WSS4C

Introduction

WSS4C is a set of C++ library classes that implement the OASIS Web Services Security: SOAP Messaging Security 1.0 (http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf) specification. Effort has been taken to closely mirror the existing Java implementation (http://ws.apache.org/ws-fx/wss4j/). It is expected that WSS4C will be incorporated in to the Apache Axis C++
project.

The specification describes three criteria that must be satisfied for WS-Security to be implemented

1. Sending security tokens as part of the message (E.g. Kerberos, Username token, X.509) 2. Ensure Message integrity (XML Signature: XML syntax used for representing signatures on digital content and 3. procedures for computing and verifying such signatures. Signatures provide for data integrity and authentication), and Message confidentiality (XML Encryption: Process for encrypting/decrypting digital content)

Contributors to the Project

- Sameera Perera
- Dinesh Premalal
- Sharanka Perera
- Farhaan Mohideen

References

- Specifications (http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf)
- WSS4J implementation (http://ws.apache.org/ws-fx/wss4j/)

Architecture

Figure 1-1 shows the Use-Case view of the overall implementation.

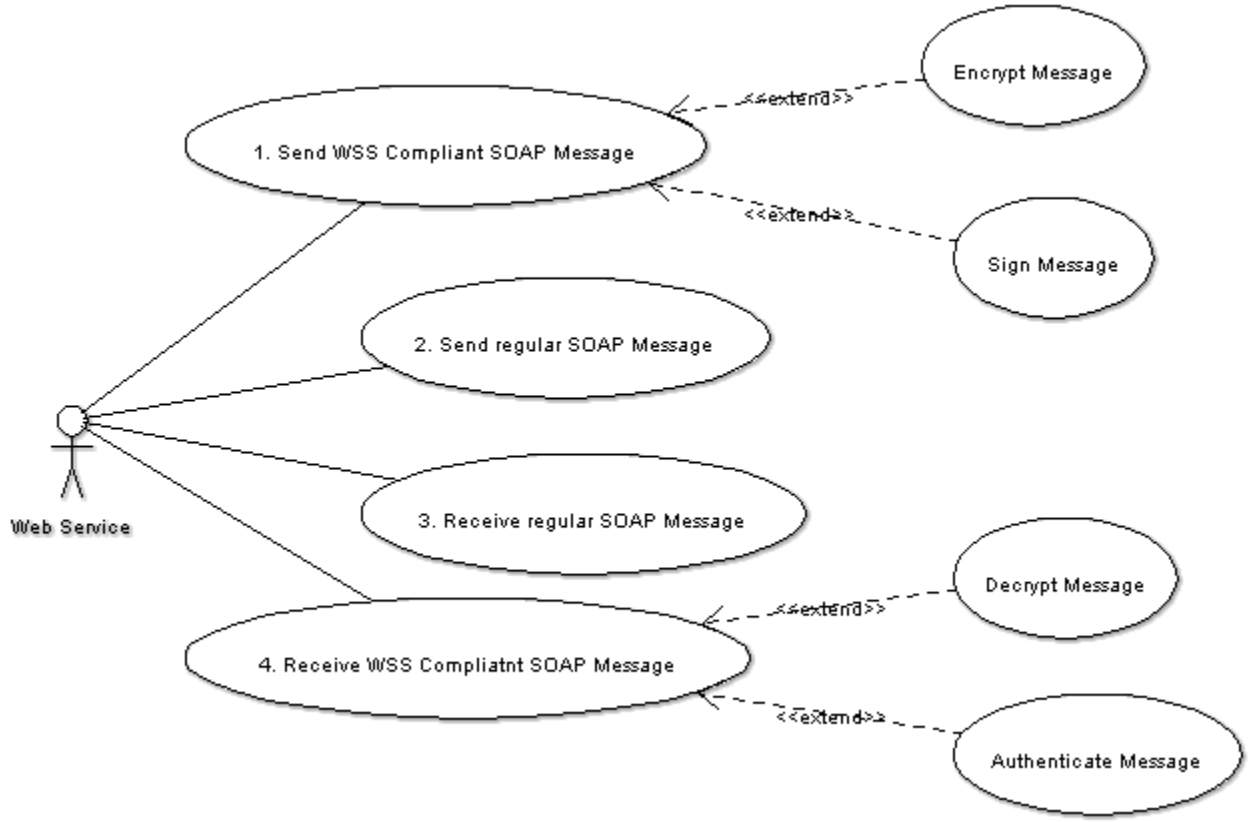

Figure 1-1

Note: Use-cases 2 and 3, signifies that WSS4C shall not interfere with the processing of regular (i.e. unencrypted and unsigned).

