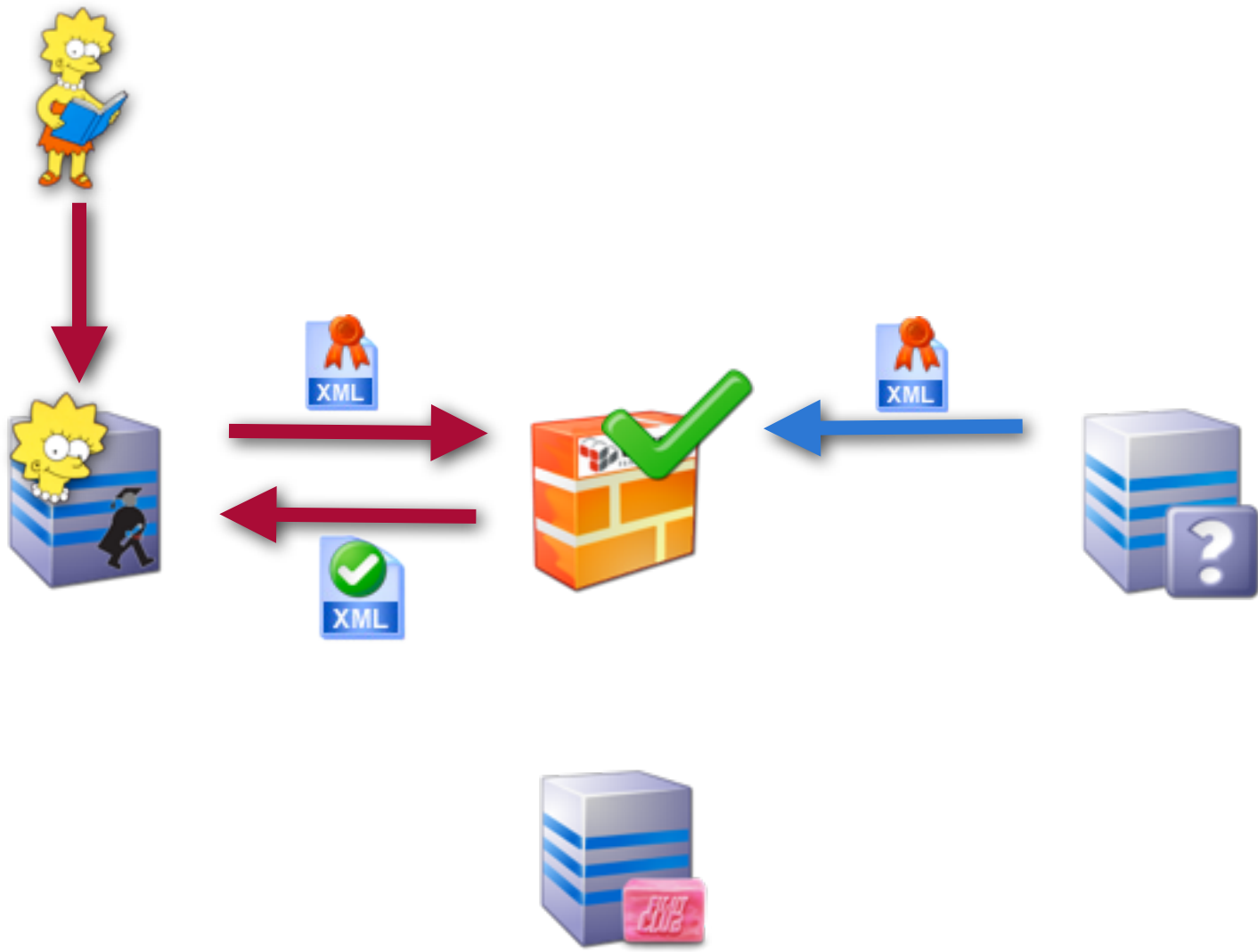
SOAP Security - Best Practices



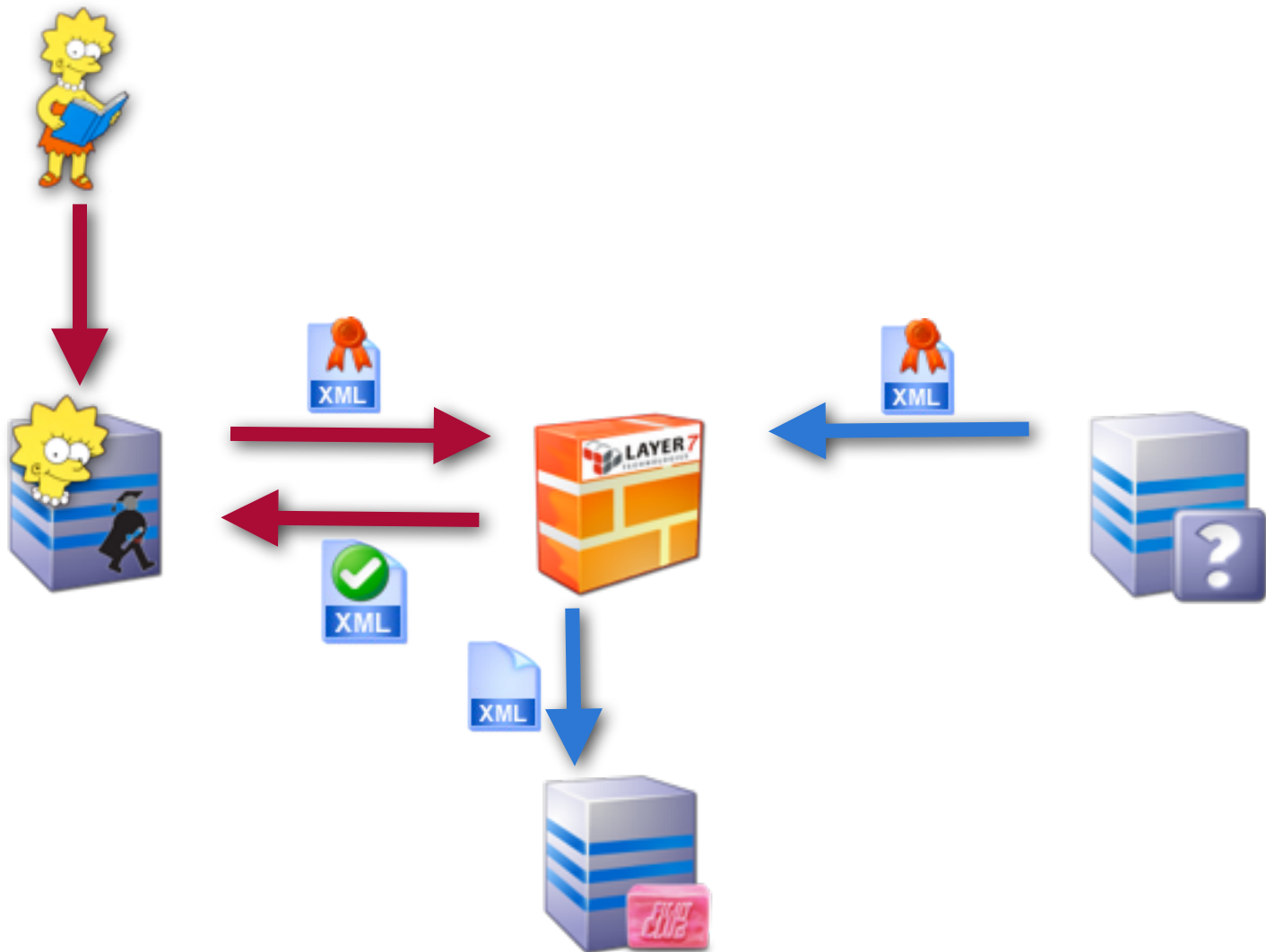
SOAP Security - Best Practices



SOAP Security - Best Practices



SOAP Security - Best Practices



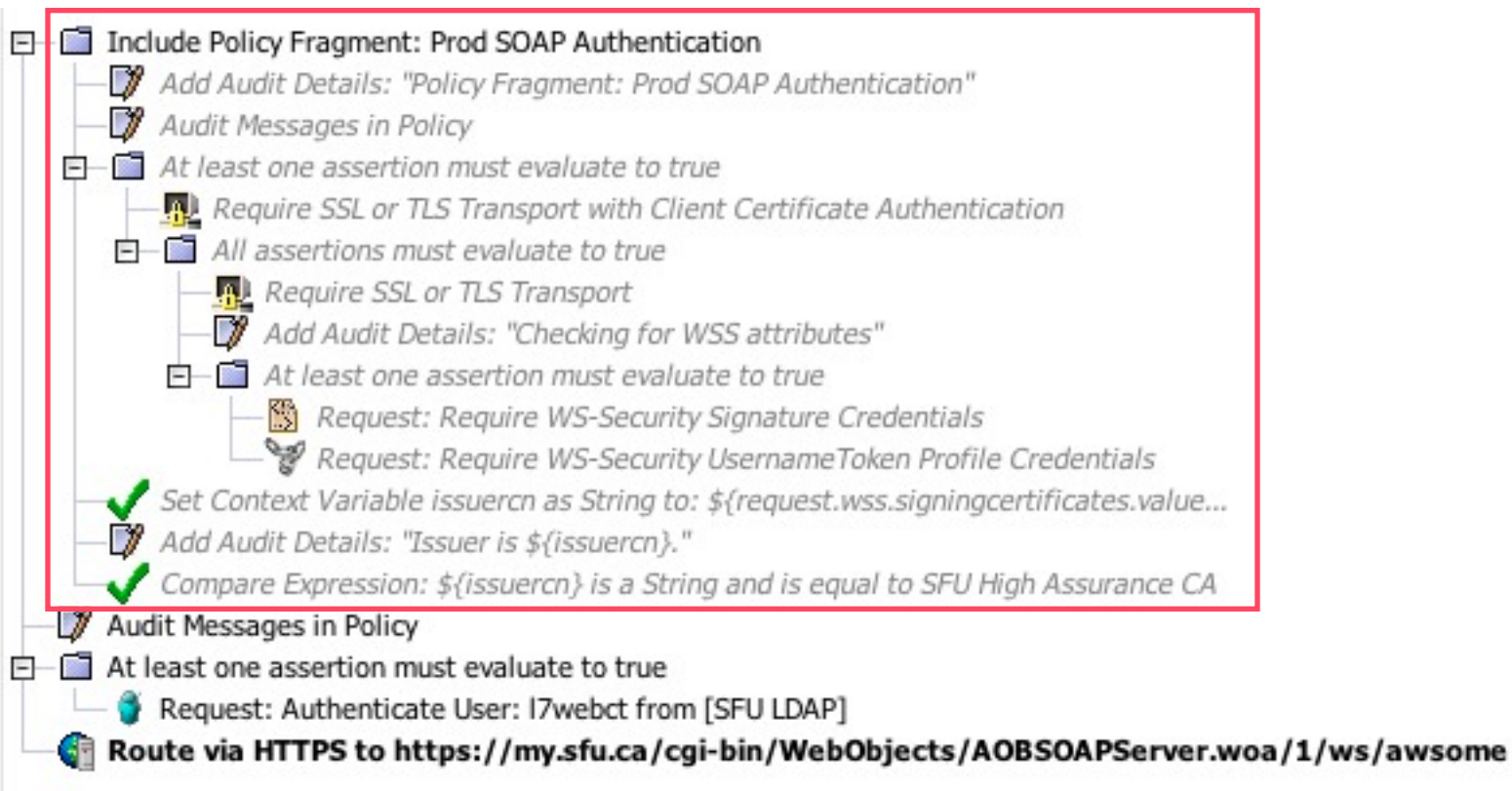
SOAP Security - Best Practices



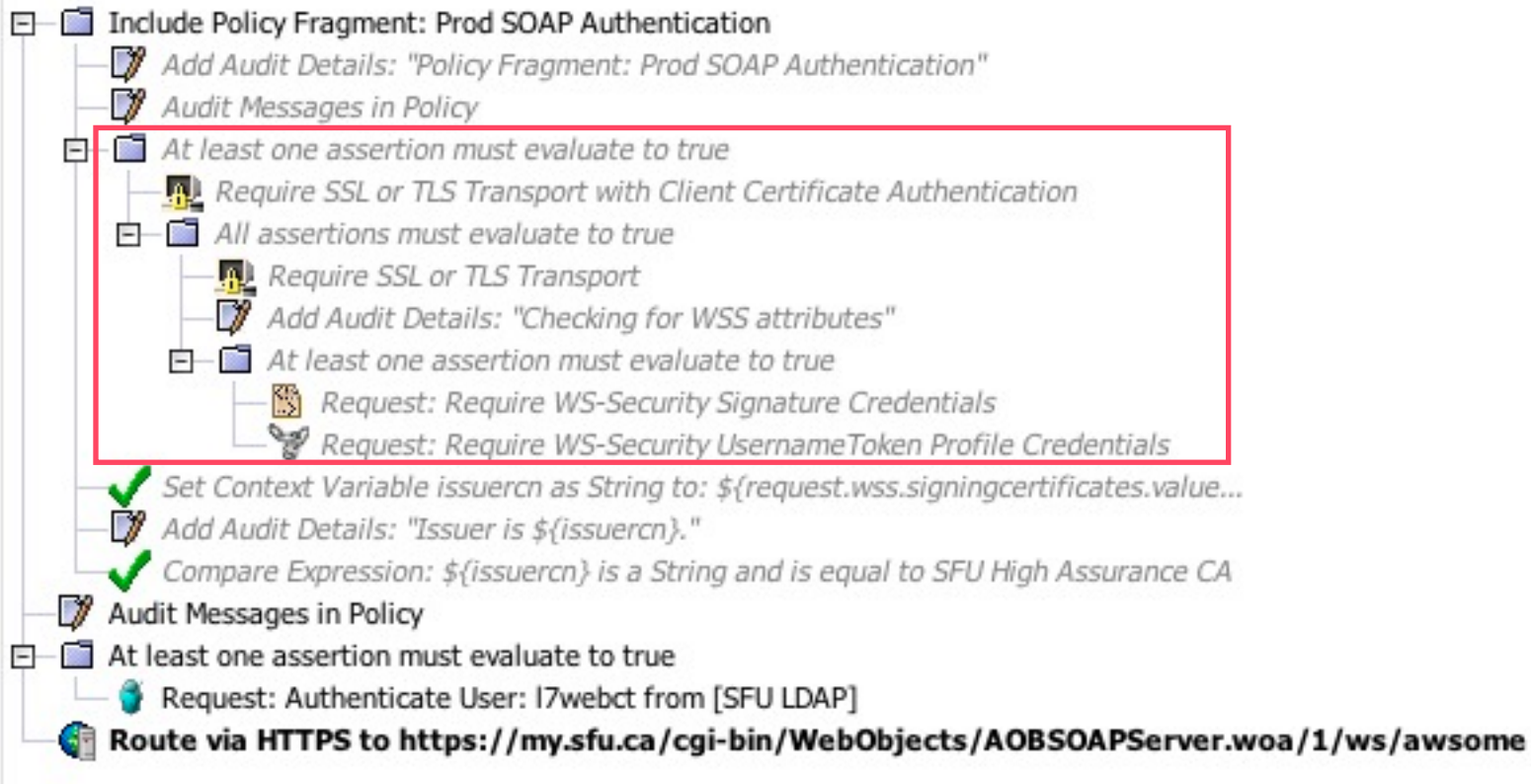
SOAP Security - Best Practices



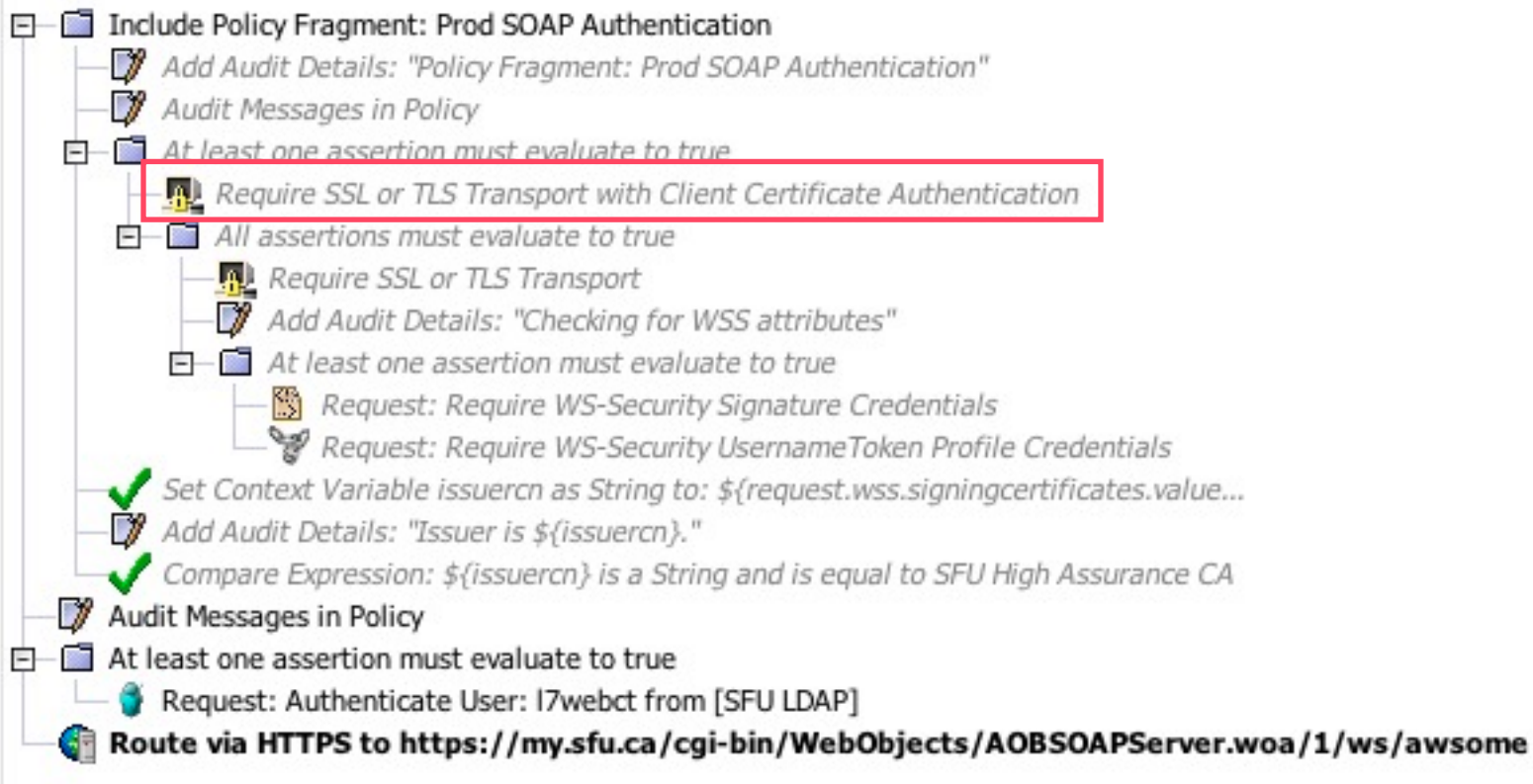
Gateway SOAP Assertions



