HEALTH with STANDARDS

Secure Web Service Transportation for HL7 V3.0 Messages

Authors:

Somia Razzaq, Maqbool Hussain, Muhammad Afzal, Hafiz Farooq Ahmad

Presented By:

Muhammad Afzal

08 May, 2009

NUST School of Electrical Engineering and Computer Science, Pakistan

Outlines

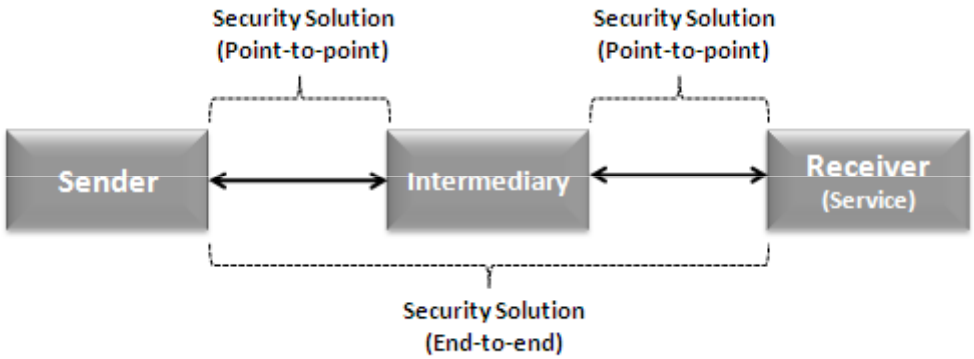
- Background
- Limitations of SSL
- HL7 V3.0 Web Service Profile
- Proposed Architecture
- Conclusion
- References

Background

- Healthcare is a many-to-many business
- Web service is a significant way for healthcare to exchange information in an interoperable way
- People are reluctant to use it due to lack of security
- Key challenge is to provide a robust end-to-end security model without compromising the interoperability of systems

Limitations of SSL

- SSL provides point-to-point security but there is need of end-to-end security solution



- SSL operates at the transport level and not at the message level
- SSL does not support element-wise signing and encryption
- SSL does not support non-repudiation

HL7 V3.0 Web Service Profile

- Provide implementation guidelines to promote interoperability between implementers using standard that fall under the general definition of web services
- Standardization of information among Healthcare applications without caring about the heterogeneity of platform, network protocol and transport protocol
- Promote interoperability as recommendations from organizations like WS-I, W3C, OASIS are taken into account
- Help to utilize the resources efficiently

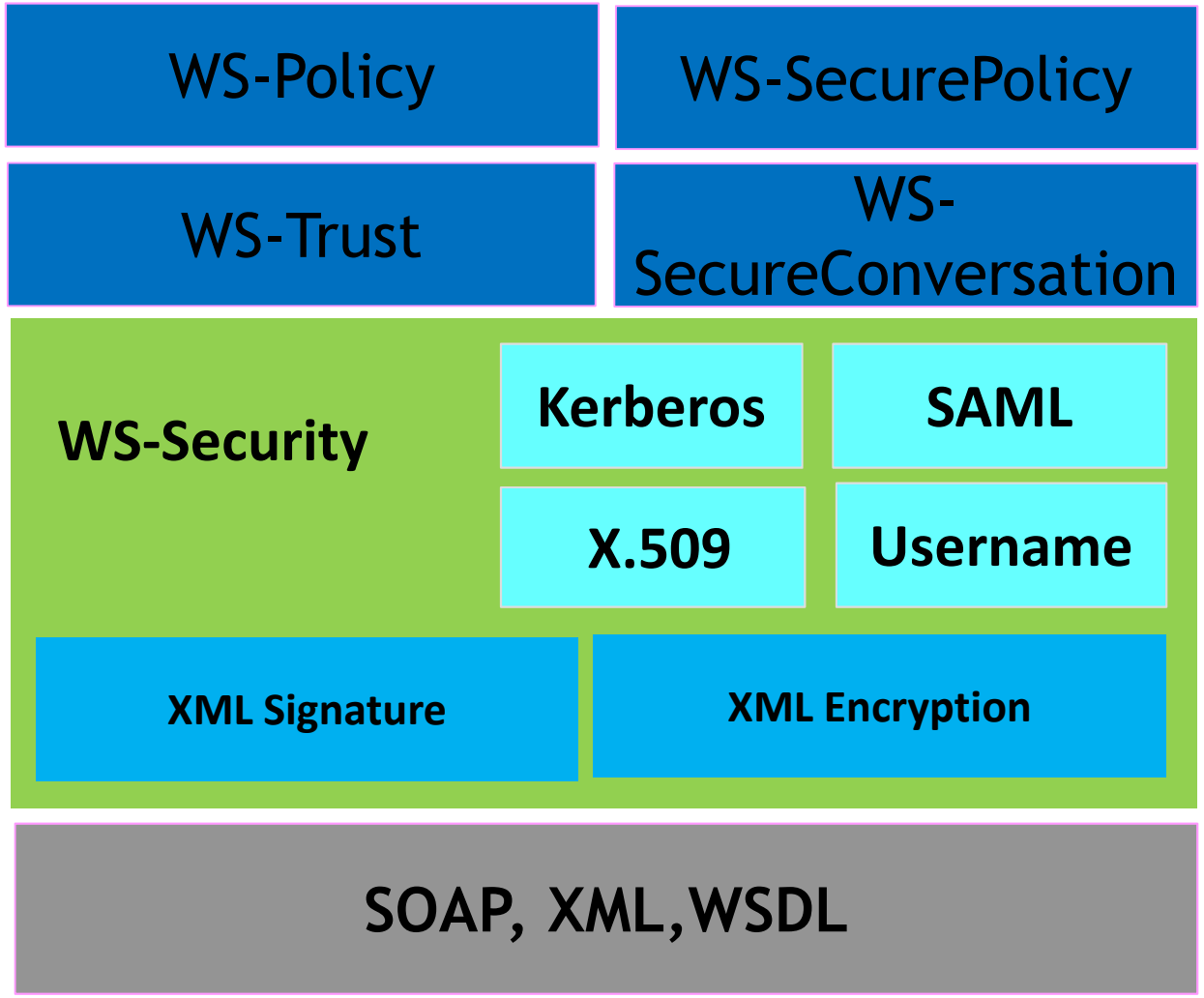
HL7 V3.0 Web Service Profile(Contd..)

