JavaCro'15

Secure WebServices

WSDL first approach with Apache CXF

Askar Akhmerov
askar.akhmerov@smava.de

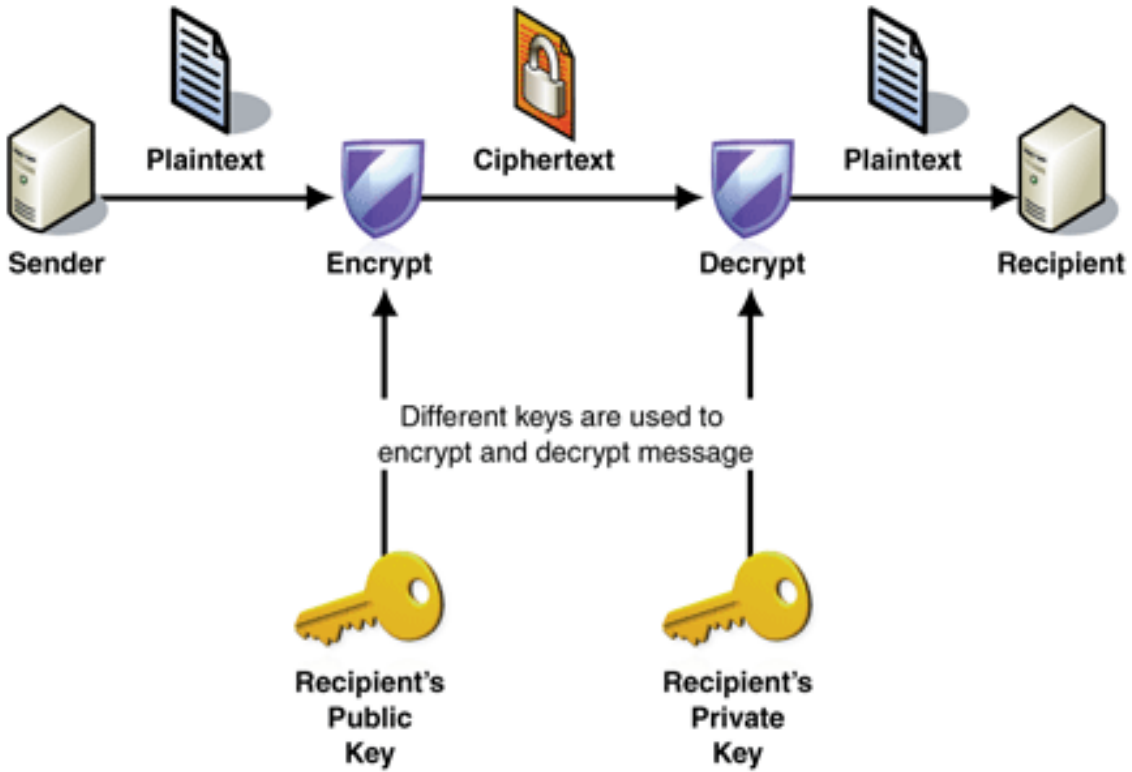
Agenda

- Use case
- SSL basics
- JAX-WS Service
- Keystores
- WS-Security
- CXF Interceptors
- WSS4J Interceptors

Agenda

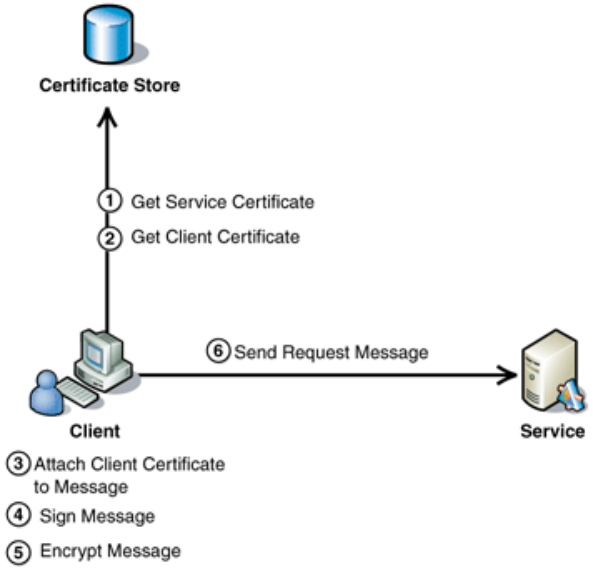
- encryptionKeyIdentifier
- Encryption Algorithms
- Write Policy
- Demo
- References
- Questions

