WS-Security Profile of the OASIS Security Assertion Markup Language (SAML)

Working Draft 04, 10 September 2002

Document identifier:
draft-sstc-ws-sec-profile-04

Location:
http://www.oasis-open.org/committees/security/docs

Editor:
Prateek Mishra, Netegrity <pmishra@netegrity.com>

Contributors:
Philip Hallam-Baker, Verisign
Jeff Hodges, Sun Microsystems
Eve Maler, Sun Microsystems
Chris McLaren, Netegrity
Irving Reid, Baltimore

Abstract:
This document specifies the WS-Security profile of SAML. WS-Security is a proposal for a standard set of SOAP extensions (message headers) that can be used to implement integrity and confidentiality. WS-Security also supports the secure addition of security tokens to SOAP messages. This specification defines how to use WS-Security headers for the secure addition of SAML assertions to SOAP messages.

Status:
Interim draft. Send comments to the editor.

Committee members should send comments on this specification to the security-services@lists.oasis-open.org list. Others should subscribe to and send comments to the security-services-comment@lists.oasis-open.org list. To subscribe, send an email message to security-services-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Security Services TC web page (http://www.oasis-open.org/committees/security/).

Table of Contents

Introduction 3
1.1 Notation 3
2 WS-Security Profile of SAML 4
2.1 Required Information 4
2.2 SAML Assertions and SOAP Headers 4
2.3 Error Codes 5
2.4 Processing Model 5
2.5 HolderOfKey Format 6
2.5.1 Sender 6
2.5.2 Receiver 6
2.5.3 Example 7
2.6 SenderVouches Format 8
2.6.1 Sender 8
2.6.2 Receiver 9
2.6.3 Example 9
2.7 Additional Issues 9
3 Security Considerations 10
3.1 Holder of Key 10
3.1.1 Eavesdropping 10
3.1.2 Replay 10
3.1.3 Message Insertion 11
3.1.4 Message Deletion 11
3.1.5 Message Modification 11
3.1.6 Man-in-the-Middle 11
3.2 Sender Vouches 11
3.2.1 Eavesdropping 12
3.2.2 Replay 12
3.2.3 Message Insertion 12
3.2.4 Message Deletion 12
3.2.5 Message Modification 12
3.2.6 Man-in-the-Middle 12
4 Conformance 14
5 References 15
Appendix A. Revision History 16
Appendix B. Notices 17

Introduction

This document specifies the WS-Security **[WS-Sec]** profile of SAML **[SAMLCore]**. WS-Security is a proposal for a standard set of SOAP **[SOAP1.1]** extensions (message headers) that can be used to implement integrity and confidentiality. WS-Security also supports the secure addition of security tokens to SOAP messages. This specification builds on these foundations in defining a message format that uses WS-Security headers for the secure addition of SAML assertions to SOAP messages.

1.1 Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in IETF RFC 2119 **[RFC2119]**.

```
Listings of productions or other normative code appear like this.
```

```
Example code listings appear like this.
```

Note: Non-normative notes and explanations appear like this.

Conventional XML namespace prefixes are used throughout this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:

- The prefix `saml:` stands for the SAML assertion namespace **[SAMLCore]**.
- The prefix `samlp:` stands for the SAML request-response protocol namespace **[SAMLCore]**.
- The prefix `ds:` stands for the W3C XML Signature namespace, `http://www.w3.org/2000/09/xmldsig#` **[XMLSig]**.
- The prefix `SOAP-ENV:` stands for the SOAP 1.1 namespace, `http://schemas.xmlsoap.org/soap/envelope` **[SOAP1.1]**.
- The prefix `wsse:` stands for the WS-Security 1.0 namespace `http://schemas.xmlsoap.org/ws/2002/04/secext` **[WS-Sec]**.