- **Basic Profile**
  - Give idea about basic message exchange specification
  - Does not focus on advanced services such as “Security”
- **Addressing Profile**
  - Focuses on Message addressing properties and end-point references
  - There is need to adopt appropriate security measures

HL7 V3.0 Web Service Profile(Contd..)

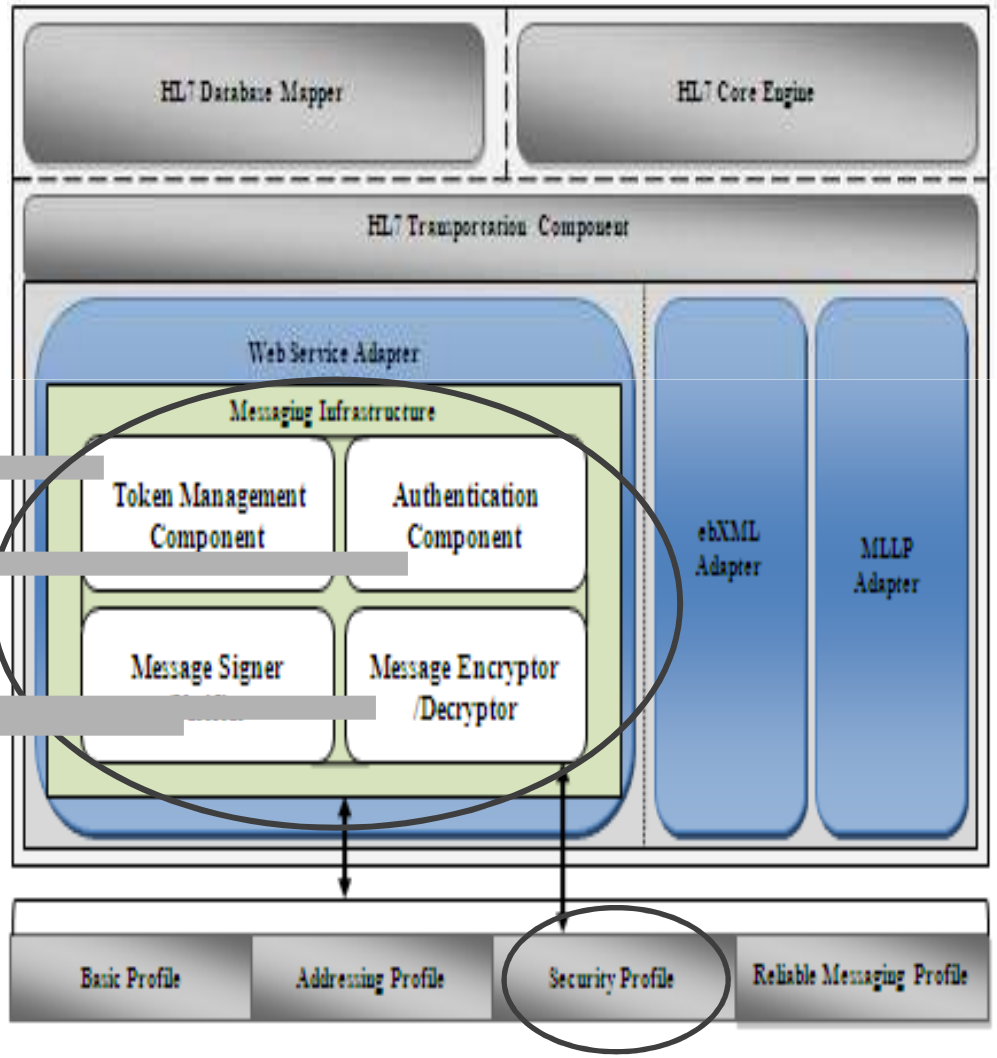
- **Security Profile**
  - General-purpose mechanism for associating security tokens with message content
  - Methods for signing and encrypting the messages
  - How to establish a security context
  - How to implement authentication mechanism for multiple message exchanges
  - How to exchange shared secrets or keys
  - How to establish or determine Trust

