Web Services Security Core Specification

Working Draft 02, 24 October 2002

Deleted: 01

Deleted: 20

Deleted: September

Document identifier:

WSS-Core-02

Deleted: 01

Location:

TBD

Editors:

Phillip Hallam-Baker, VeriSign
Chris Kaler, Microsoft
Ronald Monzillo, Sun
Anthony Nadalin, IBM

Contributors:

TBD – Revise this list to include WSS TC contributors

Bob Atkinson, Microsoft
Giovanni Della-Libera, Microsoft
Satoshi Hada, IBM
Phillip Hallam-Baker, VeriSign
Maryann Hondo, IBM
Chris Kaler, Microsoft
Johannes Klein, Microsoft
Brian LaMacchia, Microsoft
Paul Leach, Microsoft
John Manferdelli, Microsoft
Hiroshi Maruyama, IBM
Anthony Nadalin, IBM
Nataraj Nagaratnam, IBM
Hemma Prafullchandra, VeriSign
John Shewchuk, Microsoft
Dan Simon, Microsoft
Kent Tamura, IBM
Hervey Wilson, Microsoft

Abstract:

This specification describes enhancements to the SOAP messaging to provide *quality of protection* through message integrity, message confidentiality, and single message authentication. These mechanisms can be used to accommodate a wide variety of security models and encryption technologies.

This specification also provides a general-purpose mechanism for associating security tokens with messages. No specific type of security token is required; it is designed to be extensible (e.g. support multiple security token formats). For example, a client might provide one format for proof of identity and provide another format for proof that they have a particular business certification.

Additionally, this specification describes how to encode binary security tokens, a framework for XML-based tokens, and describes how to include opaque encrypted keys. It also includes extensibility mechanisms that can be used to further describe the characteristics of the tokens that are included with a message.

Status:

This is an interim draft. Please send comments to the editors.

Committee members should send comments on this specification to the wss@lists.oasis-open.org list. Others should subscribe to and send comments to the wss-comment@lists.oasis-open.org list. To subscribe, visit http://lists.oasis-open.org/ob/adm.pl.

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/who/intellectualproperty.shtml).

Table of Contents

Deleted:

1 Introduction

This specification proposes a standard set of SOAP extensions that can be used when building secure Web services to implement message level integrity and confidentiality. This specification refers to this set of extensions as the “Web Services Security Core Language” or “WSS-Core”.

This specification is flexible and is designed to be used as the basis for the construction of a wide variety of security models including PKI, Kerberos, and SSL. Specifically, this specification provides support for multiple security token formats, multiple trust domains, multiple signature formats, and multiple encryption technologies.

This specification provides three main mechanisms: message level security token propagation, message integrity, and message confidentiality. These mechanisms by themselves do not provide a complete security solution for Web services. Instead, this specification is a building block that can be used in conjunction with other Web service extensions and higher-level application-specific protocols to accommodate a wide variety of security models and security technologies.

These mechanisms can be used independently (e.g., to pass a security token) or in a tightly coupled manner (e.g., signing and encrypting a message and providing a security token hierarchy associated with the keys used for signing and encryption).

Deleted: Note that Section 1 is non-normative. ¶

1.1 Goals and Requirements

The goal of this specification is to enable applications to construct secure SOAP message exchanges.

This specification is intended to provide a flexible set of mechanisms that can be used to construct a range of security protocols; in other words this specification intentionally does not describe explicit fixed security protocols.

As with every security protocol, significant efforts must be applied to ensure that security protocols constructed using this specification are not vulnerable to a wide range of attacks.

Deleted: To summarize, t

The focus of this specification is to describe a single-message security language that provides for message security that may assume an established session, security context and/or policy agreement.

The requirements to support secure message exchange are listed below.

1.1.1 Requirements

The Web services security language must support a wide variety of security models. The following list identifies the key driving requirements for this specification:

- Multiple security token formats
- Multiple trust domains
- Multiple signature formats
- Multiple encryption technologies
- End-to-end message-level security and not just transport-level security

1.1.2 Non-Goals

The following topics are outside the scope of this document:

- Establishing a security context or authentication mechanisms.
- key derivation

Deleted: Key exchange and

Deleted: ed keys

- How trust is established or determined.

2 Notations and Terminology

This section specifies the notations, namespaces, and terminology used in this specification.

2.1 Notational Conventions

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119.

Namespace URIs (of the general form "some-URI") represent some application-dependent or context-dependent URI as defined in RFC2396.

This specification is designed to work with the general SOAPmessage structure and message processing model, and should be applicable to any version of SOAP. The current SOAP 1.2 namespace URI is used herein to provide detailed examples, but there is no intention to limit the applicability of this specification to a single version of SOAP.

Readers are presumed to be familiar with the terms in the Internet Security Glossary.

2.2 Namespaces

The XML namespace URIs that MUST be used by implementations of this specification are as follows (note that different elements in this specification are from different namespaces):

```
        http://schemas.xmlsoap.org/ws/2002/xx/secext
        http://schemas.xmlsoap.org/ws/2002/xx/utility
```

The following namespaces are used in this document:

Prefix	Namespace
S	http://www.w3.org/2001/12/soap-envelope
ds	http://www.w3.org/2000/09/xmldsig#
xenc	http://www.w3.org/2001/04/xmlenc#
wsse	http://schemas.xmlsoap.org/ws/2002/xx/secext
wsu	http://schemas.xmlsoap.org/ws/2002/xx/utility

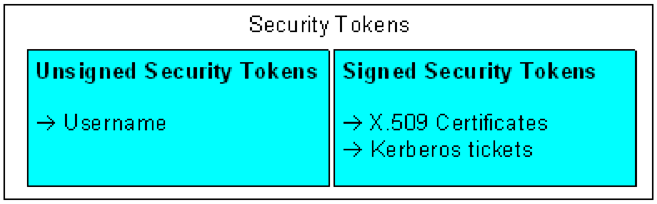
2.3 Terminology

Defined below are the basic definitions for the security terminology used in this specification.

Claim – A *claim* is a statement that a client makes (e.g. name, identity, key, group, privilege, capability, etc).

Security Token – A *security token* represents a collection of claims.

Signed Security Token – A *signed security token* is a security token that is asserted and cryptographically endorsed by a specific authority (e.g. an X.509 certificate or a Kerberos ticket).



Proof-of-Possession – *Proof-of-possession* information is data that is used in a proof process to demonstrate that a sender is acting on behalf of a (claimed) client, based on knowledge of information that should only be known to the client. Proof-of-possession information is used to bind a client and a sender acting on behalf of a client within a security token.

Integrity – *Integrity* is the process by which it is guaranteed that information is not modified.

Confidentiality – *Confidentiality* is the process by which data is protected such that only authorized roles or security token owners can view the data

Digest – A *digest* is a cryptographic checksum of an octet stream.

Signature - A *signature* is a cryptographic binding of a proof-of-possession and a digest. This covers both symmetric key-based and public key-based signatures. Consequently, non-repudiation is not always achieved.

Attachment – An *attachment* is a generic term referring to additional data that travels with a SOAP message, but is not part of the SOAP Envelope.

Deleted: The *proof-of-possession* information is data that is used in a proof process to demonstrate the sender's knowledge of information that SHOULD only be known to the claiming sender of a security token

Deleted: in transit.

Deleted: Quality of

3 Message Protection Mechanisms

In order to secure a SOAP message, two types of threats should be considered: 1) the message could be modified or read by antagonists or 2) an antagonist could send messages to a service that, while well-formed, lack appropriate security claims to warrant processing.

To understand these threats this specification defines a message security model.

3.1 Message Security Model

This document specifies an abstract *message security model* in terms of security tokens combined with digital signatures as proof of possession of the security token (key).

Security tokens assert claims and signatures provide a mechanism for proving the sender's knowledge of the key. As well, the signature can be used to "bind" or "associate" the signature with the claims in the security token (assuming the token is trusted). Note that such a binding is limited to those elements covered by the signature. Furthermore note that this document does not specify a particular method for authentication, it simply indicates that security tokens MAY be bound to messages.

A claim can be either endorsed or unendorsed by a trusted authority. A set of endorsed claims is usually represented as a signed security token that is digitally signed or encrypted by the authority. An X.509 certificate, claiming the binding between one's identity and public key, is an example of a signed security token. An endorsed claim can also be represented as a reference to an authority so that the receiver can "pull" the claim from the referenced authority.

An unendorsed claim can be trusted if there is a trust relationship between the sender and the receiver. For example, the unendorsed claim that the sender is Bob is sufficient for a certain receiver to believe that the sender is in fact Bob, if the sender and the receiver use a trusted connection and there is an out-of-band trust relationship between them.

One special type of unendorsed claim is Proof-of-Possession. Such a claim proves that the sender has a particular piece of knowledge that is verifiable by, appropriate roles. For example, a username/password is a security token with this type of claim. A Proof-of-Possession claim is sometimes combined with other security tokens to prove the claims of the sender. Note that a digital signature used for message integrity can also be used as a Proof-of-Possession claim, although in this specification does not consider such a digital signature as a type of security token.

It should be noted that this security model, by itself, is subject to multiple security attacks. Refer to the Security Considerations section for additional details.

3.2 Message Protection

Protecting the message content from being intercepted (confidentiality) or illegally modified (integrity) are primary security concerns. This specification provides a means to protect a message by encrypting and/or digitally signing a body, a header, an attachment, or any combination of them (or parts of them).