2 WS-Security Profile of SAML

The WS-Security profile of SAML is a realization of Scenarios 3-1 and 3-3 of the SAML requirements document **[SAMLReqs]** in the context of SOAP. It is based on a single interaction between a *sender* and a *receiver*, as follows:

1. The sender obtains one or more SAML assertions and/or assertion identifiers.
2. The sender adds the assertions and/or assertion identifiers to a SOAP message using WS-Security headers.
3. The sender sends the SOAP message with the included assertions and assertion identifiers to the receiver. The SOAP message may be sent over any protocol for which a SOAP protocol binding is available **[SOAP1.1]**.
4. The receiver attempts to process the assertions and assertion identifiers present in the SOAP message. If it cannot process them, it returns an error message. If it can process them, it does so and also processes the rest of the SOAP message in an application-dependent way.

In the terminology of WS-Security, SAML assertions or assertion identifiers constitute *claims*. Additional components such as signatures may also be required to provide *proof-of-possesion* or demonstrations of knowledge at the sender known only to senders with a particular relationship to the claims.

See **[SAMLBind]** for the definition of the SOAP binding for SAML, as opposed to the WS-Security profile of SAML.

2.1 Required Information

Identification: urn:oasis:names:tc:SAML:1.0:profiles:ws-security

Contact information: security-services-comment@lists.oasis-open.org

Description: Given below.

Updates: None.

2.2 SAML Assertions and SOAP Headers

SOAP provides a flexible header mechanism, which may be used for extending SOAP payloads with additional information. Rules for SOAP headers are given in **[SOAP1.1]** §4.2. WS-Security extends this foundation by proposing the use of a `<wsse:Security>` header element to provide a mechanism for attaching security-related information targeted at a specific receiver.

SAML assertions and references to assertion identifiers MUST be contained within the `<wsse:Security>` element, which in turn is carried within the `<SOAP-ENV:Header>` element.

Every SAML assertion MUST be signed by the issuer following the guidelines in **[SAMLCore]**.

Assertion identifier references and information about assertion retrieval services MUST be carried within the `<wsse:SecurityTokenReference>` element. One or more `<saml:AssertionIDReference>` elements holding the assertion identifier references may be included within the `<wsse:SecurityTokenReference>` element. The URI attribute of the `<wsse:Reference>` element specifies the location of a SAML responder implementing the SAML SOAP binding **[SAMLBind]**.

Example:

```
<wsse:SecurityTokenReference>
  <saml:AssertionIDReference>XVB12#$21abc</AssertionIDReference>
  <wsse:Reference URI=http://www.example.com/SAMLservice”/>
</wsse:SecurityTokenReference>
```

Two standard SOAP attributes are available for use with top-level header elements: `actor` and `mustUnderstand`. **[WS-Sec]** § 4 provides recommendations for the use of the `actor` attribute with the `<wsse:Security>` element. Use of `the mustUnderstand` attribute is application-dependent and no normative use is specified herein.

2.3 Error Codes

If the receiver is able to access the SAML assertions contained in the `<wsse:Security>`header, but is unable to process them, the receiver MUST use one of the fault codes listed in **[WS-Sec]** §6. A receiver MUST not return any other SAML-related fault code.

Reasons why the receiver may be unable to process SAML assertions, include, but are not limited to:

1. The assertion contains a `<saml:Condition>` element that the receiver does not understand.
2. The signature on the assertion is invalid.
3. The receiver does not accept assertions from the issuer of the assertion in question.
4. The receiver does not understand the extension schema used in the assertion.

It is RECOMMENDED that the `<SOAP-ENV:Faultstring>` element contain an informative message. This specification does not specify any normative text. Sending parties MUST NOT rely on specific contents in the `<SOAP-ENV:Faultstring>` element.

Following is an example of providing fault information:

```
<SOAP-ENV:Fault>
  <SOAP-ENV:Faultcode>wsse:UnsupportedSecurityToken</SOAP-ENV:Faultcode>
  <SOAP-ENV:Faultstring>SAML Version Error</SOAP-ENV:Faultstring>
</SOAP-ENV:Fault>
```

2.4 Processing Model

The receiver MUST resolve each assertion reference carried within a `<wsse:SecurityTokenReference>` element and acquire an assertion for each such reference. This MAY be accomplished by the receiver sending a `<samlp:Request>` message with <saml:AssertionIDReference> elements to the SAML service described by the URI attribute of the `<wsse:Reference>` element. If the receiver is unable to resolve an assertion reference it MUST return a `wsse:SecurityTokenUnavailable` error to the sender.