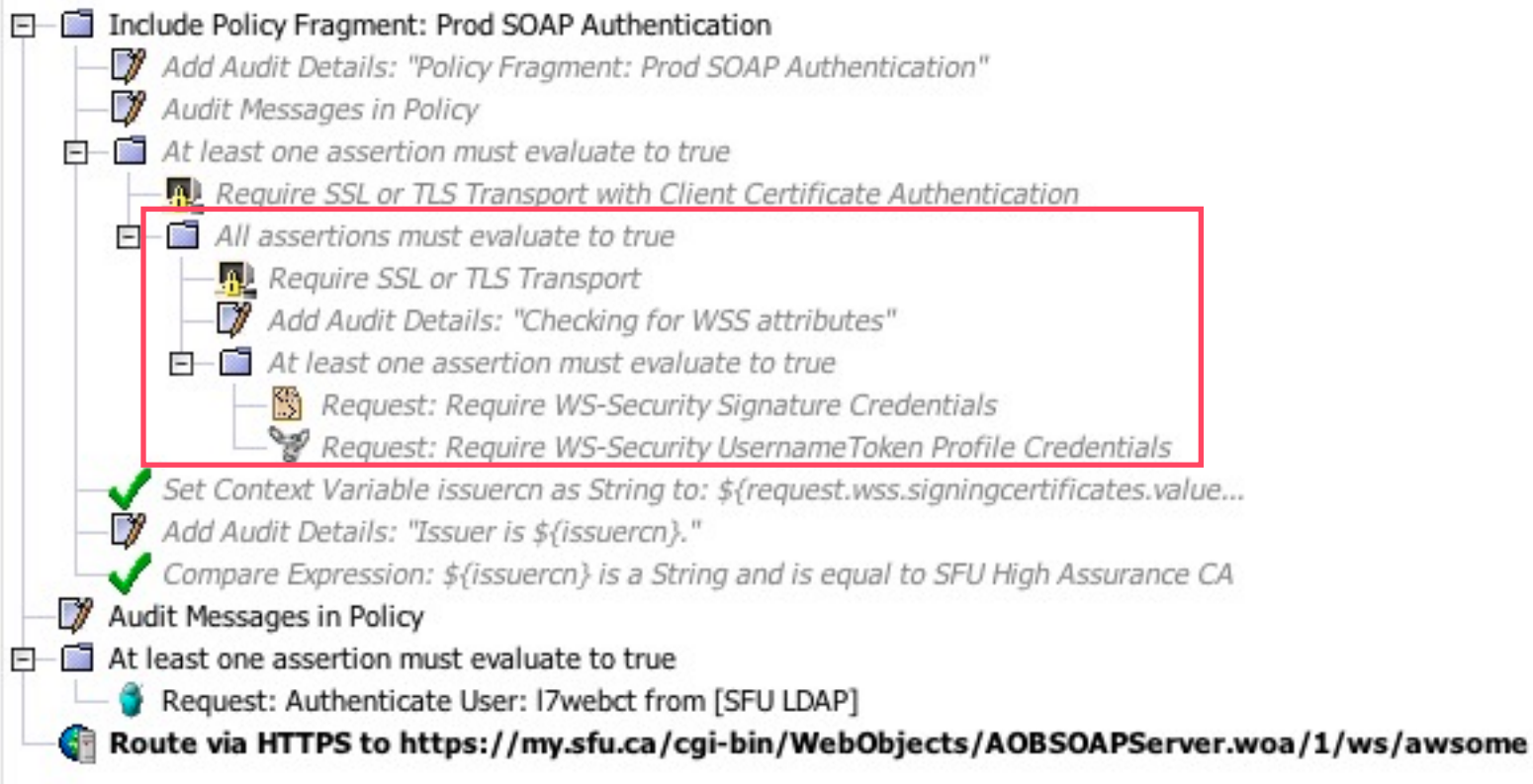
Gateway SOAP Assertions



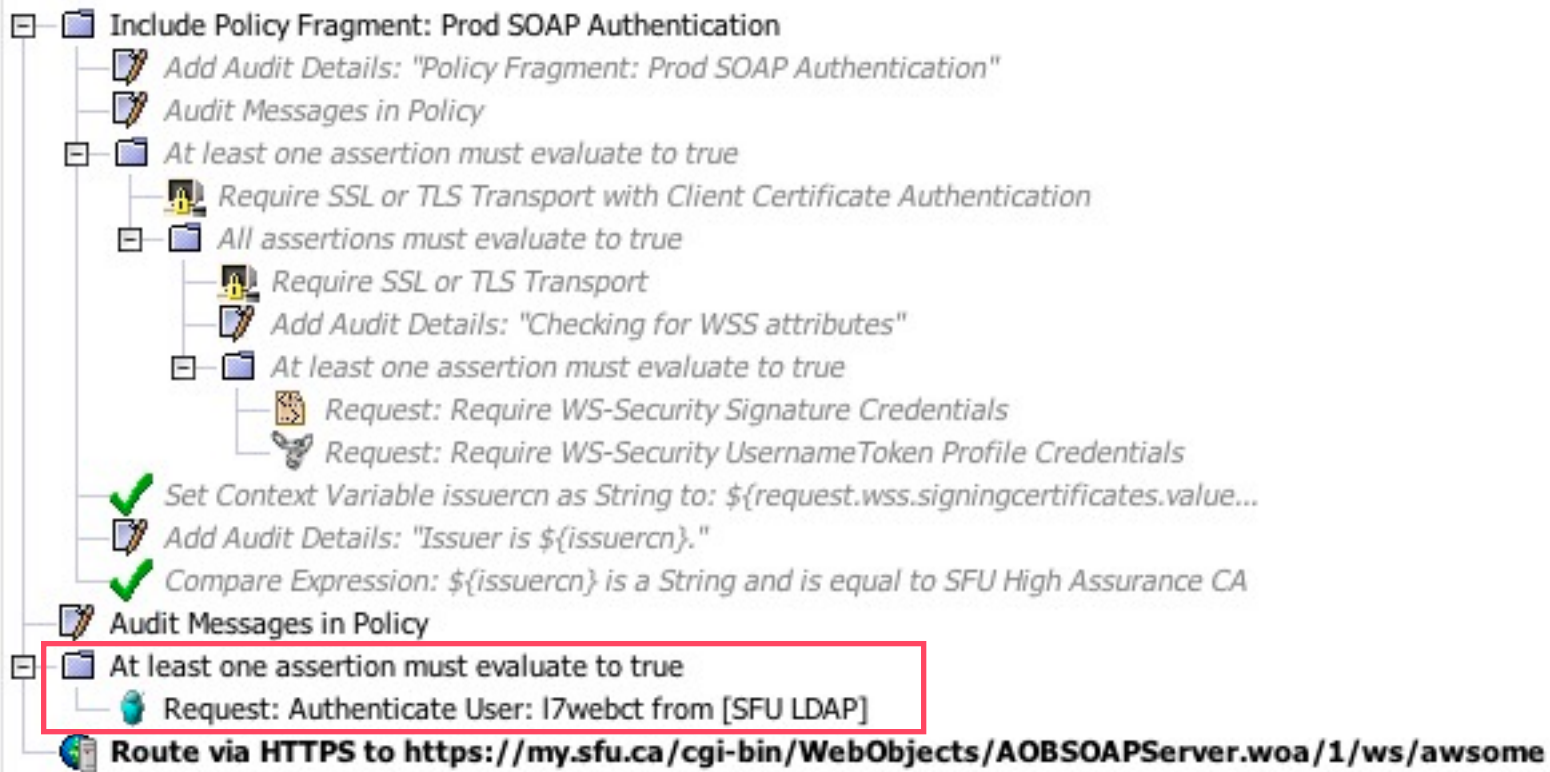
Gateway SOAP Assertions



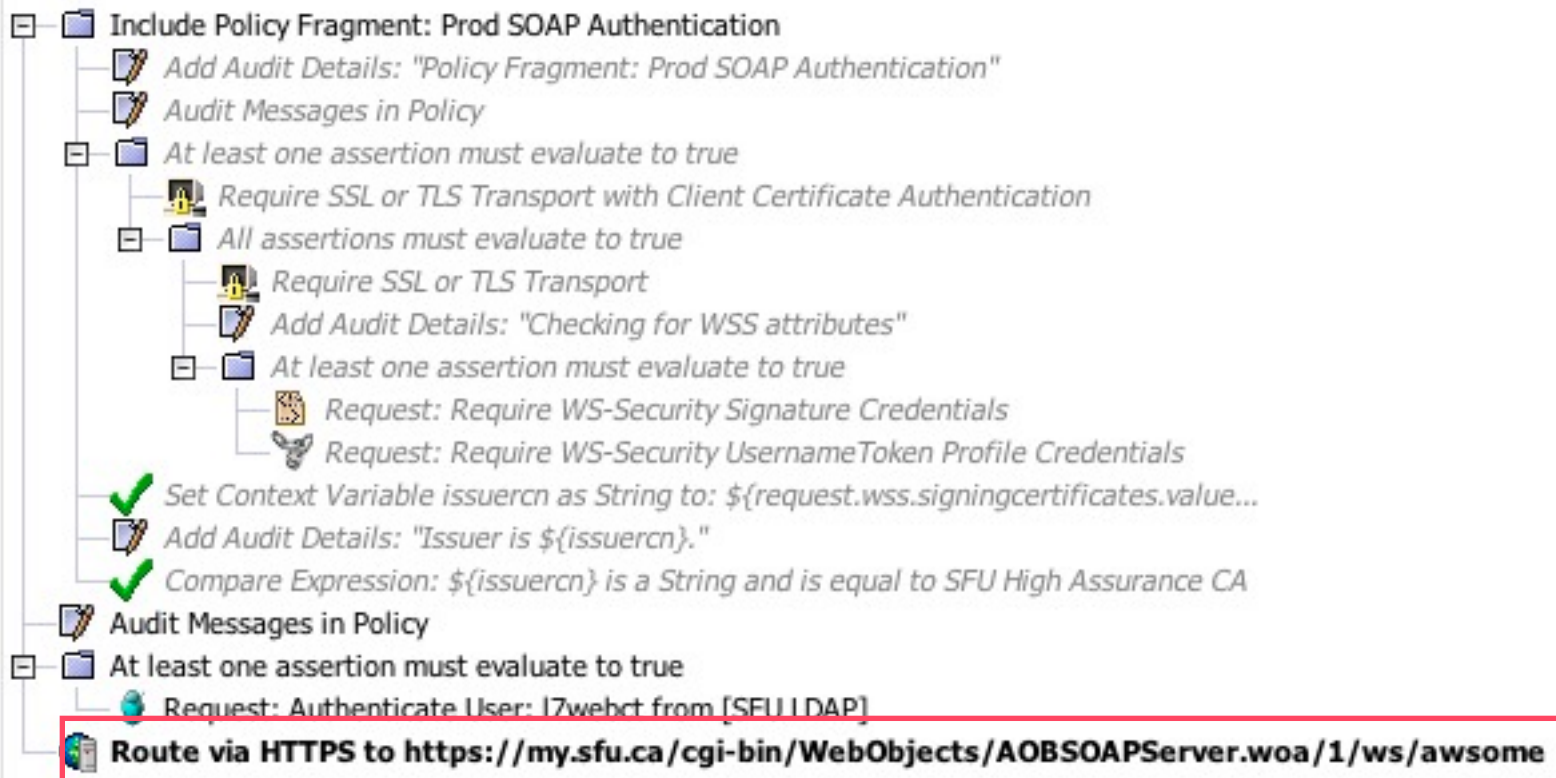
Gateway SOAP Assertions



Gateway SOAP Assertions



Gateway SOAP Assertions



Gateway SOAP Assertions

The Zimbra Conundrum

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011



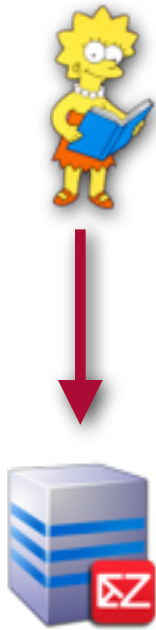
The Zimbra Conundrum

IT Services - Jeremy Rosenberg