Message integrity is provided by leveraging XML Signature in conjunction with security tokens to ensure that messages are transmitted without modifications. The integrity mechanisms are designed to support multiple signatures, potentially by multiple roles, and to be extensible to support additional signature formats.

Message confidentiality leverages XML Encryption in conjunction with security tokens to keep portions of a SOAP message confidential. The encryption mechanisms are designed to support additional encryption processes and operations by multiple roles.

3.3 Invalid or Missing Claims

Deleted: Missing or Inappropriate

The message receiver SHOULD reject a message with signature determined to be invalid, missing or unauthorized claims as it is an unauthorized (or malformed) message. This specification provides a flexible way for the message sender to make a claim about the security properties by associating zero or more security tokens with the message. An example of a security claim is the identity of the sender; the sender can claim that he is Bob, known as an employee of some company, and therefore he has the right to send the message.

Deleted: inappropriate

3.4 Example

The following example illustrates a message with a username security token:

```
(001) <?xml version="1.0" encoding="utf-8"?>
(002) <S:Envelope xmlns:S="http://www.w3.org/2001/12/soap-envelope"
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
(003)   <S:Header>
(004)      <wsse:Security
             xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/xx/secext">
(005)         <wsse:UsernameToken wsu:Id="MyID">
(006)             <wsse:Username>Zoe</wsse:Username>
(007)             <wsse:Nonce>FKJh...</wsse:Nonce>
(008)             <wsu:Created>2001-10-13T09:00:00Z</wsu:Created>
(009)         </wsse:UsernameToken>
(010)         <ds:Signature>
(011)            <ds:SignedInfo>
(012)               <ds:CanonicalizationMethod
                        Algorithm=
                          "http://www.w3.org/2001/10/xml-exc-c14n#"/>
(013)               <ds:SignatureMethod
                        Algorithm=
                        "http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
(014)               <ds:Reference URI="#MsgBody">
(015)                  <ds:DigestMethod
                          Algorithm=
                        "http://www.w3.org/2000/09/xmldsig#sha1"/>
(016)                  <ds:DigestValue>LyLsF0Pi4wPU...</ds:DigestValue>
(017)               </ds:Reference>
(018)            </ds:SignedInfo>
(019)            <ds:SignatureValue>DJbchm5gK...</ds:SignatureValue>
(020)            <ds:KeyInfo>
(021)                <wsse:SecurityTokenReference>
(022)                 <wsse:Reference URI="#MyID"/>
(023)                </wsse:SecurityTokenReference>
(024)            </ds:KeyInfo>
(025)         </ds:Signature>
(026)      </wsse:Security>
(027)   </S:Header>
(028)   <S:Body wsu:Id="MsgBody">
(029)     <tru:StockSymbol xmlns:tru="http://fabrikam123.com/payloads">
              QQQ
          </tru:StockSymbol>
(030)   </S:Body>
(031) </S:Envelope>
```

Formatted: German (Germany)

The first two lines start the SOAP envelope. Line (003) begins the headers that are associated with this SOAP message.

Line (004) starts the `<Security>` header that is defined in this specification. This header contains security information for an intended receiver. This element continues until line (026)

Lines (006) to (009) specify a security token that is associated with the message. In this case, it defines *username* of the client using the `<UsernameToken>`. Note that here that the assumption is that the service knows the password – in other words, it is a shared secret and the <Nonce> and <Created> are used to generate the key

Formatted: Font: Arial

Formatted: Font: Arial

Deleted: .

Lines (010) to (025) specify a digital signature. This signature ensures the integrity of the signed elements (that they aren't modified). The signature uses the XML Signature specification. In this example, the signature is based on a key generated from the users' password; typically stronger signing mechanisms would be used (see the Extended Example later in this document).

Lines (011) to (018) describe the digital signature. Line (012) specifies how to canonicalize (normalize) the data that is being signed.

Lines (014) to (017) select the elements that are signed and how to digest them. Specifically, line (014) indicates that the `<S:Body>` element is signed. In this example only the message body is signed; typically all critical elements of the message are included in the signature (see the Extended Example below).

Line (019) specifies the signature value of the canonicalized form of the data that is being signed as defined in the XML Signature specification.

Lines (020) to (024) provide a *hint* as to where to find the security token associated with this signature. Specifically, lines (021) to (023) indicate that the security token can be found at (pulled from) the specified URL.

Lines (028) to (030) contain the *body* (payload) of the SOAP message.

4 ID References

There are many motivations for referencing other message elements such a signature references or correlating signatures to security tokens. However, because arbitrary ID attributes require the schemas to be available and processed, ID attributes which can be referenced in a signature are restricted to the following list:

- ID attributes from XML Signature
- ID attributes from XML Encryption
- wsu:Id global attribute described below

In addition, when signing a part of an envelope such as the body, it is RECOMMENDED that an ID reference is used instead of a more general transformation, especially XPath. This is to simplify processing.

4.1 Id Attribute

There are many situations where elements within SOAP messages need to be referenced. For example, when signing a SOAP message, selected elements are included in the signature. XML Schema Part 2 provides several built-in data types that may be used for identifying and referencing elements, but their use requires that consumers of the SOAP message either to have or be able to obtain the schemas where the identity or reference mechanisms are defined. In some circumstances, for example, intermediaries, this can be problematic and not desirable.

Consequently a mechanism is required for identifying and referencing elements, based on the SOAP foundation, that does not rely upon complete schema knowledge of the context in which an element is used. This functionality can be integrated into SOAP processors so that elements can be identified and referred to without dynamic schema discovery and processing.

This section specifies a namespace-qualified global attribute for identifying an element which can be applied to any element that either allows arbitrary attributes or specifically allows a particular attribute.

Deleted: we

Deleted: this

4.2 Id Schema

To simplify the processing for intermediaries and receivers, a common attribute is defined for identifying an element. This attribute utilizes the XML Schema ID type and specifies a common attribute for indicating this information for elements.

The syntax for this attribute is as follows:

```
<anyElement wsu:Id="...">...</anyElement>
```

The following describes the attribute illustrated above:

.../@wsu:Id

This attribute, defined as type `xsd:ID`, provides a well-known attribute for specifying the local ID of an element.

Two `wsu:Id` attributes within an XML document MUST NOT have the same value. Implementations MAY rely on XML Schema validation to provide rudimentary enforcement for intra-document uniqueness. However, applications SHOULD NOT rely on schema validation alone to enforce uniqueness.

This specification does not specify how this arrtibute will be used and it is expected that other specifications MAY add additional semantics (or restrictions) for their usage of this attribute.

Deleted:

The following example illustrates use of this attribute to identify an element:

```
<x:myElement wsu:Id="ID1" xmlns:x="..."
          xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/xx/utility"/>
```

Conformant processors that do support XML Schema MUST treat this attribute as if it was defined using a global attribute declaration.

Conformant processors that do not support XML Schema or DTDs are strongly encouraged to treat this attribute information item as if its PSVI has a [type definition] which {target namespace} is "`http://www.w3.org/2001/XMLSchema`" and which {name} is "Id." Specifically, implementations MAY support the value of the `wsu:Id` as the valid identifier for use as an XPointer shorthand pointer.

Deleted: ose

Deleted: whose

5 Security Header

The <wsse:Security> header block provides a mechanism for attaching security-related information targeted at a specific receiver (SOAP role). This MAY be either the ultimate receiver of the message or an intermediary. Consequently, this header block MAY be present multiple times in a SOAP message. An intermediary on the message path MAY add one or more new sub-elements to an existing <wsse:Security> header block if they are targeted for the same SOAP node or it MAY add one or more new headers for additional targets.

As stated, a message MAY have multiple <wsse:Security> header blocks if they are targeted for separate receivers. However, only one <wsse:Security> header block can omit the S:role attribute and no two <wsse:Security> header blocks can have the same value for S:role. Message security information targeted for different receivers MUST appear in different <wsse:Security> header blocks. The <wsse:Security> header block without a specified S:role can be consumed by anyone, but MUST NOT be removed prior to the final destination or endpoint.

As elements are added to the <wsse:Security> header block, they SHOULD be prepended to the existing elements. As such, the <wsse:Security> header block represents the signing and encryption steps the message sender took to create the message. This prepending rule ensures that the receiving application MAY process sub-elements in the order they appear in the <wsse:Security> header block, because there will be no forward dependency among the sub-elements. Note that this specification does not impose any specific order of processing the sub-elements. The receiving application can use whatever policy is needed.

Deleted: should

When a sub-element refers to a key carried in another sub-element (for example, a signature sub-element that refers to a binary security token sub-element that contains the X.509 certificate used for the signature), the key-bearing security token SHOULD be prepended to the key-using sub-element being added, so that the key material appears before the key-using sub-element.

Deleted: subsequent

The following illustrates the syntax of this header:

```
<S:Envelope>
    <S:Header>
            ...
        <wsse:Security S:role="..." S:mustUnderstand="...">
            ...
        </wsse:Security>
            ...
    </S:Header>
    ...
</S:Envelope>
```

The following describes the attributes and elements listed in the example above:

/wsse:Security

This is the header block for passing security-related message information to a receiver.

/ wsse:Security/@S:role

This attribute allows a specific SOAP role to be identified. This attribute is optional; however, no two instances of the header block may omit an role or specify the same role.

/wsse:Security/{any}

This is an extensibility mechanism to allow different (extensible) types of security information, based on a schema, to be passed.

/wsse:Security/@{any}

This is an extensibility mechanism to allow additional attributes, based on schemas, to be added to the header.