Use case

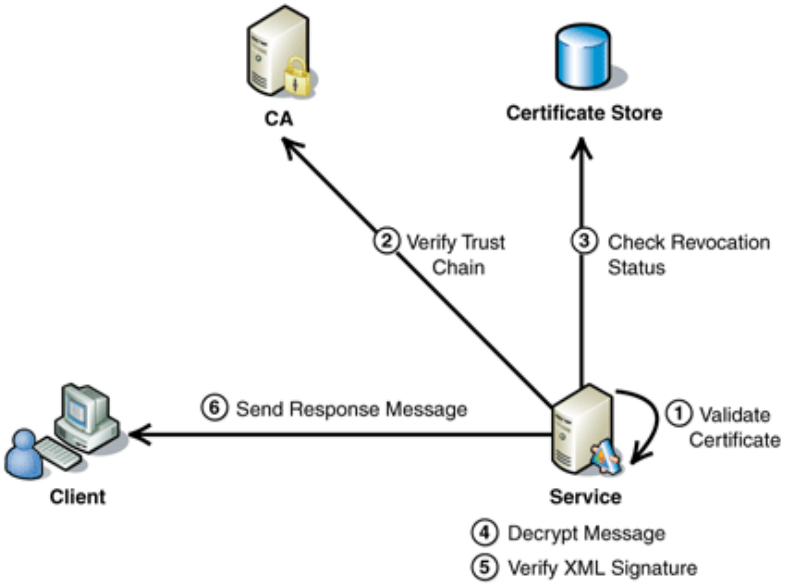

Plaintext
Ciphertext
Plaintext
Sender
Encrypt
Decrypt
Recipient
Different keys are used to
encrypt and decrypt message
Recipient's
Public
Key
Recipient's
Private
Key

Use case

client



service



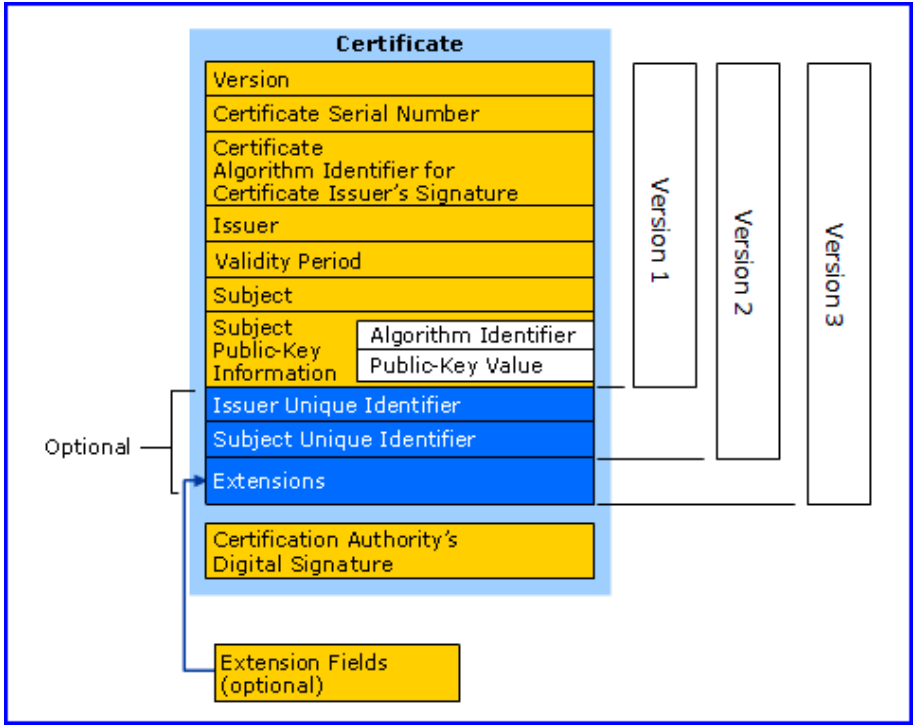
JavaCro'15

SSL basics

- use X.509 certificates and hence asymmetric cryptography
- encrypt the data of network connections in the application layer
- used web\browsers\mail\software

X.509

- Issuer - certification authority (CA)
- Authorization and issuing chains



JAX-WS Service

- prepare xsd
- write wsdl
- generate classes
- write cxf config
- generate client