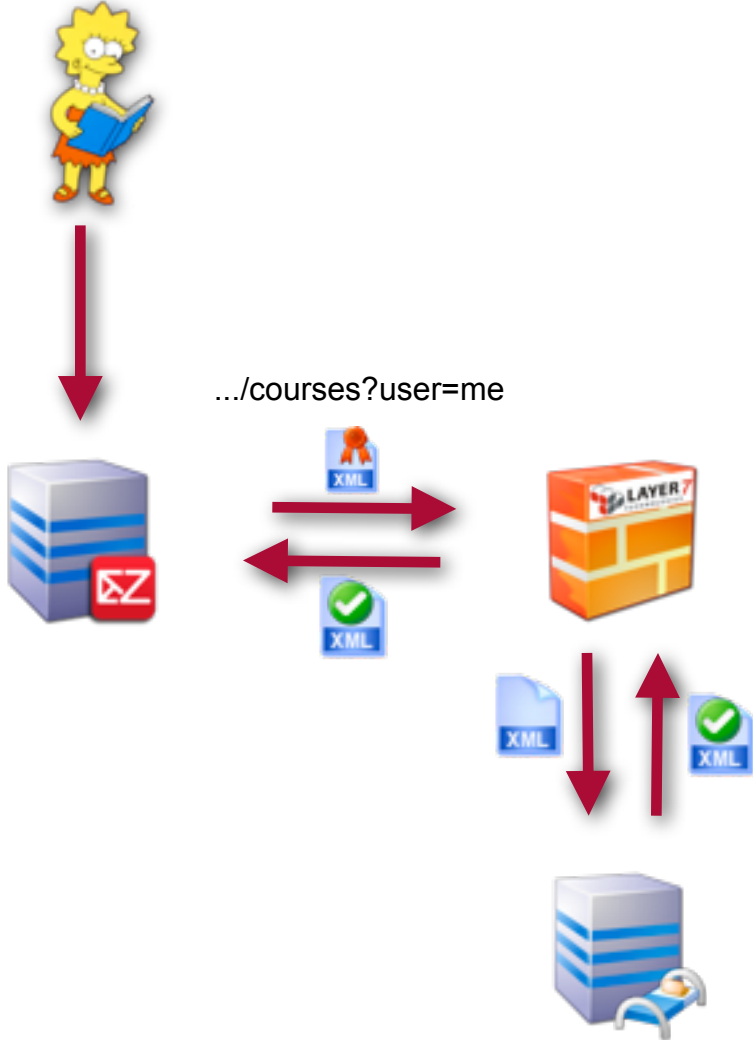


SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

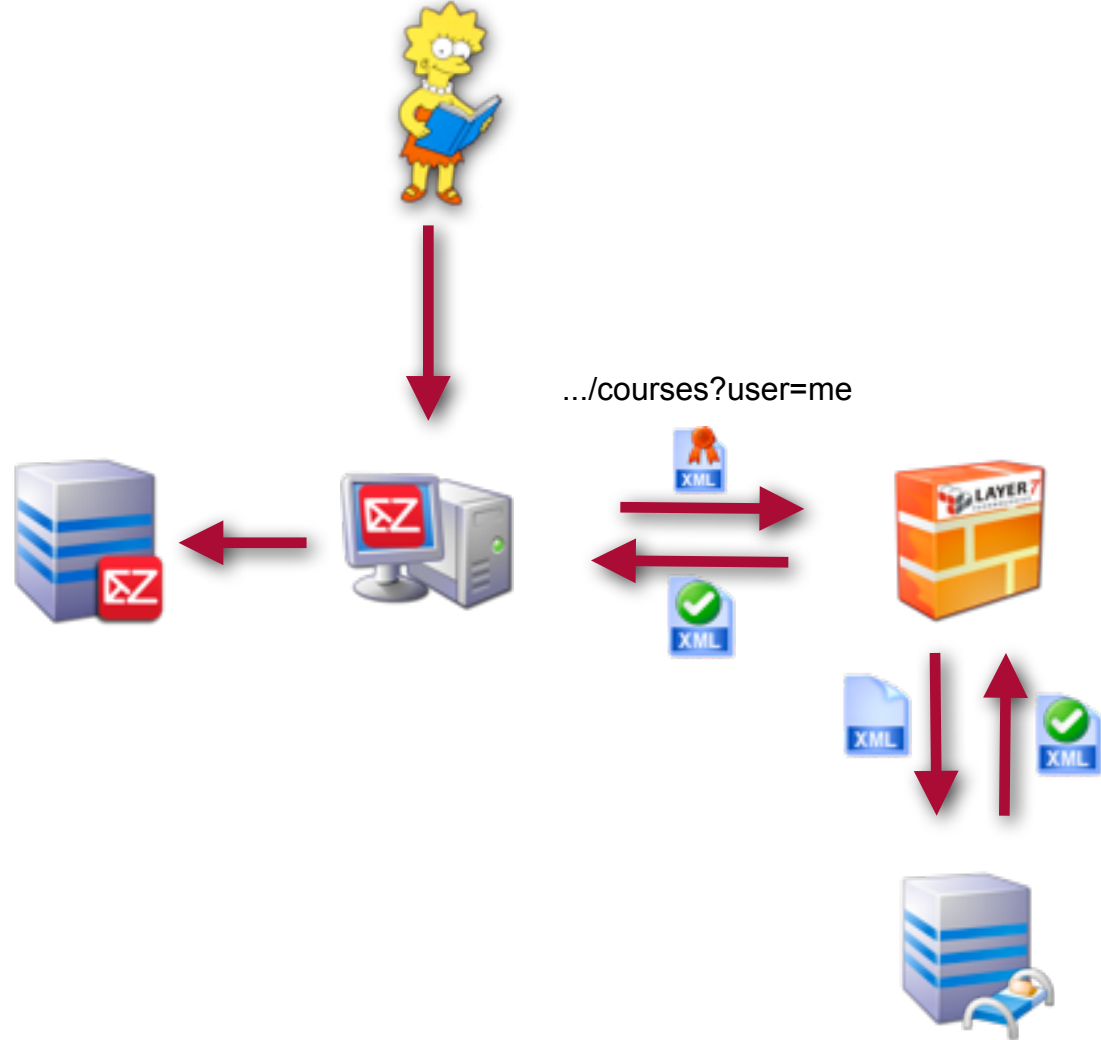
Monday, June 6, 2011



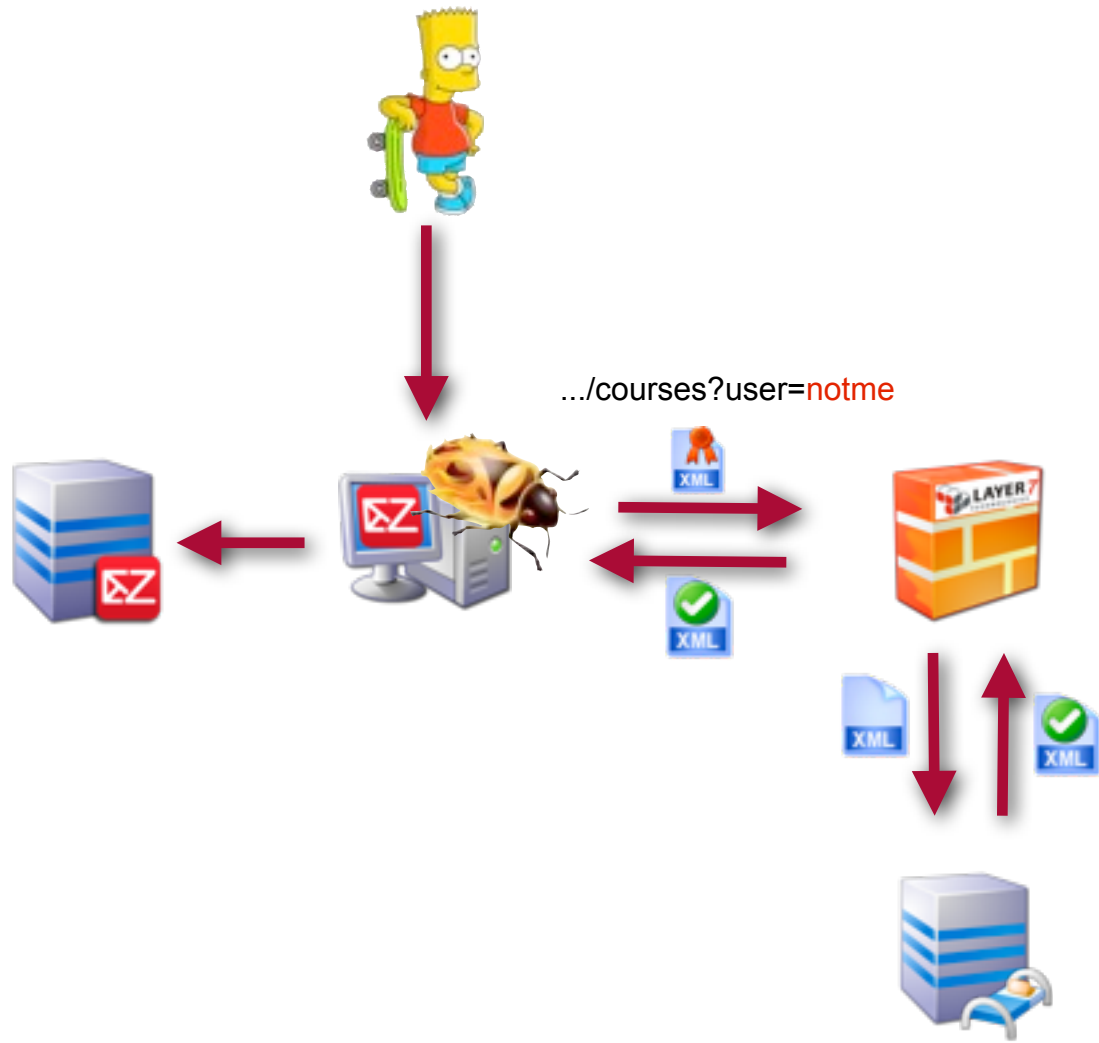
The Zimbra Conundrum



The Zimbra Conundrum



The Zimbra Conundrum



The Zimbra Conundrum



The Zimbra Conundrum

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

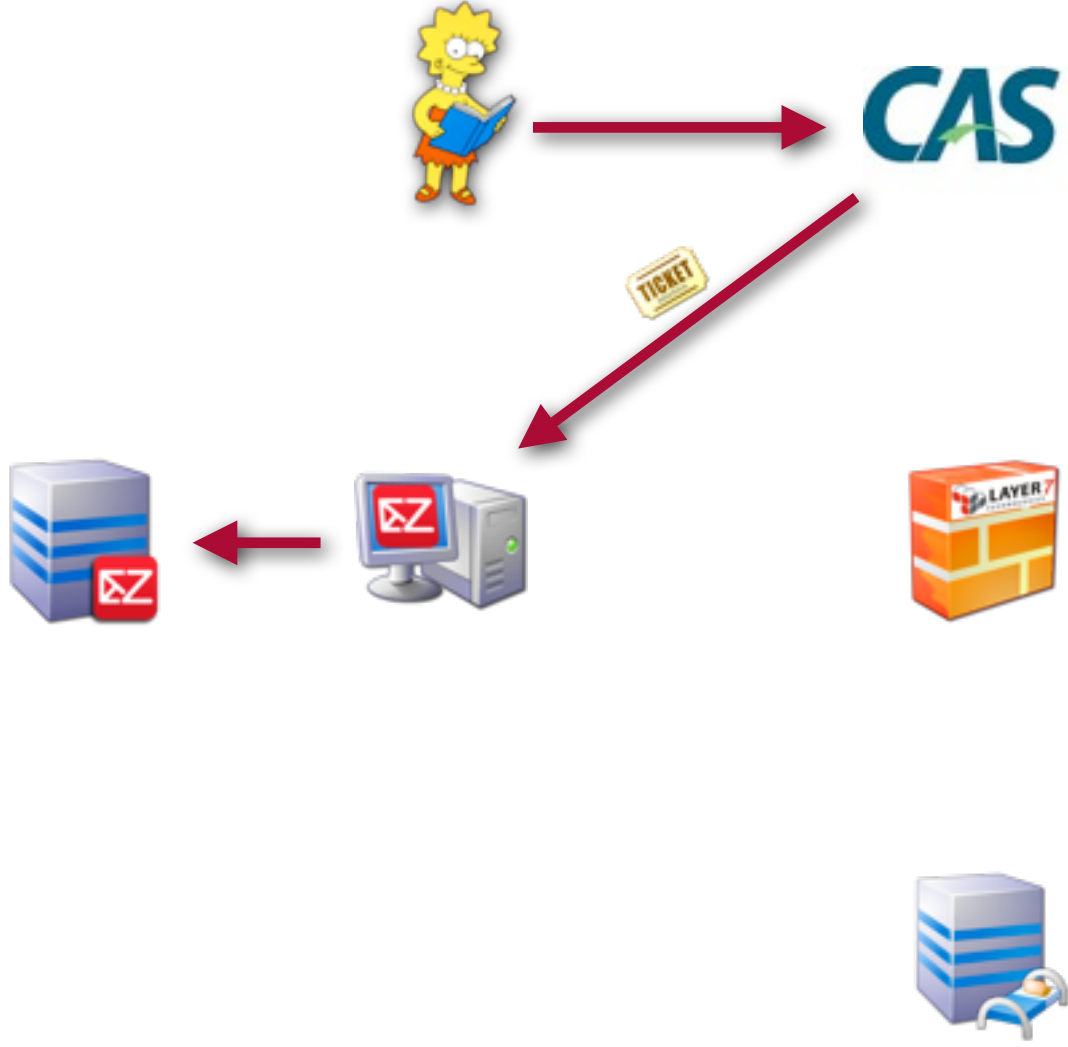
Monday, June 6, 2011