All compliant implementations MUST be able to process a `<wsse:Security>` element.

The next few sections outline elements that are expected to be used within the `<wsse:Security>` header.

6 Security Tokens

This chapter discusses different types of security tokens and how they are attached to messages.

6.1 User Name Tokens

6.1.1 Usernames and Passwords

The <wsse:UsernameToken> element is introduced as a way of proving a username and optional password information. This element is optionally included in the <wsse:Security> header.

Within this element, a <wsse:Password> element can be specified. The password has an associated type – either wsse:PasswordText or wsse:PasswordDigest. The wsse:PasswordText is not limited to only the actual password. Any password equivalent such as a derived password or S/KEY (one time password) can be used.

The wsse:PasswordDigest is defined as a *"base64-encoded SHA1 hash value of the UTF8-encoded password".* However, unless this digested password is sent on a secured channel, the digest offers no real additional security than wsse:PasswordText.

To address this issue, two additional optional elements are introduced in the <wsse:UsernameToken>: <wsse:Nonce> and <wsu:Created>. If either of these is present, they are included in the digest value as follows:

```
Password_digest = SHA1 ( nonce + created + password )
```

That is, concatenate the nonce, creation timestamp, and the password (or shared secret or password equivalent) and include the digest of the combination. This helps obscure the password and offers a basis for preventing replay attacks. It is RECOMMENDED that timestamps and nonces be cached for a given period of time, as a guideline a value of five minutes can be used as a minimum to detect replays, and that timestamps older than that given period of time set be rejected.

Deleted: minimum

Deleted: five minutes

Note that the nonce is hashed using the octet sequence of its decoded value while the timestamp is hashed using the octet sequence of its UTF8 encoding as specified in the contents of the element.

Note that password digests SHOULD NOT be used unless the plain text password, secret, or password-equivalent is available to both the requestor and the receiver.

The following illustrates the syntax of this element:

```
<wsse:UsernameToken wsu:Id="...">
    <wsse:Username>...</wsse:Username>
    <wsse:Password Type="...">...</wsse:Password>
    <wsse:Nonce EncodingType="...">...</wsse:Nonce>
    <wsu:Created>...</wsu:Created>
</wsse:UsernameToken>
```

Formatted: English (U.S.)

The following describes the attributes and elements listed in the example above:

/wsse:UsernameToken

This element is used for sending basic authentication information.

/wsse:UsernameToken/@wsu:Id

A string label for this security token.

/wsse:UsernameToken/Username

This required element specifies the username of the authenticating party.

/wsse:UsernameToken/Username/@{any}

This is an extensibility mechanism to allow additional attributes, based on schemas, to be added to the header.

/wsse:UsernameToken/Password

This optional element provides password information. It is RECOMMENDED that this element only be passed when a secure transport is being used.

/wsse:UsernameToken/Password/@Type

This optional attribute specifies the type of password being provided. The following table identifies the pre-defined types:

Value	Description
wsse:PasswordText (default)	The actual password for the username or derived password or S/KEY .
wsse:PasswordDigest	The digest of the password for the username using the algorithm described above.

/wsse:UsernameToken/Password/@{any}

This is an extensibility mechanism to allow additional attributes, based on schemas, to be added to the header.

/wsse:UsernameToken//wsse:Nonce

This optional element specifies a cryptographically random nonce.

/wsse:UsernameToken//wsse:Nonce/@EncodingType

This optional attribute specifies the encoding type of the nonce (see definition of `<wsse:BinarySecurityToken>` for valid values). If this attribute isn't specified then the default of Base64 encoding is used.

/wsse:UsernameToken//wsu:Created

This optional element which specifies a timestamp.

/wsse:UsernameToken/{any}

This is an extensibility mechanism to allow different (extensible) types of security information, based on a schema, to be passed.

/wsse:UsernameToken/@{any}

This is an extensibility mechanism to allow additional attributes, based on schemas, to be added to the header.

All compliant implementations MUST be able to process a `<wsse:UsernameToken>` element.

The following illustrates the use of this element (note that in this example the password is sent in clear text and the message should therefore be sent over a confidential channel:

Deleted: secure

```
<S:Envelope xmlns:S="http://www.w3.org/2001/12/soap-envelope"
            xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/xx/secext">
    <S:Header>
            ...
        <wsse:Security>
            <wsse:UsernameToken>
                <wsse:Username>Zoe</wsse:Username>
                <wsse:Password>ILoveDogs</wsse:Password>
            </wsse:UsernameToken>
        </wsse:Security>
            ...
    </S:Header>
    ...
</S:Envelope>
```

The following example illustrates a hashed password using both a nonce and a timestamp with the password hashed:

```
<S:Envelope xmlns:S="http://www.w3.org/2001/12/soap-envelope"
            xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/xx/secext">
    <S:Header>
            ...
        <wsse:Security>
          <wsse:UsernameToken
            xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/xx/secext"
            xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/xx/utility">
            <wsse:Username>NNK</wsse:Username>
            <wsse:Password Type="wsse:PasswordDigest">
                FEdR...</wsse:Password>
            <wsse:Nonce>FKJh...</wsse:Nonce>
            <wsu:Created>2001-10-13T09:00:00Z </wsu:Created>
          </wsse:UsernameToken>
        </wsse:Security>
            ...
    </S:Header>
    ...
</S:Envelope>
```

Formatted: German (Germany)

6.2 Binary Security Tokens

6.2.1 Attaching Security Tokens

This specification defines the `<wsse:Security>` header as a mechanism for conveying security information with and about a SOAP message. This header is, by design, extensible to support many types of security information.

6.2.2 Processing Rules

This specification describes the processing rules for using and processing XML Signature and XML Encryption. These rules MUST be followed when using any type of security token including XML-based tokens. Note that this does NOT mean that binary security tokens MUST be signed or encrypted – only that if signature or encryption is used in conjunction with binary security tokens, they MUST be used in a way that conforms to the processing rules defined by this specification.

6.2.3 Encoding Binary Security Tokens

Binary security tokens (e.g., X.509 certificates and Kerberos tickets) or other non-XML formats require a special encoding format for inclusion. This section describes a basic framework for using binary security tokens. Subsequent specifications describe rules and processes for specific binary security token formats.

The `<wsse:BinarySecurityToken>` element defines two attributes that are used to interpret it. The `ValueType` attribute indicates what the security token is, for example, a Kerberos ticket. The `EncodingType` tells how the security token is encoded, for example `Base64Binary`.

Deleted: A binary security token has

The following is an overview of the syntax:

Deleted: The `<wsse:BinarySecurityToken>` element defines a security token that is binary encoded. The encoding is specified using the `EncodingType` attribute, and the value type and space are specified using the `ValueType` attribute. ¶

```
<wsse:BinarySecurityToken wsu:Id=...
                          EncodingType=...
                          ValueType=.../>
```

The following describes the attributes and elements listed in the example above:

/wsse:BinarySecurityToken

This element is used to include a binary-encoded security token.

/wsse:BinarySecurityToken/@wsu:Id

An optional string label for this security token.

/wsse:BinarySecurityToken/@ValueType

The `ValueType` attribute is used to indicate the "value space" of the encoded binary data (e.g. an X.509 certificate). The `ValueType` attribute allows a qualified name that defines the value type and space of the encoded binary data. This attribute is extensible using XML namespaces.

/wsse:BinarySecurityToken/@EncodingType

The `EncodingType` attribute is used to indicate, using a QName, the encoding format of the binary data (e.g., `wsse:Base64Binary`). A new attribute is introduced, as there are currently issues that make derivations of mixed simple and complex types difficult within XML Schema. The `EncodingType` attribute is interpreted to indicate the encoding format of the element. The following encoding formats are pre-defined:

QName	Description
wsse:Base64Binary	XML Schema base 64 encoding
wsse:HexBinary	XML Schema hex encoding

/wsse:BinarySecurityToken/@{any}

This is an extensibility mechanism to allow additional attributes, based on schemas, to be added.

All compliant implementations MUST be able to support a `<wsse:BinarySecurityToken>` element.

Deleted: process

When a `<wsse:BinarySecurityToken>` is used in validating a signature—that is, it is referenced from a `<ds:Signature>` element—care should be taken so that the canonicalization algorithm (e.g., Exclusive XML Canonicalization) does not allow unauthorized replacement of namespace prefixes of the QNames used in the attribute or element values. In particular, it is RECOMMENDED that these namespace prefixes are declared within the `<wsse:BinarySecurityToken>` element if this token does not carry the validating key (and consequently it is not cryptographically bound to the signature). For example, if we wanted to sign the previous example, we need to include the consumed namespace definitions.

Deleted: signing

Deleted: signing

In the following example, a custom `ValueType` is used. Consequently, the namespace definition for this `ValueType` is included in the `<wsse:BinarySecurityToken>` element. Note that the definition of `wsse` is also included as it is used for the encoding type and the element.

```
<wsse:BinarySecurityToken
        xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/xx/secext"
        wsu:Id="myToken"
        ValueType="x:MyType" xmlns:x="http://www.fabrikam123.com/x"
        EncodingType="wsse:Base64Binary">
    MIIEZzCCA9CgAwIBAgIQEmtJZc0...
</wsse:BinarySecurityToken>
```

6.3 XML Tokens

This section presents the basic principles and framework for using XML-based security tokens. Subsequent specifications describe rules and processes for specific XML-based security token formats.

Deleted: als

6.3.1 Attaching Security Tokens

This specification defines the `<wsse:Security>` header as a mechanism for conveying security information with and about a SOAP message. This header is, by design, extensible to support many types of security information.