The sender and receiver MUST ensure the data integrity of SOAP messages and contained assertions. A variety of different techniques are available for providing data integrity, including, for example, use of TLS/SSL, digital signatures over the SOAP message, and IPsec.

When a receiver processes a SOAP message containing SAML assertions, it MUST make an explicit determination of the relationship between subject of the assertions and the sender. Merely obtaining a SOAP message containing assertions carries no implication about the sender's right to possess and communicate the included assertions. A variety of means are available for making such a determination, including, for example, explicit policies at the receiver, authentication of sender, and use of digital signature.

Two message formats for ensuring the data integrity of a SOAP message and included assertions, `HolderOfKey` and `SenderVouches`, are described below. The `HolderOfKey` format has the additional property that it implies a specific relationship between the sender and subject of the assertions included within the SOAP message. Senders and receivers implementing the WS-Security Profile of SAML MUST implement both formats.

2.5 HolderOfKey Format

The following section describe the `HolderOfKey` format for ensuring the data integrity of a SOAP message and included assertions.

2.5.1 Sender

In this case, the sender and the subject are the same entity. The sender obtains one or more assertions or assertion identifiers from one or more authorities. Each assertion or referenced assertion MUST include the following `<saml:SubjectConfirmation>` element:

```
<saml:SubjectConfirmation>
  <saml:ConfirmationMethod>
urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
  </saml:ConfirmationMethod>
  <ds:KeyInfo>…</ds:KeyInfo>
</saml:SubjectConfirmation>
```

The `<saml:SubjectConfirmation>` element carries information about the sender's key within the `<ds:KeyInfo>` element. The `<ds:KeyInfo>` element provides varied ways for describing information about the sender's public or secret key.

In addition to the assertions, the sender MUST include a `<ds:Signature>` element within the WS-Sec `<wsse:Security> header`. Section 4.5 of [WS-Sec] provides recommendations for the canonicalization and transformation algorithms that should be used to construct the signature.

Following the recommendations in **[WS-Sec]** §4, the `<ds:Signature>` element should be added before the SAML assertions. The `<ds:Signature>` element MUST apply to the relevant SAML assertion and `<wsse:SecurityTokenReference>` elements found in the `<wsse:Security>` element, and all the relevant portions of the `<SOAP-ENV:Body>` element, as required by the application. Specific applications might require that the signature also apply to additional elements in SOAP header.

2.5.2 Receiver

The receiver MUST verify that each assertion carries a `<saml:SubjectConfirmation>` element of the following form:

```
<saml:SubjectConfirmation>
  <saml:ConfirmationMethod>
urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
  </saml:ConfirmationMethod>
  <ds:KeyInfo>…</ds:KeyInfo>
</saml:SubjectConfirmation>
```

The receiving party MUST follow the recommendations of **[WS-Sec]** §4.5.3 for verifying integrity of the `<wsse:Security>`/`<ds:Signature>` sub-element of the SOAP message. The receiving party SHOULD use the sender's public or information about a secret key carried within the `<saml:SubjectConfirmation>`/`<ds:KeyInfo>` element carried within each assertion.

> **Note:** The `<ds:KeyInfo>` element is used only for checking integrity of assertion attachment (message integrity). Therefore, there is no requirement that the receiver validate the key or certificate. This suggests that, if needed, a sender can generate a public/private key pair and utilize it for this purpose.

Once the above steps have been completed, the receiver can further process the assertions and SOAP message contents with the assurance that portions of the SOAP message that fall within the scope of the digital signature have been constructed by the sender and have not been altered by an intermediary. Further, the sender has provided proof of possession of the corresponding private-key (or secret-key) component of the information included in the

<saml:SubjectConfirmation>/<ds:KeyInfo> element included in each assertion. If the receiver believes the assertions to be valid, then the information contained in the assertions MAY be considered to be describing the sender.