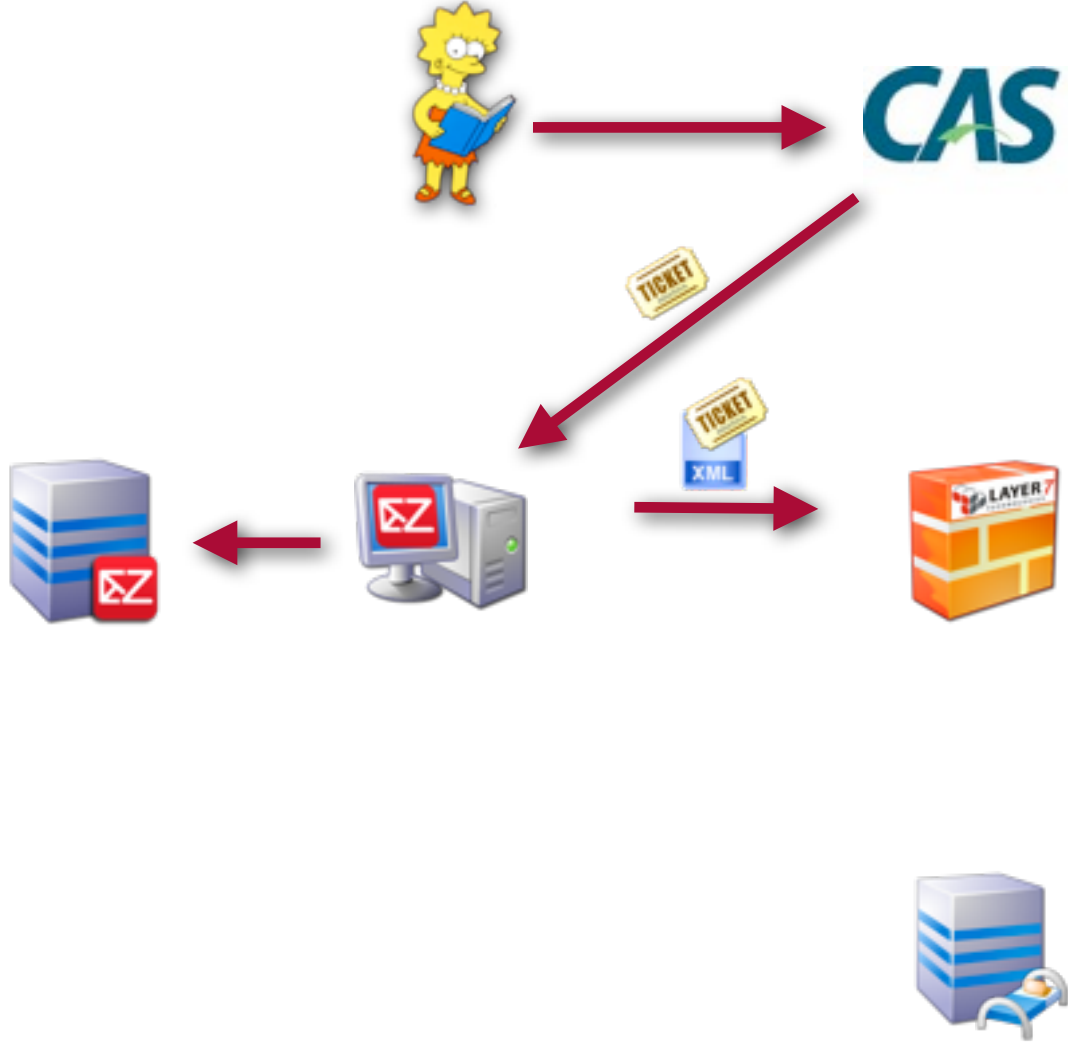
REST Security that Never Rests



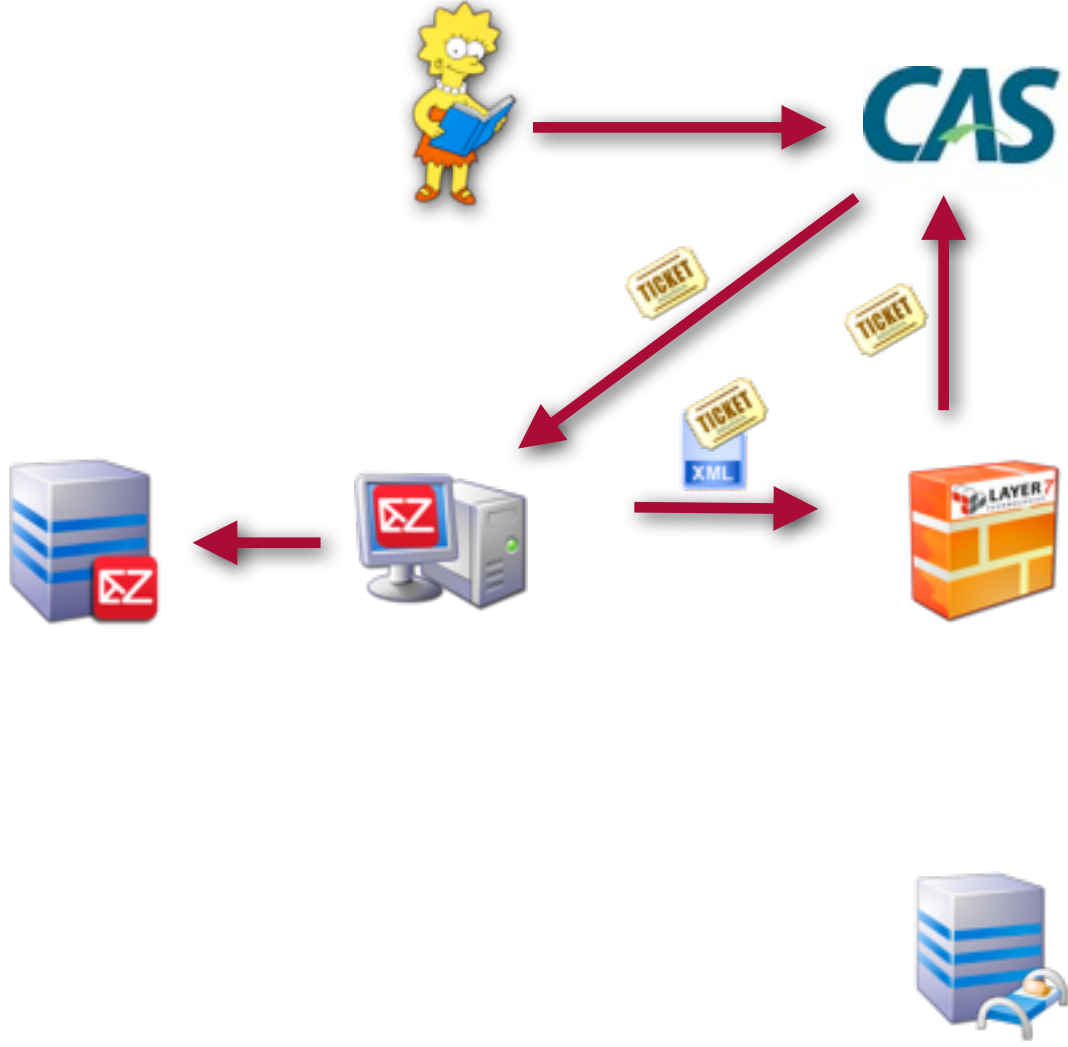
REST Security that Never Rests



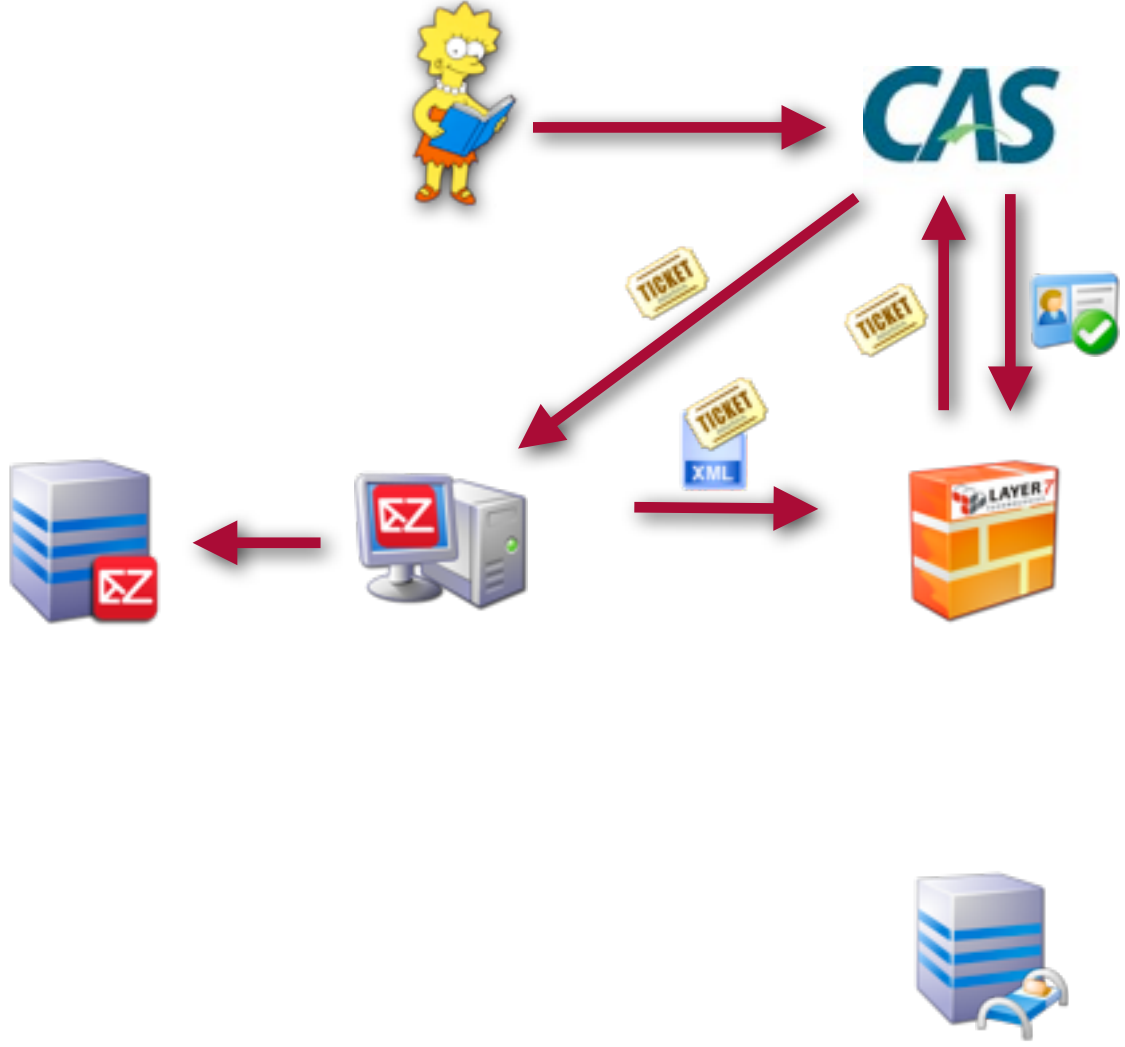
REST Security that Never Rests



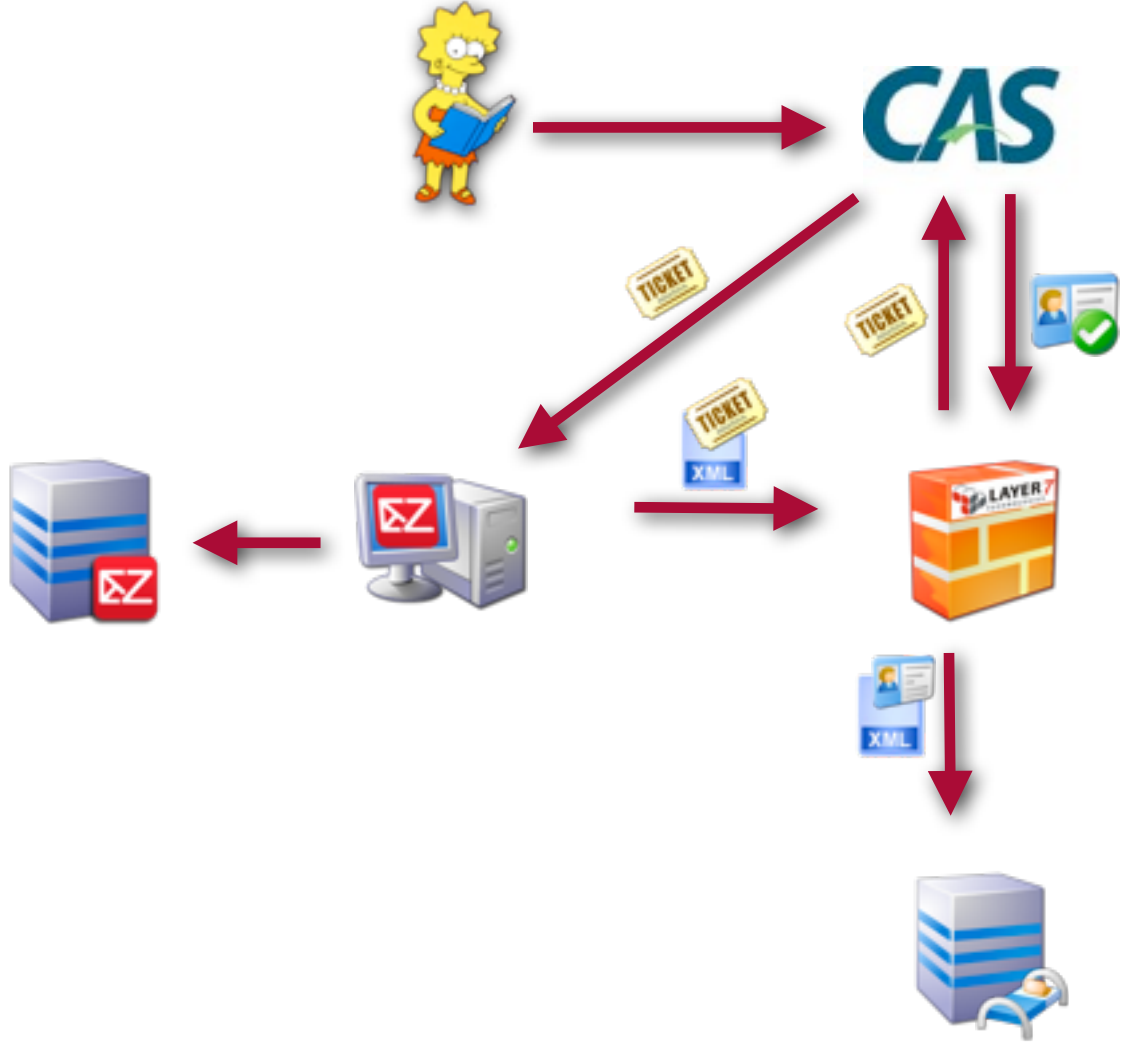
REST Security that Never Rests



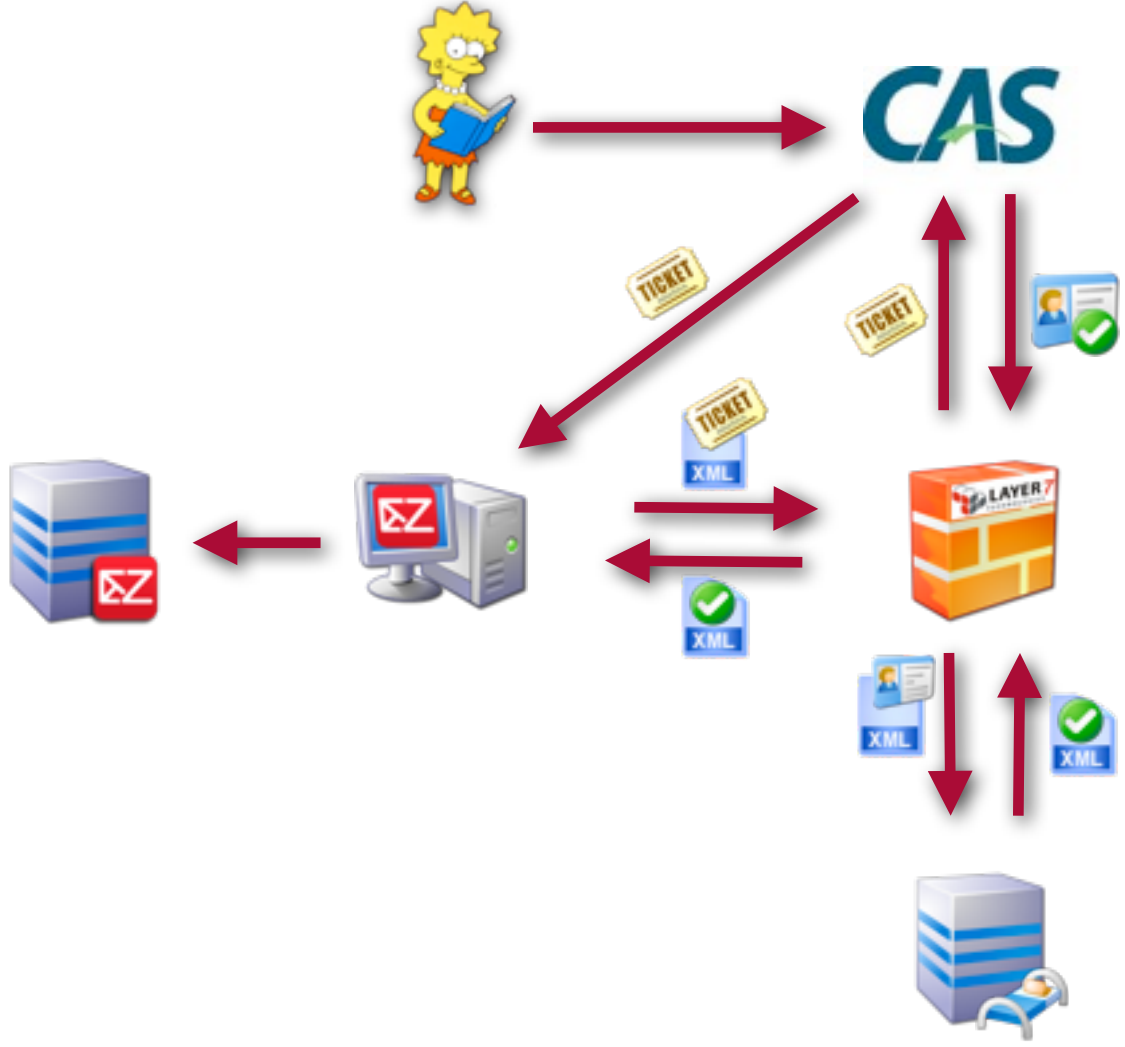
REST Security that Never Rests



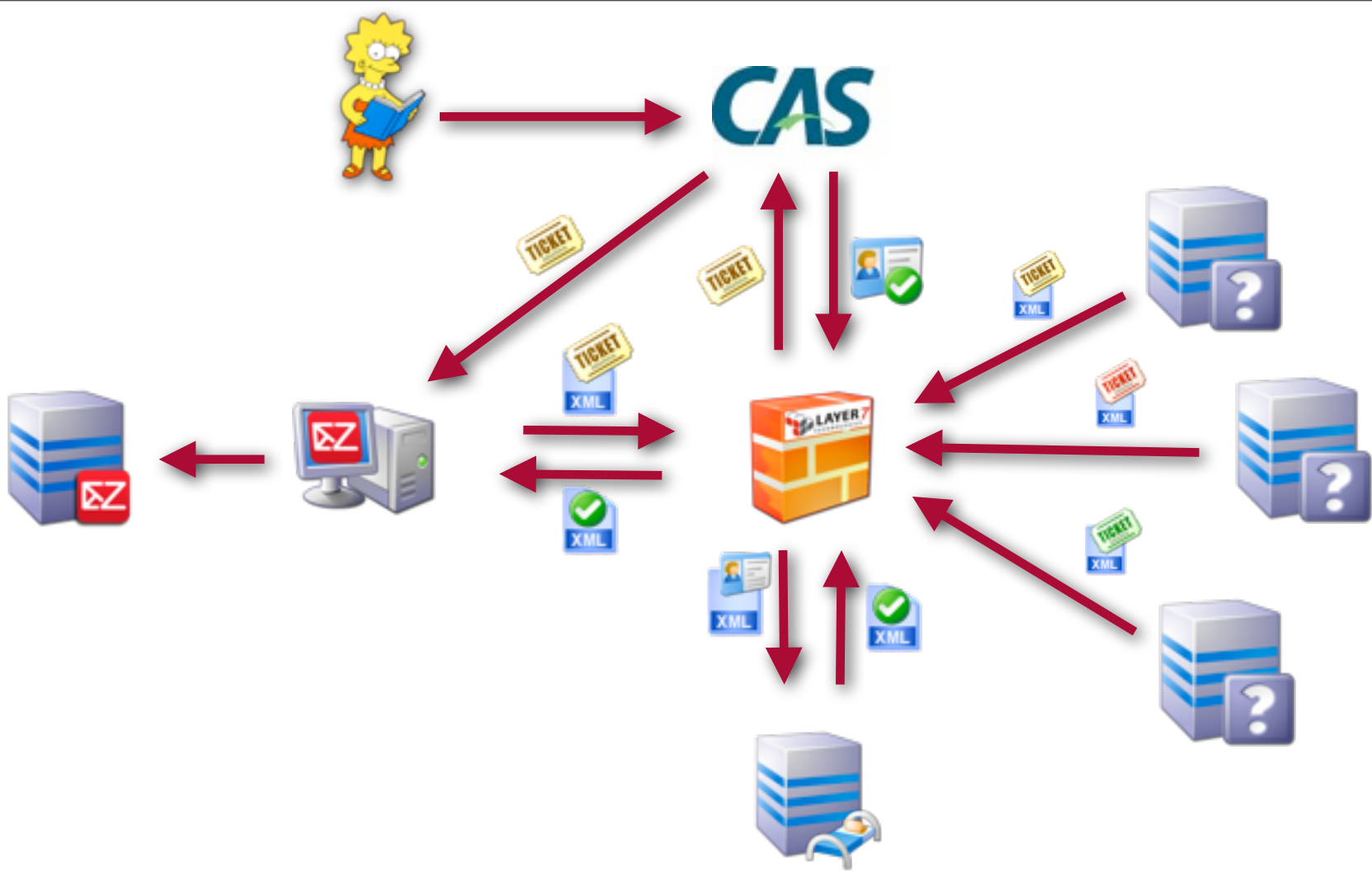
REST Security that Never Rests



REST Security that Never Rests