For security tokens based on XML, the extensibility of the `<wsse:Security>` header allows for these security tokens to be directly inserted into the header.

6.3.2 Identifying and Referencing Security Tokens

This specification also defines multiple mechanisms for identifying and referencing security tokens using the *wsu:Id* attribute and the `<wsse:SecurityTokenReference>` element (as well as some additional mechanisms). Where possible, the *wsu:Id* attribute SHOULD be used to reference XML-based tokens. However, specific extensions MAY be made to the `wsse:SecurityTokenReference>` element.

6.3.3 Subject Confirmation

This specification does not dictate if and how subject confirmation must be done, however, it does define how signatures can be used and associated with security tokens (by referencing them in the signature) as a form of Proof-of-Posession..

Deleted: towards this end

6.3.4 Processing Rules

This specification describes the processing rules for using and processing XML Signature and XML Encryption. These rules MUST be followed when using any type of security token including XML-based tokens. Note that this does NOT mean that XML-based tokens MUST be signed or encrypted – only that if signature or encryption is used in conjunction with XML-based tokens, they MUST be used in a way that conforms to the processing rules defined by this specification.

7 Token References

This chapter discusses and defines mechanisms for referencing security tokens.

7.1 SecurityTokenReference Element

A security token conveys a set of claims. Sometimes these claims reside somewhere else and need to be "pulled" by the receiving application. The `<wsse:SecurityTokenReference>` element provides an extensible mechanism for referencing security tokens.

The following illustrates the syntax of this element:

```
<wsse:SecurityTokenReference wsu:Id="...">
    ...
</wsse:SecurityTokenReference>
```

The following describes the elements defined above:

/SecurityTokenReference

This element provides a reference to a security token.

/SecurityTokenReference/@wsu:Id

A string label for this security token reference.

/SecurityTokenReference/{any}

This is an extensibility mechanism to allow different (extensible) types of security references, based on a schema, to be passed.

/SecurityTokenReference/@{any}

This is an extensibility mechanism to allow additional attributes, based on schemas, to be added to the header.

The following illustrates the use of this element:

```
<wsse:SecurityTokenReference
          xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/xx/secext">
   <wsse:Reference
             URI="http://www.fabrikam123.com/tokens/Zoe#X509token"/>
</wsse:SecurityTokenReference>
```

All compliant implementations MUST be able to process a `<wsse:SecurityTokenReference>` element.

This element can also be used as a direct child element of `<ds:KeyInfo>` to indicate a hint to retrieve the key information from a security token placed somewhere else. In particular, it is RECOMMENDED, when using XML Signature and XML Encryption, that a `<wsse:SecurityTokenReference>` element be placed inside a `<ds:KeyInfo>` to reference the security token used for the signature or encryption.

7.2 Direct References

The `<wsse:Reference>` element provides an extensible mechanism for directly referencing security tokens using URIs.

The following illustrates the syntax of this element:

```
<wsse:SecurityTokenReference wsu:Id="...">
    <wsse:Reference URI="..." ValueType="..."/>
</wsse:SecurityTokenReference>
```

The following describes the elements defined above:

/SecurityTokenReference/Reference

This element is used to identify a URI location for locating a security token.

/SecurityTokenReference/Reference/@URI

This optional attribute specifies a URI for where to find a security token.

/SecurityTokenReference/Reference/@ValueType

This required attribute specifies a QName that is used to identify the *type* of token being referenced (see `<wsse:BinarySecurityToken>`). This specification does not define any processing rules around the usage of this attribute, however, specification for individual token types MAY define specific processing rules and semantics around the value of the URI and how it is interpreted. If this attribute is not present, the URI is processed as a normal URI.

The following illustrates the use of this element:

```
<wsse:SecurityTokenReference
          xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/xx/secext">
   <wsse:Reference
             URI="http://www.fabrikam123.com/tokens/Zoe#X509token"/>
</wsse:SecurityTokenReference>
```

7.3 Key Identifiers

If a direct reference is not possible, then it is RECOMMENDED to use a key identifier to specify/reference a security token instead of a key name. The `<wsse:KeyIdentifier>` element is placed in the `<wsse:SecurityTokenReference>` element to reference a token using an identifier. This element SHOULD be used for all key identifiers.

The processing model assumes that the key identifier for a security token is constant. Consequently, processing a key identifier is simply looking for a security token whose key identifier matches a given specified consant.

Deleted: the

The following is an overview of the syntax:

```
<wsse:SecurityTokenReference>
   <wsse:KeyIdentifier wsu:Id="..."
                       ValueType="..."
                       EncodingType="...">
      ...
   </wsse:KeyIdentifier>
</wsse:SecurityTokenReference>
```

The following describes the attributes and elements listed in the example above:

/SecurityTokenReference /KeyIdentifier

This element is used to include a binary-encoded key identifier.

/SecurityTokenReference/KeyIdentifier/@wsu:Id

An optional string label for this identifier.

/SecurityTokenReference/KeyIdentifier/@ValueType

The `ValueType` attribute is used to optionally indicate the type of token with the specified identifier. If specified, this is a *hint* to the receiver. Any value specified for binary security tokens, or any XML token element QName can be specified here. If this attribute isn't specified, then the identifier applies to any type of token.

/SecurityTokenReference/KeyIdentifier/@EncodingType

The optional `EncodingType` attribute is used to indicate, using a QName, the encoding format of the binary data (e.g., `wsse:Base64Binary`). The base values defined in this specification are used:

QName	Description
wsse:Base64Binary	XML Schema base 64 encoding (default)
wsse:HexBinary	XML Schema hex encoding

/SecurityTokenReference/KeyIdentifier/@{any}

This is an extensibility mechanism to allow additional attributes, based on schemas, to be added.

7.4 ds:KeyInfo

The `<ds:KeyInfo>` element (from XML Signature) can be used for carrying the key information and is allowed for different key types and for future extensibility. However, in this specification, the use of `<wsse:BinarySecurityToken>` is the RECOMMENDED way to carry key material if the key type contains binary data.

The following example illustrates use of this element to fetch a named key:

```
<ds:KeyInfo Id="..." xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:KeyName>CN=Hiroshi Maruyama, C=JP</ds:KeyName>
</ds:KeyInfo>
```

7.5 Key Names

It is strongly RECOMMEND to use key identifiers. However, if key names are used, then it is strongly RECOMMENDED that `<ds:KeyName>` elements conform to the attribute names in section 2.3 of RFC 2253 (this is recommended by XML Signature for `<X509SubjectName>`) for interoperability.

Deleted: ,

Deleted: h

Additionally, defined are the following convention for e-mail addresses, which SHOULD conform to RFC 822:

```
     EmailAddress=ckaler@microsoft.com
```

7.6 Token Reference Lookup Processing Order

There are a number of mechanisms described in XML Signature and this specification for referencing security tokens. To resolve possible ambiguities, the following processing order SHOULD be used:

1. Resolve any `<wsse:Reference>` elements (specified within `<wsse:SecurityTokenReference>`).
2. Resolve any `<wsse:KeyIdentifier>` elements (specified within `<wsse:SecurityTokenReference>`).
3. Resolve any `<ds:KeyName>` elements.
4. Resolve any other `<ds:KeyInfo>` elements.

8 Signatures

Message senders may want to enable message receivers to determine whether a message was altered in transit and to verify that a message was sent by the possessor of a particular security token.

When an XML Signature is used in conjunction with the `<wsse:SecurityTokenReference>` element, the security token of a message signer may be correlated and a mapping made between the claims of the security token and the message as evaluated by the application.

Because of the mutability of some SOAP headers, senders SHOULD NOT use the *Enveloped Signature Transform* defined in XML Signature. Instead, messages SHOULD explicitly include the desired elements to be signed. Similarly, senders SHOULD NOT use the *Enveloping Signature* defined in XML Signature.

This specification allows for multiple signatures and signature formats to be attached to a message, each referencing different, even overlapping, parts of the message. This is important for many distributed applications where messages flow through multiple processing stages. For example, a sender may submit an order that contains an orderID header. The sender signs the orderID header and the body of the request (the contents of the order). When this is received by the order processing sub-system, it may insert a shippingID into the header. The order sub-system would then sign, at a minimum, the orderID and the shippingID, and possibly the body as well. Then when this order is processed and shipped by the shipping department, a shippedInfo header might be appended. The shipping department would sign, at a minimum, the shippedInfo and the shippingID and possibly the body and forward the message to the billing department for processing. The billing department can verify the signatures and determine a valid chain of trust for the order, as well as who did what.

All compliant implementations MUST be able to support the XML Signature standard.

8.1 Algorithms

This specification builds on XML Signature and therefore has the same algorithm requirements as those specified in the XML Signature specification.

The following table outlines additional algorithms that are strongly RECOMMENDED by this specification:

Algorithm Type	**Algorithm**	**Algorithm URI**
Canonicalization	Exclusive XML Canonicalization	http://www.w3.org/2001/10/xml-exc-c14n#
Transformations	XML Decryption Transformation	http://www.w3.org/2001/04/decrypt#

The Exclusive XML Canonicalization algorithm addresses the pitfalls of general canonicalization that can occur from *leaky* namespaces with pre-existing signatures.

Finally, if a sender wishes to sign a message before encryption, they should use the Decryption Transformation for XML Signature.