Web Service Security Framework



Proposed Architecture

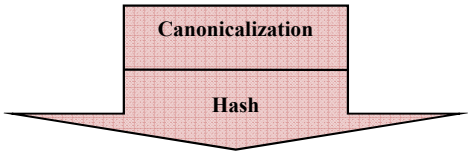
- This component helps to find "Who is the caller?" and "How does she/he prove her/his identity?" by using security tokens attached to each message
- This component is responsible for ensuring the integrity of the messages
- It works based on XML-based security tokens (SAML, REL)
  - XML Signature
  - WSSecureConversation
  - WS-Policy
- This component takes the derived token from the Token Management component, attach the derived token with the SOAP message and sign the whole message. On receiving, this component verifies the signatures
- This component is responsible for requesting, issuing, renewing and validating security tokens in order to provide confidentiality and privacy of messages
- It works based on binary security tokens (X.509 certificates, Kerberos tickets)
  - XML Encryption
  - WS-Trust



HL7 V3.0 Message Signature Generation


```
<patient>
<id root="2.16.840.1.113883.1122"  extension="375913"/>
<patient_Person> <!-- Ohio DL -->
<pat:id root="2.16.840.1.113883.1122"  extension="444-22-
2222"  validTime="-2003-05-20"
assigningAuthorityName="OH"/>
<pat:nm use="L" xsi:type="PN">
<dt:family>Everywoman</dt:family>
<dt:given>Eve</dt:given>
<dt:given>E</dt:given>
</pat:nm>  </patient_Person>
</patient>
```

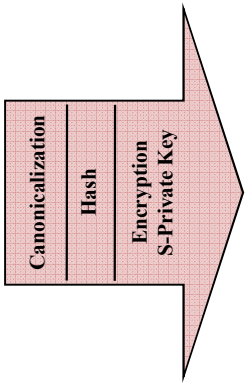
HL7 V3.0 Message




```
<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="#MsgBody">
<ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>GyGsFPi4xPU...</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
```

HL7 V3 Message Digest

Signed Information




```
<?xml….>
<S12:Envelope…> <S12:Header>
<wsse:Security …..> <ds:Signature><ds:SigedIno>
<ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsasha1>
<ds:Reference URI="#MsgBody">
<ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>GyGsFPi4xPU...</ds:DigestValue>
</ds:Reference> </ds:SignedInfo>
<ds:SignatureValue>HJJWbvqW9E84vJVQk.
</ds:SignatureValue>
<ds:KeyInfo> <wsse:SecurityTokenReference/ >
</ds:KeyInfo>
</ds:Signature></wsse:security></S12Header>
<S12:Body wsu:Id="MsgBody">
<ReportRequest>  HL7 V3 Message
</ReportRequest>
 </S12:Body>
 </S12:Envelope>
```

SOAP containing HL7 V3.0 Message with Signature

HL7 V3.0 Message Signature Verification

SOAP containing HL7 V3.0 Message with Signature

<?xml….>
<S12:Envelope…><S12:Header>
<wsse:Security …..> <ds:Signature><ds:SigedIno>
<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="#MsgBody">
<ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>GyGsFPi4xPU...</ds:DigestValue>
</ds:Reference> </ds:SignedInfo>

<ds:SignatureValue>HJJWbvqW9E84vJVQk.
</ds:SignatureValue>
<ds:KeyInfo> <wsse:SecurityTokenReference/ >
</ds:KeyInfo>
</ds:Signature>**</wsse:security></S12Header>**
<S12:Body wsu:Id="MsgBody">
<ReportRequest> **HL7 V3 Message**
</ReportRequest **</S12:Body></S12:Envelope>**

Digest Value

Compare

Verified

Decrypt (Sender's Public Key)