REST Security that Never Rests

















REST Security that Never Rests

- ✓ Set Context Variable username as String to: `${request.http.parameter.username}`
- 🌐 **Route via HTTPS to [https://cas.sfu.ca/cgi-bin/WebObjects/cas.woa/wa/proxyvalidate?ticket=\\${request.http.parameter.ticket}](https://cas.sfu.ca/cgi-bin/WebObjects/cas.woa/wa/proxyvalidate?ticket=${request.http.parameter.ticket})**
- ✍ Add Audit Details: "Cas Response = `${casResponse.mainpart}`"
- ✓ Set Context Variable casXMLblob as Message to: `<?xml version="1.0" encoding="UTF-8"?>...`
- 🔍 `${casXMLblob}` must match XPath `/cas:serviceResponse/cas:authenticationSuccess/cas:user`
- ✍ Add Audit Details: "casUsername: `${casUsername.result}`"
- ☐ At least one assertion must evaluate to true
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to `${username}`
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to grahamb
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to rosey
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to glee
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to robert
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to ray
- 🌐 **Route via HTTPS to [https://rest.its.sfu.ca/cgi-bin/WebObjects/AOBRestServer.woa/\\${request.url.file}](https://rest.its.sfu.ca/cgi-bin/WebObjects/AOBRestServer.woa/${request.url.file})**