2.5.3 Example

The following example illustrates the HolderOfKey message format:

```
<?xml:version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">

<SOAP-ENV:Header>
<wsse:Security>
  <saml:Assertion
    xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
    MajorVersion="1" MinorVersion="0"
    AssertionID="2sxJu9g/vvLG9sAN9bKp/8q0NKU="
    Issuer="www.example.com"
    IssueInstant="2002-06-19T16:58:33.173Z">
    <saml:Conditions
      NotBefore="2002-06-19T16:53:33.173Z"
      NotOnOrAfter="2002-06-19T17:08:33.173Z"/>

    <saml:AuthenticationStatement
      AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password"
      AuthenticationInstant="2002-06-19T16:57:30.000Z">
      <saml:Subject>
        <saml:NameIdentifier
          NameQualifier="www.example.com"
          Format="">
uid=joe,ou=people,ou=saml-demo,o=example.com
        </saml:NameIdentifier>
        <saml:SubjectConfirmation>
          <saml:ConfirmationMethod>
urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
          </saml:ConfirmationMethod>
          <ds:KeyInfo>
            <ds:KeyValue>…</ds:KeyValue>
          </ds:KeyInfo>
        </saml:SubjectConfirmation>
      </saml:Subject>
    </saml:AuthenticationStatement>

    <saml:AttributeStatement>
      <saml:Subject>
        <saml:NameIdentifier
          NameQualifier="www.example.com"
          Format="">
uid=joe,ou=people,ou=saml-demo,o=baltimore.com
        </saml:NameIdentifier>
        <saml:SubjectConfirmation>
          <saml:ConfirmationMethod>
urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
          </saml:ConfirmationMethod>
          <ds:KeyInfo>
            <ds:KeyValue>…</ds:KeyValue>
          </ds:KeyInfo>
        </saml:SubjectConfirmation>
      </saml:Subject>
```

```
      <saml:Attribute
        AttributeName="MemberLevel"
        AttributeNamespace="http://www.oasis-
open.org/Catalyst2002/attributes">
          <saml:AttributeValue>gold</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute
        AttributeName="E-mail"
        AttributeNamespace="http://www.oasis-
open.org/Catalyst2002/attributes">
        <saml:AttributeValue>joe@yahoo.com</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
    <ds:Signature>…</ds:Signature>
  </saml:Assertion>
  <ds:Signature>
    <ds:SignedInfo>…</ds:SignedInfo>
    <ds:SignatureValue>
HJJWbvqW9E84vJVQkjjLLA6nNvBX7mY00TZhwBdFNDElgscSXZ5Ekw==
    </ds:SignatureValue>
  </ds:Signature>
</wsse:Security>
</SOAP-ENV:Header>

<SOAP-ENV:Body>
  <ReportRequest>
    <TickerSymbol>SUNW</TickerSymbol>
  </ReportRequest>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

2.6 SenderVouches Format

The following section describe the `SenderVouches` format for ensuring the data integrity of a SOAP message and included assertions.

2.6.1 Sender

In this case, the sender and subject MAY be distinct entities. The sender obtains one or more assertions or assertion identifiers from one or more authorities and includes them in a SOAP message. Each assertion or referenced assertion MUST include the following `<saml:SubjectConfirmation>` element:

```
<saml:SubjectConfirmation>
  <saml:ConfirmationMethod>
urn:oasis:names:tc:SAML:1.0:cm:sender-vouches
  </saml:ConfirmationMethod>
</saml:SubjectConfirmation>
```

In addition to the assertions, the sender MUST include a `<ds:Signature>` element within the WS-Security `<wsse:Security>` element. The `<ds:Signature>` element MUST apply to the relevant SAML assertion and `<wsse:SecurityTokenReference>` elements found in the `<wsse:Security>` element, and all the relevant portions of the `<SOAP-ENV:Body>` element, as required by the application. Specific applications might require that the signature also apply to additional elements in SOAP header.

Following the XML Signature specification, the sender MAY include a `<ds:KeyInfo>` element within the `<ds:Signature>` element. The `<ds:KeyInfo>` element provides varied ways for describing information about the sender's public or secret key. If it is omitted, the receiver is expected to identify the key based on context.

2.6.2 Receiver

The receiver MUST verify that each assertion carries a `<saml:SubjectConfirmation>` element of the following form:

```
<saml:SubjectConfirmation>
  <saml:ConfirmationMethod>
urn:oasis:names:tc:SAML:1.0:cm:sender-vouches
  </saml:ConfirmationMethod>
</saml:SubjectConfirmation>
```

The receiving party MUST check the validity of the signature found in the `<wsse:Security>/<ds:Signature>` element. Information about the sender's public or secret key either is found in the `<wsse:Security>/<ds:Signature>/<ds:KeyInfo>` element carried within the SOAP envelope or is based on application context.

Once the above steps have been completed, the receiver can further process the assertions and SOAP message contents with the assurance that portions of the SOAP message that fall within the scope of the digital signature have been constructed by the sender and have not been altered by an intermediary.

In contrast to the `HolderOfKey` case, information about the sender either is provided by the contents of the `<ds:KeyInfo>` element found within the signature or is based on application context.

2.6.3 Example

The following example illustrates the `SenderVouches` message format:

```
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header
    xmlns:saml="…"
    <wsse:Security>
      <wsse:SecurityTokenReference>
      <saml:AssertionIDReference>XVB12#$21abc</AssertionIDReference>
      <wsse:Reference URI=http://www.example.com/SAMLservice”/>
      </wsse:SecurityTokenReference>
      <saml:Assertion>…</saml:Assertion>
      <ds:Signature>…
        <ds:KeyInfo>…</ds:KeyInfo>
      </ds:Signature>
    </wsse:Security>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    …
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

2.7 Additional Issues

The processing models described in this section does not take into account replay attacks, authentication of sender by receiver, authentication of receiver by sender, or confidentiality. These concerns must be addressed by means other than those described in this section.

3 Security Considerations

This profile defines methods for securely attaching SAML assertions to a SOAP document. SOAP documents are used in multiple contexts, specifically including cases where the message is transported without an active session, the message can be persisted, and the message is routed through a number of intermediaries. Such a general context of use suggests that users of this profile must be concerned with a variety of threats. In particular, no consideration has been given to the issue of sender or receiver authentication. Therefore, if required, the sender may need to authenticate the receiver using some authentication technique dependent on the context of use. Further, the receiver may need to authenticate the sender using some techniques dependent on the context of use. In the latter case, there is a possibility that the receiver may authenticate the sender utilizing the attached SAML assertions as a credential together with other information.

3.1 Holder of Key

This profile has one or more authorities issuing assertions that contain `<SubjectConfirmation>` elements that essentially say “This assertion is valid if it is presented with proof that the presenter is the holder of the specified key.”

A sender inserts these assertions in a message and the entire message (payload and assertions) are digitally signed using the specified key—thus providing proof to the receiver that the sender of the message held the key specified in the assertions.

3.1.1 Eavesdropping

Eavesdropping continues to be a threat in the same manner as for the SAML SOAP binding, as discussed in **[SAMLSecure][SAMLSecure]**. The routable nature of SOAP adds the potential for a large number of steps and actors in the course of a message’s lifetime, which means that the potential incidences of eavesdropping are increased as the number of possible times a message is in transit increases.

The persistent nature of SOAP messages adds an additional possibility of eavesdropping, in that stored items can be read from their store.

To provide maximum protection from eavesdropping, assertions should be encrypted in such a way that only the intended audiences can view the material. This removes threats of eavesdropping in transit, but does not remove risks associated with storage by the receiver or poor handling of the clear text by the receiver.