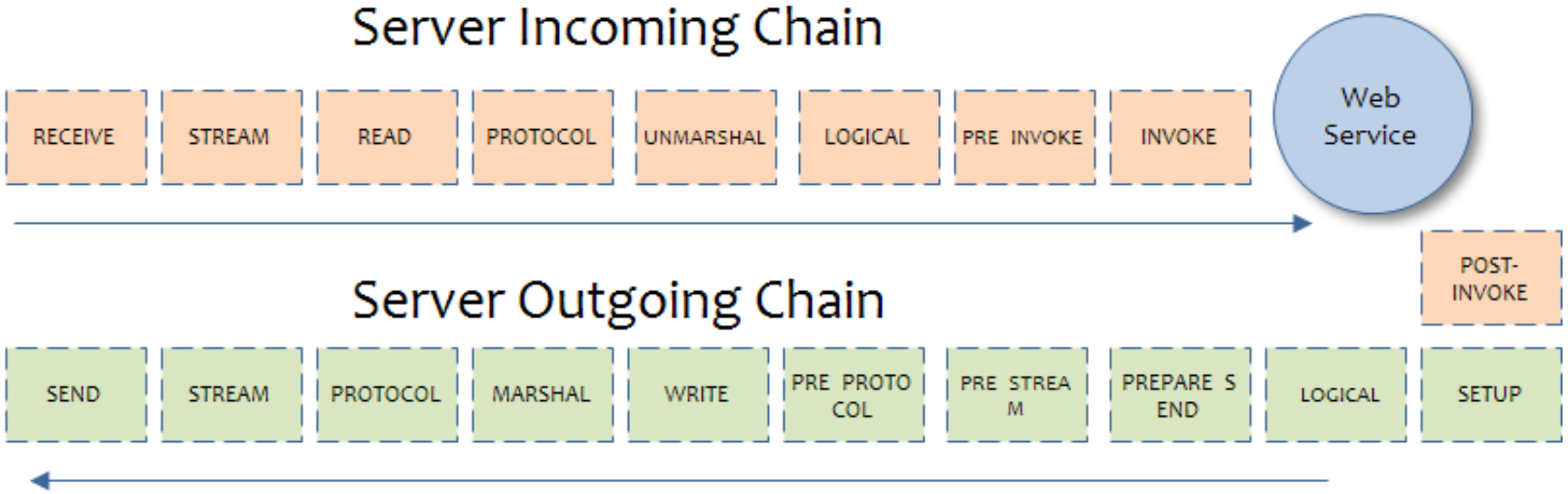
Keystores Manipulations

- generate private keys
- export keys
- import keys
- maven usage

WS-Security

- Based on policies
  - requires wsdl adjustments
- Based on interceptors
  - preserves wsdl
  - customizations done through code
  - customizations done through spring context

CXF Interceptors



WSS4J Interceptors

JavaCro'15

- Password Callback Class
- WSS4JOutInterceptor (Phase.PRE_PROTOCOL)
  - action
  - signaturePropFile
  - signatureParts
  - encryptionPropFile
- WSS4JInInterceptor (Phase.PRE_PROTOCOL)
  - action
  - signaturePropFile
  - signatureParts
  - decryptionPropFile

Encryption Key Identifiers

- IssuerSerial (default)
- DirectReference
- X509KeyIdentifier
- Thumbprint
- SKIKeyIdentifier
- KeyValue (signature only)
- EncryptedKeySHA1 (encryption only)

Encryption Algorithms

- http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html#sec-Algorithms
- Based on JCE
- http://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html

Write Policy

- WS-Policy Declaration

```
<wsp:Policy wsu:Id="UniqueIdentifier">
   <wsp:ExactlyOne>
      ...
   </wsp:ExactlyOne>
</wsp:Policy>
```

- Policy reference

```
<wsp:PolicyReference URI="#UniqueIdentifier"/>
```

Demo

https://github.com/Smava/wssecurity

References

http://cxf.apache.org/docs/ws-security.html
http://www.javaworld.com/article/2073287/soa/secure-web-services.html
http://en.wikipedia.org/wiki/Secure_Sockets_Layer#Applications_and_adoption
http://en.wikipedia.org/wiki/X.509
http://msdn.microsoft.com/en-us/library/ff647097.aspx
http://www.ibm.com/developerworks/opensource/library/j-jws18/index.html
http://www.ibm.com/developerworks/opensource/library/j-jws13/index.html
http://www.ibm.com/developerworks/java/library/j-jws14/index.html
http://concentricsky.com/blog/2012/dec/implementing-ws-security-cxf-wsdl-first-web-service
http://www.benoitschweblin.com/2013/03/run-jetty-in-maven-life-cycle.html
http://mojo.codehaus.org/keytool/keytool-maven-plugin/usage.html
http://coheigea.blogspot.de/2013/03/signature-and-encryption-key.html
http://specs.xmlsoap.org/ws/2005/07/securitypolicy/ws-securitypolicy.pdf
http://www.masterthebоss.com/jboss-web-services/apache-cxf-interceptors

Summary

- Use case
- SSL basics
  - X.509
- JAX-WS Service
- Keystores
- WS-Security
- CXF Interceptors
- WSS4J Interceptors

Summary

- encryptionKeyIdentifier
- Encryption Algorithms
- Write Policy
- Demo
- References
- Questions

JavaCro'15

Questions?