8.2 Signing Messages

The `<wsse:Security>` header block is used to carry a signature compliant with the XML Signature specification within a SOAP Envelope for the purpose of signing one or more elements in the SOAP Envelope. Multiple signature entries MAY be added into a single SOAP Envelope within the `<wsse:Security>` header block. Senders should take care to sign all important elements of the message, but care must be taken in creating a signing policy that will not to sign parts of the message that might legitimately be altered in transit.

SOAP applications MUST satisfy the following conditions:

1. The application MUST be capable of processing the required elements defined in the XML Signature specification.
2. To add a signature to a `<wsse:Security>` header block, a `<ds:Signature>` element conforming to the XML Signature specification SHOULD be prepended to the existing content of the `<wsse:Security>` header block. That is, the new information would be before (prepended to) the old. All the `<ds:Reference>` elements contained in the signature SHOULD refer to a resource within the enclosing SOAP envelope, or in an attachment.

XPath filtering can be used to specify objects to be signed, as described in the XML Signature specification. However, since the SOAP message exchange model allows intermediate applications to modify the Envelope (add or delete a header block; for example), XPath filtering does not always result in the same objects after message delivery. Care should be taken in using XPath filtering so that there is no subsequent validation failure due to such modifications.

The problem of modification by intermediaries is applicable to more than just XPath processing. Digital signatures, because of canonicalization and digests, present particularly fragile examples of such relationships. If overall message processing is to remain robust, intermediaries must exercise care that their transformations do not occur within the scope of a digitally signed component.

Due to security concerns with namespaces, this specification strongly RECOMMENDS the use of the "Exclusive XML Canonicalization" algorithm or another canonicalization algorithm that provides equivalent or greater protection.

For processing efficiency it is RECOMMENDED to have the signature added and then the security token pre-pended so that a processor can read and cache the token before it is used.

8.3 Signature Validation

The validation of a `<ds:Signature>` element inside an `<wsse:Security>` header block fails if

Deleted: ntry

1. the syntax of the content of the entry does not conform to this specification, or
2. the validation of the signature contained in the entry fails according to the core validation of the XML Signature specification, or
3. the application applying its own validation policy rejects the message for some reason (e.g., the signature is created by an untrusted key – verifying the previous two steps only performs cryptographic verification of the signature).

If the verification of the signature entry fails, applications MAY report the failure to the sender using the fault codes defined in Section 12 Error Handling.

Deleted: Section 6

Deleted: .

8.4 Example

The following sample message illustrates the use of integrity and security tokens. For this example, we sign only the message body.

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<S:Envelope xmlns:S="http://www.w3.org/2001/12/soap-envelope"
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
            xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/xx/secext"
            xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
   <S:Header>
      <wsse:Security>
         <wsse:BinarySecurityToken
                     ValueType="wsse:X509v3"
                     EncodingType="wsse:Base64Binary"
                     wsu:Id="X509Token">
                  MIIEZzCCA9CgAwIBAgIQEmtJZc0rqrKh5i...
         </wsse:BinarySecurityToken>
         <ds:Signature>
            <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="#myBody">
                  <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>EULddytSo1...</ds:DigestValue>
               </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>
              BL8jdfToEb1l/vXcMZNNjPOV...
            </ds:SignatureValue>
            <ds:KeyInfo>
                <wsse:SecurityTokenReference>
                    <wsse:Reference URI="#X509Token"/>
                </wsse:SecurityTokenReference>
            </ds:KeyInfo>
         </ds:Signature>
      </wsse:Security>
   </S:Header>
   <S:Body wsu:Id="myBody">
      <tru:StockSymbol xmlns:tru="http://www.fabrikam123.com/payloads">
        QQQ
      </tru:StockSymbol>
   </S:Body>
</S:Envelope>
```

Formatted: English (U.S.)

9 Encryption

This specification allows encryption of any combination of body blocks, header blocks, any of these sub-structures, and attachments by either a common symmetric key shared by the sender and the receiver or a key carried in the message in an encrypted form.

In order to allow this flexibility, this specification leverages the XML Encryption standard. Specifically, described is how three elements (listed below and defined in XML Encryption) can be used within the `<wsse:Security>` header block. When a sender or an intermediary encrypts portion(s) of a SOAP message using XML Encryption they MUST add a sub-element to the `<wsse:Security>` header block. Furthermore, the encrypting party MUST prepend the sub-element into the `<wsse:Security>` header block for the targeted receiver that is expected to decrypt these encrypted portions. The combined process of encrypting portion(s) of a message and adding one of these sub-elements referring to the encrypted portion(s) is called an *encryption step* hereafter. The sub-element should have enough information for the receiver to identify which portions of the message are to be decrypted by the receiver.

Deleted: will

All compliant implementations MUST be able to support the XML Encryption standard.

9.1 xenc:ReferenceList

When encrypting elements or element contents within a SOAP envelope, the `<xenc:ReferenceList>` element from XML Encryption MAY be used to create a manifest of encrypted portion(s), which are expressed as `<xenc:EncryptedData>` elements within the envelope. An element or element content to be encrypted by this encryption step MUST be replaced by a corresponding `<xenc:EncryptedData>` according to XML Encryption. All the `<xenc:EncryptedData>` elements created by this encryption step SHOULD be listed in `<xenc:DataReference>` elements inside an `<xenc:ReferenceList>` element.

Although in XML Encryption, `<xenc:ReferenceList>` is originally designed to be used within an `<xenc:EncryptedKey>` element (which implies that all the referenced `<xenc:EncryptedData>` elements are encrypted by the same key), this specification allows that `<xenc:EncryptedData>` elements referenced by the same `<xenc:ReferenceList>` MAY be encrypted by different keys. Each encryption key can be specified in `<ds:KeyInfo>` within individual `<xenc:EncryptedData>`.

A typical situation where the `<xenc:ReferenceList>` sub-element is useful is that the sender and the receiver use a shared secret key. The following illustrates the use of this sub-element:

```
<S:Envelope
   xmlns:S="http://www.w3.org/2001/12/soap-envelope"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/xx/secext"
   xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
    <S:Header>
        <wsse:Security>
            <xenc:ReferenceList>
                <xenc:DataReference URI="#bodyID"/>
            </xenc:ReferenceList>
        </wsse:Security>
    </S:Header>
    <S:Body>
        <xenc:EncryptedData Id="bodyID">
          <ds:KeyInfo>
            <ds:KeyName>CN=Hiroshi Maruyama, C=JP</ds:KeyName>
          </ds:KeyInfo>
          <xenc:CipherData>
            <xenc:CipherValue>...</xenc:CipherValue>
          </xenc:CipherData>
        </xenc:EncryptedData>
    </S:Body>
</S:Envelope>
```

9.2 xenc:EncryptedKey

When the encryption step involves encrypting elements or element contents within a SOAP envelope with a key, which is in turn to be encrypted by the recipient's key and embedded in the message, `<xenc:EncryptedKey>` MAY be used for carrying such an encrypted key. This sub-element SHOULD have a manifest, that is, an `<xenc:ReferenceList>` element, in order for the recipient to know the portions to be decrypted with this key (if any exist). An element or element content to be encrypted by this encryption step MUST be replaced by a corresponding `<xenc:EncryptedData>` according to XML Encryption. All the `<xenc:EncryptedData>` elements created by this encryption step SHOULD be listed in the `<xenc:ReferenceList>` element inside this sub-element.

This construct is useful when encryption is done by a randomly generated symmetric key that is in turn encrypted by the recipient's public key. The following illustrates the use of this element:

```
<S:Envelope
   xmlns:S="http://www.w3.org/2001/12/soap-envelope"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/xx/secext"
   xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
    <S:Header>
        <wsse:Security>
            <xenc:EncryptedKey>
               <xenc:EncryptionMethod Algorithm="..."/>
               <wsse:KeyIdentifier EncodingType="wsse:Base64Binary"
                     ValueType="wsse:X509v3">MIGfMa0GCSq...
               </wsse:KeyIdentifier>
               <xenc:CipherData>
                   <xenc:CipherValue>...</xenc:CipherValue>
               </xenc:CipherData>
               <xenc:ReferenceList>
                  <xenc:DataReference URI="#bodyID"/>
               </xenc:ReferenceList>
            </xenc:EncryptedKey>
        </wsse:Security>
    </S:Header>
    <S:Body>
        <xenc:EncryptedData Id="bodyID">
            <xenc:CipherData>
              <xenc:CipherValue>...</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </S:Body>
</S:Envelope>
```

Deleted: `<ds:KeyInfo>¶`

`<ds:KeyName>CN=Hiroshi Maruyama, C=JP</ds:KeyName>¶`
`</ds:KeyInfo>`

While XML Encryption specifies that `<xenc:EncryptedKey>` elements MAY be specified in `<xenc:EncryptedData>` elements, this specification strongly RECOMMENDS that `<xenc:EncryptedKey>` elements be placed in the `<wsse:Security>` header.

9.3 xenc:EncryptedData

In some cases security-related information is provided in a purely encrypted form or non-XML attachments MAY be encrypted. The `<xenc:EncryptedData>` element from XML Encryption can be used for these scenarios. For each part of the encrypted attachment, one encryption step is needed; that is, for each attachment to be encrypted, one <xenc:EncryptedData> sub-element MUST be added with the following rules (note that steps 2-4 applies only if MIME types are being used for attachments).

1. The contents of the attachment MUST be replaced by the encrypted octet string.
2. The replaced MIME part MUST have the media type application/octet-stream.
3. The original media type of the attachment MUST be declared in the MimeType attribute of the <xenc:EncryptedData> element.
4. The encrypted MIME part MUST be referenced by an <xenc:CipherReference> element with a URI that points to the MIME part with cid: as the scheme component of the URI.

The following illustrates the use of this element to indicate an encrypted attachment:

