

FIRMS WS-Security Implementation

Introduction

WS Security is implemented in FIRMS by using WSS4J and custom handlers developed by the OMII. Security is implemented on both the client and the server side. Every message generated at the client and server are passed through the chain of security handlers and authenticated by a set of security handlers within the handler chain in the request flow of the web services.

Client Side Implementation

Client side security is implemented by the WSOutboundHandler. This handler reads from crypto.properties file, PWSecurityCallback class and other information. This information is provided in the "FIRMS-conf" folder in the class path at the client side.

User has to change the omii.ks file location to OMIIClient installed directory in the crypto.properties file.

Server Side Implementation

Server side security is implemented by a set of handlers in the request and response flow of the SOAP Messages. Deployment descriptors for FIRMS web services have the information required to implement WS Security.

SOAP Message security header is validated by the set of handlers in the request flow. The snippet below depicts the SOAP Message with WS Security of the created WSRM SOAP Message.

```
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"><soapenv:Header>
<wsse:Security soapenv:mustUnderstand="1"
xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-
secext-1.0.xsd"><wsse:BinarySecurityToken
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
wsu:Id="CertId-3875628" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-
1.0.xsd">MIIDJjCCAg6gAwIBAgICFAAwDQYJKoZIhvcNAQEEBQAwwYIixLTArBgNVBAMTJE
9NSUkgVGVTcG9yYXJ5J5IENlcnRzZmljYXRlIEF1dGhvcml0eTESMBAGA1UECBMJSGFtcHNNoa
XJlMQswCQYDVQQGEwJVSzEhMB8GCSqGSIb3DQEJARYSc3VwcG9ydEBvbWlpLmFjLnVrMQ0w
CwYDVQQKEwRPTULJMB4XDTA2MDEwNTE5Mzg0N1oXDTA2MDIwNDE5Mzg0N1owgZ0xHjAcBgN
VBAMTFWxvY2FsaG9zdC5sb2NhbGRvbWVpbnEjEQMA4GA1UECBMHSW5kaWFuYTEMMAoGA1UEBh
MDVVBmSEwHwYJKoZIhvcNAQkBFhJkeWVtbWVAAaW5kaWFuYS5lZHUxGzAZBgNVBAoTEkluz
GhIhbmEgVW5pdmVyc2l0eTEbMBkGA1UECmMSSW5kaWFuYS5lZHUxGzAZBgNVBAMTJE9NSUkg
SIb3DQEBAQUAA4GNADCBiQKBgQCnPg77zY0Cn8n6zKzWRAZVbOhulbvsoBhrdaxlryxwMVI
ttpCWuU0HyWsOwUbtUhsKcaqDmYCvsv+a8s9lq1Y3x8T8yDWNT7vhOtUQUleKpDe9YoN390
ijite/G8YwJNvQXBajEhb56TqQeGK/POQzFImTtE/0g5Q/x8SBisNSSQIDAQABow0wCzAJB
gNVHRMEAjaAMA0GCSqGSIb3DQEBAQUAA4IBAQA69jW8XVmIWMTHP5/hW7XaZgd/mrElQrnc
OURuCuB0z8zh/PuBVgXW2CIkHP/xkWMbpYfGMBUESsXxe+q39Qb9KnKuc4NutkTl
A/xwU4PqjxhUiKx8zfiLhTvYcld7nCKzd487CuKol2bMRUgJ4wEy2HJwddvuJXNG/PUR7EY
```

```

qbMGXwh8yLs4I1WhvkdGGp/y+UqYjL5aKJnVy/19SUCUFNlCfXGu1/pdM61G5KIzREs5cx/
p4AAIQrOxsLLRsAs/MGYyV/jgJKGxd1hkiKFiXgxycfnbwjicoBcDqZdGYmF0mmU9w5MAYZ
UJ6cLrByjkKQ2KkJqoTlyBzekl/20xC</wsse:BinarySecurityToken><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="#id-9449509">
<ds:Transforms>
<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>I9TnvZIf+c5yrb4QotJbTzYR+6U=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
XlUDo7xyLDLdkt2L9a7rXhoP6gAlFcUmictK3eRkKvhafwXyw+0I0bq+0aLoNqP21PrEsX8
OG5Cumd2AbsC3HS+KMW3vuoadZEhNMZg+byME9tfx4N2/+ehLci0YyiQP+bt0e3S9Q9arEg
6wQWmaguXrpebgD9irBuZNPmbl4Tg=
</ds:SignatureValue>
<ds:KeyInfo Id="KeyId-18997034">
<wsse:SecurityTokenReference wsu:Id="STRId-8573456"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"><wsse:Reference URI="#CertId-3875628"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3"/></wsse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature></wsse:Security><nar:wsm.application.message
xmlns:nar="http://www.naradabroking.org">Tracker
:0.1662104721442097</nar:wsm.application.message><add:MessageID
xmlns:add="http://schemas.xmlsoap.org/ws/2004/08/addressing">cdf6f164-
9d3d-4a09-8d86-01f5fdb21a5</add:MessageID><add:From
xmlns:add="http://schemas.xmlsoap.org/ws/2004/08/addressing"><add:Adre
ss>http://156.56.104.46:18080/axis/services/WsrmserviceA</add:Address><
/add:From><add:To
xmlns:add="http://schemas.xmlsoap.org/ws/2004/08/addressing">http://156
.56.104.135:18080/axis/services/WsrmserviceB</add:To></soapenv:Header><
soapenv:Body wsu:Id="id-9449509" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"><nar:wsm.application.message
xmlns:nar="http://www.naradabroking.org">Tracker
:0.1662104721442097</nar:wsm.application.message></soapenv:Body></soap
env:Envelope>

```