Security Tokens

XML Signature

This section describes the WSS4C implementation of the Digital Signatures for SOAP Message Security. Figure 2-1 illustrates the overall goals of the implementation.

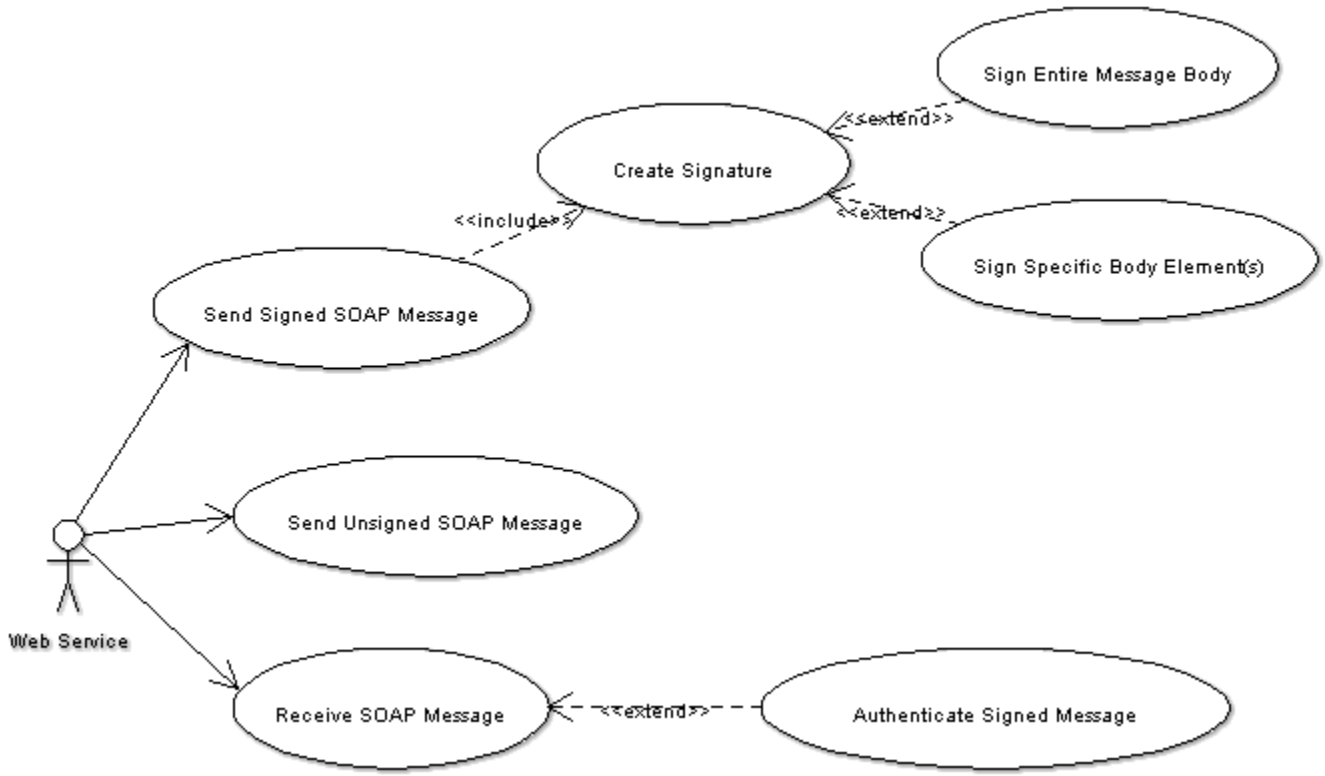

Figure 2-1

2.1 Architecture_of_Digital_Signature_Implementation

2.2 CurrentIssues

XML Encryption

The implementation of WSS4C has used Section 9 (Encryption) of OASIS WSS: SOAP Message Security 1.0 specification, as its starting point. As such, the development effort can be viewed as a “bottom-up” process.

Following diagram reflects the current state of the library.

? Unknown Attachment

A client class (e.g. an Axis Handler) of the library would simply make a function call on to WSEncryptBody which in turn will carry out the encryption of the specified SOAP message as par to the above mentioned specification. Following diagram reflects the current state of the library.

For Time being Encryption part carried out separatly By using XML-Security Library. For encryption , use many code from XML-Security library.

In this case , encrypts an element(and all its children) from pre-genarated key. It uses randomly genarated key to handle bulk encryption , and then encrypts this using RSA public key. The resultant encrypted key is embeded in an
<EncryptedKey> element.

Now it Encrypts only Element what we assinged.

Deployment

Details to be included here