```
<S:Envelope
   xmlns:S="http://www.w3.org/2001/12/soap-envelope"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/xx/secext"
   xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
    <S:Header>
        <wsse:Security>
            <xenc:EncryptedData MimeType="image/png">
               <xenc:EncryptionMethod Algorithm="foo:bar"/>
               <wsse:KeyIdentifier EncodingType="wsse:Base64Binary"
                     ValueType="wsse:X509v3">MIGfMa0GCSq ...
               </wsse:KeyIdentifier>
               <xenc:CipherData>
                   <xenc:CipherReference URI="cid:image"/>
               </xenc:CipherData>
            </xenc:EncryptedData>
        </wsse:Security>
    </S:Header>
    <S:Body> </S:Body>
</S:Envelope>
```

Deleted: <ds:KeyInfo>¶

<ds:KeyName>CN=Hiroshi Maruyama, C=JP</ds:KeyName>¶
</ds:KeyInfo>

9.4 Processing Rules

Encrypted parts or attachments to the SOAP message using one of the sub-elements defined above MUST be in compliance with the XML Encryption specification. An encrypted SOAP envelope MUST still be a valid SOAP envelope. The message creator MUST NOT encrypt the <S:Envelope>, <S:Header>, or <S:Body> elements but MAY encrypt child elements of either the <S:Header> and <S:Body> elements. Multiple steps of encryption MAY be added into a single <Security> header block if they are targeted for the same recipient.

When an element or element content inside a SOAP envelope (e.g. of the contents of <S:Body>) is to be encrypted, it MUST be replaced by an <xenc:EncryptedData>, according to XML Encryption and it SHOULD be referenced from the <xenc:ReferenceList> element created by this encryption step. This specification allows placing the encrypted octet stream in an attachment. For example, f an <xenc:EncryptedData> appearing inside the <S:Body> element has <xenc:CipherReference> that refers to an attachment, then the decrypted octet stream SHALL replace the <xenc:EncryptedData>. However, if the <enc:EncryptedData> element is located in the <Security> header block and it refers to an attachment, then the decrypted octet stream MUST replace the encrypted octet stream in the attachment.

Deleted: s

Deleted: ¶

Formatted: Bullets and Numbering

9.4.1 Encryption

The general steps (non-normative) for creating an encrypted SOAP message in compliance with this specification are listed below (note that use of <xenc:ReferenceList> is RECOMMENDED).

1. Create a new SOAP envelope.
2. Create an `<xenc:ReferenceList>` sub-element, an `<xenc:EncryptedKey>` sub-element, or an `<xenc:EncryptedData>` sub-element in the `<Security>` header block (note that if the SOAP "role" and "mustUnderstand" attributes are different, then a new header block may be necessary), depending on the type of encryption.
3. Locate data items to be encrypted, i.e., XML elements, element contents within the target SOAP envelope, and attachments.
4. Encrypt the data items as follows: For each XML element or element content within the target SOAP envelope, encrypt it according to the processing rules of the XML Encryption specification. Each selected original element or element content MUST be removed and replaced by the resulting `<xenc:EncryptedData>` element. For an attachment, the contents MUST be replaced by encrypted cipher data as described in section 8.3 Signature Validation.
5. The optional `<ds:KeyInfo>` element in the `<xenc:EncryptedData>` element MAY reference another `<ds:KeyInfo>` element. Note that if the encryption is based on an attached security token, then a `<SecurityTokenReference>` element SHOULD be added to the `<ds:KeyInfo>` element to facilitate locating it.
6. Create an `<xenc:DataReference>` element referencing the generated `<xenc:EncryptedData>` elements. Add the created `<xenc:DataReference>` element to the `<xenc:ReferenceList>`.

Deleted: section 4.5.3

9.4.2 Decryption

On receiving a SOAP envelope with encryption header entries, for each encryption header entry the following general steps should be processed (non-normative):

1. Locate the `<xenc:EncryptedData>` items to be decrypted (possibly using the `<xenc:ReferenceList>`).
2. Decrypt them as follows: For each element in the target SOAP envelope, decrypt it according to the processing rules of the XML Encryption specification and the processing rules listed above.
3. If the decrypted data is part of an attachment and MIME types were used, then revise the MIME type of the attachment to the original MIME type (if one exists).

If the decryption fails for some reason, applications MAY report the failure to the sender using the fault code defined in Section 12 Error Handling.

Deleted: Section 6

9.5 Decryption Transformation

The ordering semantics of the `<wsse:Security>` header are sufficient to determine if signatures are over encrypted or unencrypted data. However, when a signature is included in one `<wsse:Security>` header and the encryption takes place in another `<wsse:Security>` header, the order may not be explicitly understood.

If the sender wishes to sign a message that is subsequently encrypted by an intermediary along the transmission path, the sender MAY use the Decryption Transform for XML Signature to explicitly specify the order of decryption.

10 Message Timestamps

When requestors and services are exchanging messages, it is often important to be able to understand the *freshness* of a message. In some cases, a message may be so *stale* that the receiver may decide to ignore it.

This specification does not provide a mechanism for synchronizing time. The assumption is either that the receiver is using a mechanism to synchronize time (e.g. NTP) or, more likely for federated applications, that they are making assessments about time based on three factors: creation time of the message, transmission checkpoints, and transmission delays.

To assist a receiver in making an assessment of staleness, a requestor may wish to indicate a suggested expiration time, beyond which the requestor recommends ignoring the message. The specification provides XML elements by which the requestor may express the expiration time of a message, the requestor's clock time at the moment the message was created, checkpoint timestamps (when an role received the message) along the communication path, and the delays introduced by transmission and other factors subsequent to creation. The quality of the delays is a function of how well they reflect the actual delays (e.g., how well they reflect transmission delays).

It should be noted that this is not a protocol for making assertions or determining when, or how fast, a service produced or processed a message.

This specification defines and illustrates time references in terms of the *dateTime* type defined in XML Schema. It is RECOMMENDED that all time references use this type. It is further RECOMMENDED that all references be in UTC time. If, however, other time types are used, then the *ValueType* attribute (described below) MUST be specified to indicate the data type of the time format.

10.1 Model

This specification provides several tools for receivers to use to assess the expiration time presented by the requestor. The first is the creation time. Receivers can use this value to assess possible clock synchronization issues. However, to make some assessments, the time required to go from the requestor to the receiver may also be useful in making this assessment. Two mechanisms are provided for this. The first is that intermediaries may add timestamp elements indicating when they received the message. This knowledge can be useful to get a holistic view of clocks along the message path. The second is that intermediaries can specify any delays they imposed on message delivery. It should be noted that not all delays can be accounted for, such as wire time and parties that don't report. Receivers need to take this into account when evaluating clock trust.

10.2 Timestamp Elements

This specification defines the following message timestamp elements. These elements are defined for use with the `<wsu:Timestamp>` header for SOAP messages, but they can be used anywhere within the header or body that creation, expiration, and intermediary markers are needed.

10.2.1 Expiration

The `<wsu:Expires>` element specifies the expiration timestamp. The exact meaning and processing rules for expiration depend on the context in which the element is used. The syntax for this element is as follows:

```
<wsu:Expires  ValueType="..." wsu:Id="...">...</wsu:Expires>
```

The following describes the attributes and elements listed in the schema above:

/Expires

This element's value represents an expiration time. The time specified SHOULD be a UTC format as specified by the ValueType attribute (default is XML Schema type dateTime).

/Expires/@ValueType

This optional attribute specifies the type of the time data. This is specified as the XML Schema type. If this attribute isn't specified, the default value is `xsd:dateTime`.

/Expires/@wsu:Id

This optional attribute specifies an XML Schema ID that can be used to reference this element.

The expiration is relative to the requestor's clock. In order to evaluate the expiration time, receivers need to recognize that the requestor's clock may not be synchronized to the receiver's clock. The receiver, therefore, will need to make a assessment of the level of trust to be placed in the requestor's clock, since the receiver is called upon to evaluate whether the expiration time is in the past relative to the requestor's, not the receiver's, clock. The receiver may make a judgment of the requestor's likely current clock time by means not described in this specification, for example an out-of-band clock synchronization protocol. The receiver may also use the creation time and the delays introduced by intermediate roles to estimate the degree of clock synchronization.

One suggested formula for estimating synchronization is

```
skew = receiver's arrival time - creation time - transmission time
```

Transmission time may be estimated by summing the values of delay elements, if present. It should be noted that wire-time is only part of this if delays include it in estimates. Otherwise the transmission time will not reflect the on-wire time. If no delays are present, there are no special assumptions that need to be made about processing time.

10.2.2 Creation

The `<wsu:Created>` element specifies a creation timestamp. The exact meaning and semantics are dependent on the context in which the element is used. The syntax for this element is as follows:

```
<wsu:Created ValueType="..." wsu:Id="...">...</wsu:Created>
```

The following describes the attributes and elements listed in the schema above:

/Created

This element's value is a creation timestamp. The time specified SHOULD be a UTC format as specified by the ValueType attribute (default is XML Schema type dateTime).

/Created/@ValueType

This optional attribute specifies the type of the time data. This is specified as the XML Schema type. If this attribute isn't specified, the default value is `xsd:dateTime`.

/Created/@wsu:Id

This optional attribute specifies an XML Schema ID that can be used to reference this element.

10.3 Timestamp Header

A `<wsu:Timestamp>` header provides a mechanism for expressing the creation and expiration times of a message introduced throughout the message path. Specifically, is uses the previously defined elements in the context of message creation, receipt, and processing.

All times SHOULD be in UTC format as specified by the XML Schema type (dateTime). It should be noted that times support time precision as defined in the XML Schema specification.

Multiple `<wsu:Timestamp>` headers can be specified if they are targeted at different roles. The ordering within the header is as illustrated below.

The ordering of elements in this header is fixed and MUST be preserved by intermediaries.

To preserve overall integrity of each `<wsu:Timestamp>` header, it is strongly RECOMMENDED that each role create or update the appropriate `<wsu:Timestamp>` header destined to itself.

Deleted: the particular role

The schema outline for the `<wsu:Timestamp>` header is as follows:

```
<wsu:Timestamp wsu:Id="...">
    <wsu:Created>...</wsu:Created>
    <wsu:Expires>...</wsu:Expires>
    ...
</wsu:Timestamp>
```

The following describes the attributes and elements listed in the schema above:

/Timestamp

This is the header for indicating message timestamps.

/Timestamp/Created

This represents the creation time of the message. This element is optional, but can only be specified once in a `Timestamp` header. Within the SOAP processing model, creation is the instant that the infoset is serialized for transmission. The creation time of the message SHOULD NOT differ substantially from its transmission time.

Deleted: materially

/Timestamp/Expires

This represents the expiration of the message. This is optional, but can appear at most once in a `Timestamp` header. Upon expiration, the requestor asserts that the message is no longer valid. It is strongly RECOMMENDED that receivers (anyone who processes this message) discard (ignore) any message that has passed its expiration. A Fault code (wsu:MessageExpired) is provided if the receiver wants to inform the requestor that its message was expired. A service MAY issue a Fault indicating the message has expired.

Deleted: */Timestamp/Received*¶
This represents the point in time at which the message was received by a specific role. This is optional, but SHOULD appear at most once per role in a `Timestamp` header (multiple entries MAY exist if looping is present, but the value MUST be different).

/Timestamp/{any}

This is an extensibility mechanism to allow additional elements to be added to the header.

/Timestamp/@wsu:Id

This optional attribute specifies an XML Schema ID that can be used to reference this element.

/Timestamp/@{any}

This is an extensibility mechanism to allow additional attributes to be added to the header.

The following example illustrates the use of the `<wsu:Timestamp>` element and its content.

```
<S:Envelope xmlns:S="http://www.w3.org/2001/12/soap-envelope"
            xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/xx/utility">
  <S:Header>
    <wsu:Timestamp>
       <wsu:Created>2001-09-13T08:42:00Z</wsu:Created>
       <wsu:Expires>2001-10-13T09:00:00Z</wsu:Expires>
    </wsu:Timestamp>
    ...
  </S:Header>
  <S:Body>
    ...
  </S:Body>
</S:Envelope>
```

10.4 TimestampTrace Header

A `<wsu:TimestampTrace>` header provides a mechanism for expressing the delays introduced throughout the message path. Specifically, is uses the previously defined elements in the context of message creation, receipt, and processing.

All times SHOULD be in UTC format as specified by the XML Schema type (dateTime). It should be noted that times support time precision as defined in the XML Schema specification.

Multiple `<wsu:TimestampTrace>` headers can be specified if they reference a different role.

The `<wsu:Received>` element specifies a receipt timestamp with an optional processing delay. The exact meaning and semantics are dependent on the context in which the element is used.

It is also strongly RECOMMENDED that each role sign its elements by referencing their ID, NOT by signing the `TimestampTrace` header as the header is mutable.

The syntax for this element is as follows:

```
<wsu:TimestampTrace>
   <wsu:Received Role="..." Delay="..." ValueType="..."
                wsu:Id="...">...</wsu:Received>
</wsu:TimestampTrace>
```

The following describes the attributes and elements listed in the schema above:

/Received

This element's value is a receipt timestamp. The time specified SHOULD be a UTC format as specified by the ValueType attribute (default is XML Schema type dateTime).

/Received/@Role

A required attribute, `Role`, indicates which role is indicating receipt. Roles MUST include this attribute, with a value matching the role value as specified as a SOAP intermediary.

/Received/@Delay

The value of this attribute is the delay associated with the role expressed in milliseconds. The delay represents processing time by the Role after it received the message, but before it forwarded to the next recipient.

/Received/@ValueType

This optional attribute specifies the type of the time data (the element value). This is specified as the XML Schema type. If this attribute isn't specified, the default value is `xsd:dateTime`.

/Received/@wsu:Id

This optional attribute specifies an XML Schema ID that can be used to reference this element.

The delay attribute indicates the time delay attributable to an role (intermediate processor). In some cases this isn't know n; for others it can be computed as *role's send time – role's receipt time*.

Each delay amount is indicated in units of milliseconds, without fractions. If a delay amount would exceed the maximum value expressible in the datatype, the value should be set to the maximum value of the datatype.

The following example illustrates the use of the `<wsu:Timestamp>` header and a `<wsu:TimestampTrace>` header indicating a processing delay of one minute subsequent to the receipt which was two minutes after creation.

```
<S:Envelope xmlns:S="http://www.w3.org/2001/12/soap-envelope"
            xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/xx/utility">
  <S:Header>
    <wsu:Timestamp>
       <wsu:Created>2001-09-13T08:42:00Z</wsu:Created>
       <wsu:Expires>2001-10-13T09:00:00Z</wsu:Expires>
    </wsu:Timestamp>
    <wsu:TimespampTrace>
       <wsu:Received Role="http://x.com/" Delay="60000">
                2001-09-13T08:44:00Z</wsu:Received>
    </wsu:TimestampTrace>
    ...
  </S:Header>
  <S:Body>
    ...
  </S:Body>
</S:Envelope>
```

11 Extended Example

The following sample message illustrates the use of security tokens, signatures, and encryption. For this example, the timestamp and the message body are signed prior to encryption. The decryption transformation is not needed as the signing/encryption order is specified within the `<wsse:Security>` header.

```
(001) <?xml version="1.0" encoding="utf-8"?>
(002) <S:Envelope xmlns:S="http://www.w3.org/2001/12/soap-envelope"
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
            xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/xx/secext"
            xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/xx/utility"
            xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
(003)   <S:Header>
(004)       <wsu:Timestamp>
(005)           <wsu:Created wsu:Id="T0">
(006)               2001-09-13T08:42:00Z
(007)           </wsu:Created>
(008)       </wsu:Timestamp>
(009)      <wsse:Security>
(010)         <wsse:BinarySecurityToken
                     ValueType="wsse:X509v3"
                     wsu:Id="X509Token"
                     EncodingType="wsse:Base64Binary">
(011)         MIIEZzCCA9CgAwIBAgIQEmtJZc0rqrKh5i...
(012)         </wsse:BinarySecurityToken>
(013)         <xenc:EncryptedKey>
(014)             <xenc:EncryptionMethod Algorithm=
                        "http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
(015)             <wsse:KeyIdentifier EncodingType="wsse:Base64Binary"
(016)                ValueType="wsse:X509v3">MIGfMa0GCSq...
(017)             </wsse:KeyIdentifier>
(018)             <xenc:CipherData>
(019)                <xenc:CipherValue>d2FpbmdvbGRfE0lm4byV0...
(020)                </xenc:CipherValue>
(021)             </xenc:CipherData>
(022)             <xenc:ReferenceList>
(023)                 <xenc:DataReference URI="#enc1"/>
(024)             </xenc:ReferenceList>
(025)         </xenc:EncryptedKey>
(026)         <ds:Signature>
(027)            <ds:SignedInfo>
(028)               <ds:CanonicalizationMethod
                  Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
(029)               <ds:SignatureMethod
               Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
(039)               <ds:Reference URI="#T0">
(031)                  <ds:Transforms>
(032)                     <ds:Transform
                  Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
(033)                  </ds:Transforms>
(034)                  <ds:DigestMethod
                   Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
(035)                  <ds:DigestValue>LyLsF094hPi4wPU...
(036)                   </ds:DigestValue>
(037)               </ds:Reference>
(038)               <ds:Reference URI="#body">
(039)                  <ds:Transforms>
(040)                     <ds:Transform
```

Deleted: `<ds:KeyInfo>¶`
`(016) <ds:KeyName>CN=Hiroshi Maruyama, C=JP</ds:KeyName>¶`
`(017) </ds:KeyInfo>`