3.1.2 Replay

Binding of assertions to a document opens the door to replay attacks by a malicious user. Issuing a `HolderOfKey` assertion amounts to “blessing the user’s key” for the purpose of binding assertions to documents. Once a `HolderOfKey` assertion has been issued to a user, that user can bind it to any document or documents he chooses.

While each assertion is signed, and bound by a second signature into a document, which prevents a malicious third-party (who has no access to the private key required for the binding signature) from binding the assertions to arbitrary documents, there is nothing preventing a malicious **user** (who by definition has access to the private key) from detaching a signed assertion from the document it arrived in and rebinding it to another document.

There are two lines of defense against this type of attack. The first is to consider carefully to whom you issue `HolderOfKey` assertions (can they be trusted with the right to attach the assertion to any document?) and what kind of assertions you issue as `HolderOfKey` assertions (do you want to give up control over the binding of this particular statement to a given

document?). The second is a short lifetime on the assertion, to narrow the window of opportunity for this attack.

The capture and resubmission of the entire message (SAML assertions and business payload) is a threat. One counter-measure is to add information about time, or a sequence number to the digital signature included in the SOAP header. The receiver can use this information to detect duplicate messages.

3.1.3 Message Insertion

There is no message insertion attack at the level of the `HolderOfKey` format of this profile.

3.1.4 Message Deletion

There is no message deletion attack at the level of the `HolderOfKey` format of this profile.

3.1.5 Message Modification

The double signing in this profile prevents most message modification attacks. The receiver is always able to verify the signature on the assertion itself (and should be able to verify that the key used in that signing act is associated with the putative signer by means of X509v3 certificate, Certificate Revocation List checks, and so on), which provides a guarantee that the assertion is unaltered.

The receiver can also verify the binding signature to ensure that the message to which the assertion is attached is unaltered.

The profile is secure against modification within the context of an existing trust relationship. The remaining threats (compromised keys, revoked certificates being used, and so on) are outside the scope of SAML.

Note that the threat of message modification by the holder of the key exists, as discussed in the discussion of replay attacks in Section 3.1.2.

3.1.6 Man-in-the-Middle

An MITM attack is impossible for the `HolderOfKey` format of this profile, since the assertion specifies the key that must be used for the binding signature, and the assertion itself is protected against tampering by a signature.

The MITM can eavesdrop (if communication is not protected by some confidentiality scheme) but cannot alter the document without detection.

Note that a MITM could alter parts of the document unprotected by the signature (i.e. the other header elements within the `<ds:Signature>` element). For example, a MITM could remove an included `<ds:KeyInfo>` block from a `<ds:Signature>` without affecting the validity of the signature. Theoretically this could force an XKMS lookup or other network call that could be perverted to malicious ends. However this does not pose a threat for the HolderOfKey profile since (1) the assertion has issuer info (so you know who originated the assertion came) (2) the signed assertion includes the key for the binding signature.

3.2 Sender Vouches

This profile has one or more authorities issuing assertions that contain `<SubjectConfirmation>` elements that basically say “Trust these if you trust the issuer and the entity who signed them”.

A sender collects these assertions and inserts them in a message. The sender then signs over the entire message, with the signature being used to indicate that these assertions (which are themselves signed by their issuers) are vouched for by the sender.

3.2.1 Eavesdropping

Eavesdropping continues to be a threat in the same manner as for the SAML SOAP binding, as discussed in **[SAMLSecure]**. The routable nature of SOAP adds the potential for a large number of steps and actors in the course of a message's lifetime, which means that the potential incidences of eavesdropping are increased as the number of possible times a message is in transit increases.

The persistent nature of SOAP messages adds an additional possibility of eavesdropping, in that persisted items can be read from their store.

To provide maximum protection from eavesdropping, assertions should be encrypted in such a way that only the intended audiences can view the material. This removes threats of eavesdropping in transit, but does not remove risks associated with storage by the receiver or poor handling of the clear text by the receiver.