Gateway REST Assertions

- ✓ Set Context Variable username as String to: `${request.http.parameter.username}`
- Route via HTTPS to [https://cas.sfu.ca/cgi-bin/WebObjects/cas.woa/wa/proxyvalidate?ticket=\\${request.http.parameter.ticket}](https://cas.sfu.ca/cgi-bin/WebObjects/cas.woa/wa/proxyvalidate?ticket=${request.http.parameter.ticket})
- ✎ Add Audit Details: "Cas Response = `${casResponse.mainpart}`"
- ✓ Set Context Variable casXMLblob as Message to: `<?xml version="1.0" encoding="UTF-8"?>...`
- ✎ `${casXMLblob}` must match XPath `/cas:serviceResponse/cas:authenticationSuccess/cas:user`
- ✎ Add Audit Details: "casUsername: `${casUsername.result}`"
- ☐ At least one assertion must evaluate to true
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to `${username}`
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to grahamb
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to rosey
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to glee
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to robert
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to ray
- Route via HTTPS to [https://rest.its.sfu.ca/cgi-bin/WebObjects/AOBRestServer.woa/\\${request.url.file}](https://rest.its.sfu.ca/cgi-bin/WebObjects/AOBRestServer.woa/${request.url.file})

Gateway REST Assertions

-  ~~Set Context Variable username as String to: `${request.http.parameter.username}`~~
-  **Route via HTTPS to `https://cas.sfu.ca/cgi-bin/WebObjects/cas.woa/wa/proxyvalidate?ticket=${request.http.parameter.ticket}`**
-  Add Audit Details: "Cas Response = `${casResponse.mainpart}`"
-  Set Context Variable casXMLblob as Message to: `<?xml version="1.0" encoding="UTF-8"?>...`
-  `${casXMLblob}` must match XPath `/cas:serviceResponse/cas:authenticationSuccess/cas:user`
-  Add Audit Details: "casUsername: `${casUsername.result}`"
-  At least one assertion must evaluate to true
 -  Compare Expression: `${casUsername.result}` is a String and is equal to `${username}`
 -  Compare Expression: `${casUsername.result}` is a String and is equal to grahamb
 -  Compare Expression: `${casUsername.result}` is a String and is equal to rosey
 -  Compare Expression: `${casUsername.result}` is a String and is equal to glee
 -  Compare Expression: `${casUsername.result}` is a String and is equal to robert
 -  Compare Expression: `${casUsername.result}` is a String and is equal to ray
-  Route via HTTPS to `https://rest.its.sfu.ca/cgi-bin/WebObjects/AOBRestServer.woa/${request.url.file}`

Gateway REST Assertions

- ✓ Set Context Variable username as String to: `${request.http.parameter.username}`
- 🌐 **Route via HTTPS to [https://cas.sfu.ca/cgi-bin/WebObjects/cas.woa/wa/proxyvalidate?ticket=\\${request.http.parameter.ticket}](https://cas.sfu.ca/cgi-bin/WebObjects/cas.woa/wa/proxyvalidate?ticket=${request.http.parameter.ticket})**
- ✍ Add Audit Details: "Cas Response = `${casResponse.mainpart}`"
- ✓ **Set Context Variable casXMLblob as Message to: `<?xml version="1.0" encoding="UTF-8"?>...`**
- 🔗 ~~`${casXMLblob}` must match XPath `/cas:serviceResponse/cas:authenticationSuccess/cas:user`~~
- ✍ Add Audit Details: "casUsername: `${casUsername.result}`"
- ☐ At least one assertion must evaluate to true
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to `${username}`
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to grahamb
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to rosey
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to glee
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to robert
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to ray
- 🌐 **Route via HTTPS to [https://rest.its.sfu.ca/cgi-bin/WebObjects/AOBRestServer.woa/\\${request.url.file}](https://rest.its.sfu.ca/cgi-bin/WebObjects/AOBRestServer.woa/${request.url.file})**

Gateway REST Assertions

- ✓ Set Context Variable username as String to: `${request.http.parameter.username}`
- 🌐 **Route via HTTPS to [https://cas.sfu.ca/cgi-bin/WebObjects/cas.woa/wa/proxyvalidate?ticket=\\${request.http.parameter.ticket}](https://cas.sfu.ca/cgi-bin/WebObjects/cas.woa/wa/proxyvalidate?ticket=${request.http.parameter.ticket})**
- ✍ Add Audit Details: "Cas Response = `${casResponse.mainpart}`"
- ✓ Set Context Variable casXML blob as Message to: `<?xml version="1.0" encoding="UTF-8"?>...`
- 📄 **`${casXMLblob}` must match XPath `/cas:serviceResponse/cas:authenticationSuccess/cas:user`**
- ✍ Add Audit Details: "casUsername: `${casUsername.result}`"
- ☐ At least one assertion must evaluate to true
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to `${username}`
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to grahamb
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to rosey
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to glee
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to robert
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to ray
- 🌐 **Route via HTTPS to [https://rest.its.sfu.ca/cgi-bin/WebObjects/AOBRestServer.woa/\\${request.url.file}](https://rest.its.sfu.ca/cgi-bin/WebObjects/AOBRestServer.woa/${request.url.file})**

Gateway REST Assertions

- ✓ Set Context Variable username as String to: `${request.http.parameter.username}`
- 🌐 **Route via HTTPS to [https://cas.sfu.ca/cgi-bin/WebObjects/cas.woa/wa/proxyvalidate?ticket=\\${request.http.parameter.ticket}](https://cas.sfu.ca/cgi-bin/WebObjects/cas.woa/wa/proxyvalidate?ticket=${request.http.parameter.ticket})**
- ✍ Add Audit Details: "Cas Response = `${casResponse.mainpart}`"
- ✓ Set Context Variable casXMLblob as Message to: `<?xml version="1.0" encoding="UTF-8"?>...`
- 🔍 `${casXMLblob}` must match XPath `/cas:serviceResponse/cas:authenticationSuccess/cas:user`
- ✍ Add Audit Details: "casUsername: `${casUsername.result}`"
- ☐ At least one assertion must evaluate to true
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to `${username}`
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to grahamb
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to rosey
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to glee
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to robert
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to ray
- 🌐 **Route via HTTPS to [https://rest.its.sfu.ca/cgi-bin/WebObjects/AOBRestServer.woa/\\${request.url.file}](https://rest.its.sfu.ca/cgi-bin/WebObjects/AOBRestServer.woa/${request.url.file})**

Gateway REST Assertions

- ✓ Set Context Variable username as String to: `${request.http.parameter.username}`
- 🌐 **Route via HTTPS to `https://cas.sfu.ca/cgi-bin/WebObjects/cas.woa/wa/proxyvalidate?ticket=${request.http.parameter.ticket}`**
- 📄 Add Audit Details: "Cas Response = `${casResponse.mainpart}`"
- ✓ Set Context Variable casXMLblob as Message to: `<?xml version="1.0" encoding="UTF-8"?>...`
- 🔍 `${casXMLblob}` must match XPath `/cas:serviceResponse/cas:authenticationSuccess/cas:user`
- 📄 Add Audit Details: "casUsername: `${casUsername.result}`"
- ☐ At least one assertion must evaluate to true
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to `${username}`
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to grahamb
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to rosey
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to glee
 - ✓ Compare Expression: `${casUsername.result}` is a String and is equal to robert
 - ~~✓ Compare Expression: `${casUsername.result}` is a String and is equal to ray~~
- 🌐 **Route via HTTPS to `https://rest.its.sfu.ca/cgi-bin/WebObjects/AOBRestServer.woa/${request.url.file}`**

Gateway REST Assertions



Next Steps

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011

- LDAP groups for developers (done)



Next Steps

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

- LDAP groups for developers (done)
- Upgrade CAS (Currently 3.3.2)



Next Steps

- LDAP groups for developers (done)
- Upgrade CAS (Currently 3.3.2)
- Use SAML tokens



Next Steps

- LDAP groups for developers (done)
- Upgrade CAS (Currently 3.3.2)
- Use SAML tokens
- Integrate with new CMS



Next Steps

- LDAP groups for developers (done)
- Upgrade CAS (Currently 3.3.2)
- Use SAML tokens
- Integrate with new CMS
- PKI?



Next Steps



Lessons Learned

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011

- Security is an enabler



Lessons Learned

- Security is an enabler
- Stick to standards where possible



Lessons Learned

- Security is an enabler
- Stick to standards where possible
- Start small



Lessons Learned

- Security is an enabler
- Stick to standards where possible
- Start small
 - Control the service and consumer



Lessons Learned

Thank You

rosenberg@sfu.ca

(I'll put you in touch with Ray)



THANK YOU

IT Services - Jeremy Rosenberg



SIMON FRASER UNIVERSITY
THINKING OF THE WORLD

Monday, June 6, 2011