```
                  Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
(041)                  </ds:Transforms>
(042)                  <ds:DigestMethod
                   Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
(043)                  <ds:DigestValue>LyLsF094hPi4wPU...
(044)                   </ds:DigestValue>
(045)              </ds:Reference>
(046)           </ds:SignedInfo>
(047)           <ds:SignatureV alue>
(048)                    Hp1ZkmFZ/2kQLXDJbchm5gK...
(049)           </ds:SignatureValue>
(050)           <ds:KeyInfo>
(051)               <wsse:SecurityTokenReference>
(052)                   <wsse:Reference URI="#X509Token"/>
(053)               </wsse:SecurityTokenReference>
(054)           </ds:KeyInfo>
(055)        </ds:Signature>
(056)     </wsse:Security>
(057)   </S:Header>
(058)   <S:Body wsu:Id="body">
(059)      <xenc:EncryptedData
                  Type="http://www.w3.org/2001/04/xmlenc#Element"
                  wsu:Id="enc1">
(060)         <xenc:EncryptionMethod
              Algorithm="http://www.w3.org/2001/04/xmlenc#3des-cbc"/>
(061)         <xenc:CipherData>
(062)            <xenc:CipherValue>d2FpbmdvbGRfE0lm4byV0...
(063)            </xenc:CipherValue>
(064)         </xenc:CipherData>
(065)      </xenc:EncryptedData>
(066)   </S:Body>
(067) </S:Envelope>
```

Let's review some of the key sections of this example:

Lines (003)-(057) contain the SOAP message headers.

Lines (004)-(008) specify the timestamp information. In this case it indicates the creation time of the message.

Lines (009)-(056) represent the `<wsse:Security>` header block. This contains the security-related information for the message.

Lines (010)-(012) specify a security token that is associated with the message. In this case, it specifies an X.509 certificate that is encoded as Base64. Line (011) specifies the actual Base64 encoding of the certificate.

Lines (013)-(025) specify the key that is used to encrypt the body of the message. Since this is a symmetric key, it is passed in an encrypted form. Line (014) defines the algorithm used to encrypt the key. Lines (015)-(017) specify the name of the key that was used to encrypt the symmetric key. Lines (018)-(021) specify the actual encrypted form of the symmetric key. Lines (022)-(024) identify the encryption block in the message that uses this symmetric key. In this case it is only used to encrypt the body (Id="enc1").

Lines (026)-(055) specify the digital signature. In this example, the signature is based on the X.509 certificate. Lines (027)-(046) indicate what is being signed. Specifically, Line (039) references the creation timestamp and line (038) references the message body.

Lines (047)-(049) indicate the actual signature value – specified in Line (042).

Lines (051)-(053) indicate the key that was used for the signature. In this case, it is the X.509 certificate included in the message. Line (052) provides a URI link to the Lines (010)-(012).

The body of the message is represented by Lines (056)-(066).

Lines (059)-(065) represent the encrypted metadata and form of the body using XML Encryption. Line (059) indicates that the "element value" is being replaced and identifies this encryption. Line

(060) specifies the encryption algorithm – Triple-DES in this case. Lines (062)-(063) contain the actual cipher text (i.e., the result of the encryption). Note that we don't include a reference to the key as the key references this encryption – Line (023).

12 Error Handling

There are many circumstances where an *error* can occur while processing security information. For example:

- Invalid or unsupported type of security token, signing, or encryption
- Invalid or unauthenticated or unauthenticatable security token
- Invalid signature
- Decryption failure
- Referenced security token is unavailable

These can be grouped into two *classes* of errors: unsupported and failure. For the case of unsupported errors, the receiver MAY provide a response that informs the sender of supported formats, etc. For failure errors, the receiver MAY choose not to respond, as this may be a form of Denial of Service (DOS) or cryptographic attack. We combine signature and encryption failures to mitigate certain types of attacks.

If a failure is returned to a sender then the failure MUST be reported using SOAP's Fault mechanism. The following tables outline the predefined security fault codes. The "unsupported" class of errors are:

Error that occurred	**faultcode**
An unsupported token was provided	wsse:UnsupportedSecurityToken
An unsupported signature or encryption algorithm was used	wsse:UnsupportedAlgorithm

The "failure" class of errors are:

Error that occurred	**faultcode**
An error was discovered processing the `<wsse:Security>` header.	wsse:InvalidSecurity
An invalid security token was provided	wsse:InvalidSecurityToken
The security token could not be authenticated or authorized	wsse:FailedAuthentication
The signature or decryption was invalid	wsse:FailedCheck
Referenced security token could not be retrieved	wsse:SecurityTokenUnavailable

13 Security Considerations

It is strongly RECOMMENDED that messages include digitally signed elements to allow message receivers to detect replays of the message when the messages are exchanged via an open network. These can be part of the message or of the headers defined from other SOAP extensions. Four typical approaches are:

- Timestamp
- Sequence Number
- Expirations
- Message Correlation

This specification defines the use of XML Signature and XML Encryption in SOAP headers. As one of the building blocks for securing SOAP messages, it is intended to be used in conjunction with other security techniques. Digital signatures need to be understood in the context of other security mechanisms and possible threats to an entity.

Digital signatures alone do not provide message authentication. One can record a signed message and resend it (a replay attack). To prevent this type of attack, digital signatures must be combined with an appropriate means to ensure the uniqueness of the message, such as timestamps or sequence numbers (see earlier section for additional details).

When digital signatures are used for verifying the identity of the sending party, the sender must prove the possession of the private key. One way to achieve this is to use a challenge-response type of protocol. Such a protocol is outside the scope of this document.

To this end, the developers can attach timestamps, expirations, and sequences to messages.

Implementers should also be aware of all the security implications resulting from the use of digital signatures in general and XML Signature in particular. When building trust into an application based on a digital signature there are other technologies, such as certificate evaluation, that must be incorporated, but these are outside the scope of this document.

Requestors should use digital signatures to sign security tokens that do not include signatures (or other protection mechanisms) to ensure that they have not been altered in transit.

Also, as described in XML Encryption, we note that the combination of signing and encryption over a common data item may introduce some cryptographic vulnerability. For example, encrypting digitally signed data, while leaving the digital signature in the clear, may allow plain text guessing attacks. The proper useage of nonce guards aginst replay attacks.

Deleted: Care should be taken by application designers not to introduce such vulnerabilities.

In order to *trust* Ids and timestamps, they SHOULD be signed using the mechanisms outlined in this specification. This allows readers of the IDs and timestamps information to be certain that the IDs and timestamps haven't been forged or altered in any way. It is strongly RECOMMENDED that IDs and timestamp elements be signed.

Timestamps can also be used to mitigate replay attacks. Signed timestamps MAY be used to keep track of messages (possibly by caching the most recent timestamp from a specific service) and detect replays of previous messages. It is RECOMMENDED that timestamps and nonces be cached for a given period of time, as a guideline a value of five minutes can be used as a minimum to detect replays, and that timestamps older than that given period of time set be rejected. in interactive scenarios.

Deleted: It is RECOMMENDED that timestamps and nonces be cached for a minimum of five minutes to detect replays, and that timestamps older than five minutes be rejected

In one-way message authentication, it is RECOMMENDED that the sender and the receiver re-use the elements and structure defined in this specification for proving and validating freshness of a message. It is RECOMMEND that the nonce value be unique per message (never been used as a nonce before by the sender and receiver) and use the `<wsse:Nonce>` element within the `<wsse:Security>` header. Further, the `<wsu:Timestamp>` header SHOULD be used with a

<wsu:Created> element. It is strongly RECOMMENDED that the <wsu:Created>, <wsse:Nonce> elements be included in the signature on <wsu:Timestamp> element

Deleted: these

Formatted: Default Paragraph Font

Deleted: signature

14 Privacy Considerations

TBD

15 Acknowledgements

This specification was developed as a result of joint work of many individuals from the WSS TC including: TBD

The input specifications for this document were developed as a result of joint work with many individuals and teams, including: Keith Ballinger, Microsoft, Bob Blakley, IBM, Allen Brown, Microsoft, Joel Farrell, IBM, Mark Hayes, VeriSign, Kelvin Lawrence, IBM, Scott Konersmann, Microsoft, David Melgar, IBM, Dan Simon, Microsoft, Wayne Vicknair, IBM.

16 References

[DIGSIG] Informational RFC 2828, "Internet Security Glossary," May 2000.

[Kerberos] J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)," RFC 1510, September 1993, http://www.ietf.org/rfc/rfc1510.txt .

[KEYWORDS] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, Harvard University, March 1997

[SHA -1] FIPS PUB 180-1. Secure Hash Standard. U.S. Department of Commerce / National Institute of Standards and Technology. http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.txt

[SOAP11] W3C Note, "SOAP: Simple Object Access Protocol 1.1," 08 May 2000.

[SOAP12] **W3C Working Draft, "**SOAP Version 1.2 Part 1: Messaging Framework", 26 June 2002

[SOAP-SEC] W3C Note, "SOAP Security Extensions: Digital Signature," 06 February 2001.

[URI] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax," RFC 2396, MIT/LCS, U.C. Irvine, Xerox Corporation, August 1998.

[WS-Security] "Web Services Security Language", IBM, Microsoft, VeriSign, April 2002.
"WS-Security Addendum", IBM, Microsoft, VeriSign, August 2002.
"WS-Security XML Tokens", IBM, Microsoft, VeriSign, August 2002.

[XML-C14N] W3C Recommendation, "Canonical XML Version 1.0," 15 March 2001

[XML-Encrypt] W3C Working Draft, "XML Encryption Syntax and Processing," 04 March 2002.

[XML-ns] W3C Recommendation, "Namespaces in XML," 14 January 1999.

[XML-Schema] W3C Recommendation, "XML Schema Part 1: Structures,"2 May 2001.
W3C Recommendation, "XML Schema Part 2: Datatypes," 2 May 2001.

[XML Signature] W3C Recommendation, "XML Signature Syntax and Processing," 12 February 2002.

[X509] S. Santesson, et al,"Internet X.509 Public Key Infrastructure Qualified Certificates Profile," http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-X.509-200003-I

[XPath] W3C Recommendation, "XML Path Language", 16 November 1999

Appendix A: Revision History

Rev	Date	What
01	20-Sep-02	Initial draft based on input documents and editorial review
02	24-Oct-02	Update with initial comments (technical and grammatical)

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.

Copyright © OASIS Open 2002. *All Rights Reserved.*

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself does not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an “AS IS” basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.