3.2.2 Replay

The fact that the sender does all binding prevents a variety of replay attacks that reuse the assertion with different documents. In this case the assertions are directly signed into the document, so separating them from the document for reuse would not benefit a malicious user. (i.e. The assertions are only as valid as the binding signature of the sender, so reusing them with a different key does not pose a risk).

Authorities should note that once a "SenderVouches" assertion has been issued, there is no control over who may use it. Any entity coming into contact with the assertion can separate these assertions and use them by signing them with their own keys. Consumers of SenderVouches assertions must, therefore, carefully decide which senders to allow to vouch for what assertions.

The capture and resubmission of the entire message (SAML assertions and business payload) is a threat. One counter-measure is to add information about time, or a sequence number to the digital signature included in the SOAP header. The receiver can use this information to detect duplicate messages.

3.2.3 Message Insertion

There is no message insertion attack at the level of the `SenderVouches` format of this profile.

3.2.4 Message Deletion

There is no message insertion attack at the level of the `SenderVouches` format of this profile.

3.2.5 Message Modification

The binding signature should prevent any message modification attacks. Selection of what parts of the document to sign should be made carefully with the possibility of this attack in mind.

Receivers should consider only the portions of the document actually bound by signature to the assertions as valid with respect to the assertions.

3.2.6 Man-in-the-Middle

The requirement for a signature here should prevent MITM attacks. Note that the verifiability of the signature is key to this step: Not only must a receiver be able to verify that a document was signed with a key, but he also needs to be able to verify the binding of key to identity. This may be accomplished by including an X509v3 certificate with the digital signature, which the receiver verifies by some means (XKMS, OCSP, CRLs) and further maps onto a known identity for the signer.

If this step is skipped, then MITM becomes a possibility: The MITM captures the original document, alters it, and passes along this new document signed with a key that purports to be from the original sender (but which is actually held by the MITM).

The MITM can eavesdrop (if communication is not protected by some confidentiality scheme) but cannot alter the document without detection.

4 Conformance

TBD

5 References

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

[SAMLBind] P. Mishra (Editor), Bindings and Profiles for the OASIS *Security Assertion Markup Language (SAML)*, Committee Specification 01, available from http://www.oasis-open.org/committees/security, OASIS, May 2002.

[SAMLCore] P. Hallam-Baker, P., and E. Maler, (Editors), *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)*, Committee Specification 01, available from http://www.oasis-open.org/committees/security, OASIS, May 2002.

[SAMLReqs] D. Platt et al., SAML Requirements and Use Cases, OASIS, December 2001.

[SAMLSecure] Security and Privacy Cpnsiderations for the OASIS Security Assertion Markup Language (SAML), http://www.oasis-open.org/committees/security/docs/cs-sstc-sec-consider-01.doc

[SOAP1.1] D. Box et al., *Simple Object Access Protocol (SOAP) 1.1*, http://www.w3.org/TR/SOAP, World Wide Web Consortium Note, May 2000.

[WS-Sec] Web Services Security (WS-Security), Version 1.0, August 5, 2002, available from http://www.verisign.com/spotlight

[XMLSig] D. Eastlake et al., *XML-Signature Syntax and Processing*, http://www.w3.org/TR/xmldsig-core/, World Wide Web Consortium.

Appendix A. Revision History

Rev	Date	By Whom	What
wd-00	2002-06-16	Prateek Mishra	Added use of WS-Security headers to contents of draft-sstc-soap-profile-01.doc.
wd-01	2002-07-23	Prateek Mishra	Added use of <wsse:SecurityTokenReference> to carry SAML assertion id references.
wd-02	2002-08-16	Prateek Mishra	Comments from Allen Rogers, Dipak Chopra. Added use of terminology from WS-Security draft.
wd-03	2002-08-21	Prateek Mishra, Eve Maler	Editorial cleanup. Addition of assertion reference example.
wd-04	2002-09-10	Prateek Mishra	Clarification on authorship and IPR issues relevant to WSS submission

Appendix B. Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.