Compare

Hash **Canonicalization**

Hash **Canonicalization**

HL7 V3.0 Message

<patient>
<id root="2.16.840.1.113883.1122"
extension="375913"/>
<patient_Person>
<!-- Ohio DL -->
<pat:id root="2.16.840.1.113883.1122"
extension="444-22-2222"
validTime="-2003-05-20"
assigningAuthorityName="OH"/>
<pat:nm use="L" xsi:type="PN">
<dt:family>Everywoman</dt:family>
<dt:given>Eve</dt:given>
<dt:given>E</dt:given>
</pat:nm>
</patient_Person>
</patient>

<ds:SignedInfo>
<ds:CanonicalizationMethodAlgorithm
="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference
URI="#MsgBody">
<ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>GyGsFPi4xPU...</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>

Signed Information

Message Encryptor/Decryptor


```
<S11:Envelope xmlns:S11="..."
xmlns:wsse="..." xmlns:wsu="..." xmlns:ds="..."
xmlns:xenc="...">
<S11:Header>  <wsse:Security>
 <xenc:ReferenceList> <xenc:DataReference
URI="#HL7msgbodyID"/>
 </xenc:ReferenceList></wsse:Security>
</S11:Header>
 <S11:Body>
 <xenc:EncryptedData Id="HL7msgbodyID">
 <ds:KeyInfo>  <ds:KeyName>CN=HL7 Msg,
C=JP</ds:KeyName> </ds:KeyInfo>
 <xenc:CipherData>
 <xenc:CipherValue>.....</xenc:CipherValue>
 </xenc:CipherData>
</xenc:EncryptedData>
</S11:Body>
</S11:Envelope>
```

Encryption using different keys

```
<S11:Envelope xmlns:S11="..."
xmlns:wsse="..."xmlns:wsu="..."
xmlns:ds="..."xmlns:xenc="...">
<S11:Header>
<wsse:Security>
<xenc:EncryptedKey>
 ...
<ds:KeyInfo>
 <wsse:SecurityTokenReference>
<ds:X509IssuerSerial>
<ds:X509IssuerName>
DC=IEEECorp, DC=com
</ds:X509IssuerName>
<ds:X509SerialNumber>12345678</ds:X509SerialNu
mber>
</ds:X509IssuerSerial>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
...
</xenc:EncryptedKey>
 ...
</wsse:Security>
</S11:Header>
<S11:Body>
<xenc:EncryptedData Id="bodyID">
 <xenc:CipherData>
<xenc:CipherValue>...</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
</S11:Body>
</S11:Envelope>
```

Encryption using Same key

Conclusion and Future Work

- A flexible, scalable, cost-effective and interoperable solution can be achieved using HL7 V3.0 WS-Security profile
- Use of XML, SOAP and WSDL extensible models helps to achieve these goals
- The implementation of this security model is a challenging work
- The proposed security architecture can be extended to reliability architecture by incorporating web service reliability profile

References

- Securing Web Services and the Java WSDP 1.5 XWS-SecurityFramework http://java.sun.com/developer/technicalArticles/WebServices/security/
- Gib Trub, M. Partner,L. Olski, Managing Director GM, Global Report on SOA/Web services security initiatives, September 2008, version 1
- M.Afzal, Maqbool Hussain, H.Farooq Ahmad, Arshad Ali, “Design and Implementation of Open Source HL7 Version 3 for e-Health Services”IHIC 2008
- HL7 Version 3 Standard: Transport Specification – Web Services Profile, Release 2 Committee Ballot 1 - May 2008
- OASIS Standard Specification: Web Service Security: SAML Token Profile 1.1, 1 February 2006
- OASIS Standard Specification: WS-Trust 1.3, March 2007
- WS-MetaDataExchange version 1.1, August 2006
- OASIS Standard Specification: WS-SecureConversation 1.3, 1st March 2007
- OASIS Standard Specification: Web Service Security Username Token Profile 1.1, 1 February 2006
- OASIS Standard: Security Assertion Markup Language (SAML) V2.0 Technical Overview, Committee Draft 02, 25 March 2008
- OASIS Standard: Web Service Security SOAP Message Security 1.0, 1 March 2004
- W3C Recommendation: Exclusive XML Canonicalization Version 1.0, 18 July 2002
- W3C Recommendation: XML Encryption Syntax and Processing, 10 December 2002

Q&A

Thanks!

Challenge w.r.t Implementation

- Making existing systems compliant to HL7 V3.0 WS-Security profiles to achieve interoperability
- Formation of WS-Policy according to their own organizational, geographical and technical requirements
- Enabling interaction among systems following heterogeneous WS-Policy
- Establishment of WS-Trust and WS-SecureConversation among heterogeneous systems is a challenge