Web Services Security:
SAML Token Profile

OASIS STANDARD, 01 Dec. 2004

日本語訳 2006 年 7 月

日本語訳作成 (Japanese Translation):

XML コンソーシアム セキュリティ部会 (XML Consortium Security SIG)

日本語訳編集 (Editors):

高木 基成	TAKAGI, Motoshige	株式会社サンモアテック

日本語訳貢献者 (Contributors):

西村 利浩	NISHIMURA, Toshihiro	富士通株式会社
秋本 論史	AKIMOTO, Satoshi	大日本印刷株式会社
松永 豊	MATSUNAGA, Yutaka	東京エレクトロン株式会社
岡村 和英	OKAMURA, Kazuhide	株式会社ネット・タイム
中山 弘二郎	NAKAYAMA, Kojiro	株式会社日立製作所
山根 利夫	YAMANE, Toshio	株式会社日立製作所

免責事項 (disclaimer notice):

This translated document is provided by XML Consortium as an informational service to the global community. This is an unofficial, non-normative translation of the official document, Web Services Security: SAML Token Profile, located at http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0.pdf, © copyright OASIS 2002-2004. This translation is published with acknowledgement of and in agreement with terms specified in the OASIS Translation Policy. Neither OASIS nor XML Consortium assume responsibility for any errors contained herein.

本翻訳文書は、XML コンソーシアムによって世界中の地域社会に提供される情報サービスです。これは、http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0.pdf に掲載された公文書 Web Services Security: SAML Token Profile、copyright OASIS 2002-2004 の非公式かつ非規範的な翻訳です。本翻訳は OASIS 翻訳方針に規定された条件を認知し、かつこれに同意の上で公表されます。OASIS および XML コンソーシアムでは、ここに含まれるいかなる誤りについてもその責任は負いません。

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR

FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL XML CONSORTIUM, BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS) ARISING OUT OF THIS DOCUMENT.

XML コンソーシアムは、本書の記載内容に関して、その正確性、商品性、利用目的への適合性等に関して保証するものではなく、特許権、著作権、その他の権利を侵害していないことを保証するものでもありません。本書の利用により生じた損害について、XML コンソーシアムは、法律上のいかなる責任も負いません。

Web Services Security: SAML Token Profile

OASIS STANDARD, 01 Dec. 2004

Document identifier:

oasis-wss–saml-token-profile-1.0(PDF)(Word)

Location:

http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0.pdf

Errata Location:

http://www.oasis-open.org/committees/wss

Editors:

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

Contributors (voting members of the WSS TC as of Sept 8, 2004)

Gene Thurston	AmberPoint
Frank Siebenlist	Argonne National Laboratory
Hal Lockhart	BEA Systems, Inc.
Corinna Witt	BEA Systems, Inc.
Merlin Hughes	Betrusted (Baltimore Technologies)
Davanum Srinivas	Computer Associates
Thomas DeMartini	ContentGuard
Guillermo Lao	ContentGuard
Sam Wei	Documentum
Tim Moses	Entrust
Dana Kaufman	Forum Systems, Inc.
Toshihiro Nishimura	Fujitsu
Kefeng Chen	GeoTrust
Irving Reid	Hewlett-Packard
Kojiro Nakayama	Hitachi
Paula Austel	IBM
Derek Fu	IBM
Maryann Hondo	IBM
Kelvin Lawrence	IBM (TC Chair)
Michael McIntosh	IBM

Anthony Nadalin	IBM
Nataraj Nagaratnam	IBM
Ron Williams	IBM
Don Flinn	Individual
Bob Morgan	Internet2
Kate Cherry	Lockheed Martin
Paul Cotton	Microsoft Corporation
Vijay Gajjala	Microsoft Corporation
Alan Geller	Microsoft Corporation
Chris Kaler	Microsoft Corporation (TC Chair)
Rich Levinson	Netegrity, Inc.
Prateek Mishra	Netegrity, Inc.
Frederick Hirsch	Nokia
Senthil Sengodan	Nokia
Abbie Barbir	Nortel Networks
Lloyd Burch	Novell
Charles Knouse	Oblix
Steve Anderson	OpenNetwork (Secretary)
Vamsi Motukuru	Oracle
Ramana Turlapati	Oracle
Ben Hammond	RSA Security
Andrew Nash	RSA Security
Rob Philpott	RSA Security
Martijn de Boer	SAP
Blake Dournaee	Sarvega
Coumara Radja	Sarvega
Pete Wenzel	SeeBeyond Technology Corporation
Jeff Hodges	Sun Microsystems
Ronald Monzillo	Sun Microsystems
Jan Alexander	Systinet
Symon Chang	Tibco
J Weiland	US Dept of the Navy
Phillip Hallam-Baker	Verisign
Maneesh Sahu	Westbridge Technology

Contributors of input Documents (if not already listed above):

Hiroshi Maruyama	IBM
Chris McLaren	Netegrity
Jerry Schwarz	Oracle
Eve Maler	Sun Microsystems
Hemma Prafullchandra	VeriSign

Abstract:

本文書は、Web Services Security (WSS): SOAP Message Security 規定における Security Assertion Markup Language (SAML) V1.1 アサーションの使用方法を記載する。

Status:

本文書は OASIS 標準です。コメントは編集者に送付されたい。

委員会メンバー【Committee members】は、本規定に関するコメントを wss@lists.oasis-open.org リストに送付されたい。委員以外の方は、wss-comment@lists.oasis-open.org リストを購読し、コメントを送付されたい。申し込みは、http://lists.oasis-open.org/ob/adm.pl を参照のこと。

Web Services Security TC の作業に関連した Intellectual Property Rights やライセンス条項の開示情報は、http://www.oasis-open.org/committees/wss/ にある TC Web ページの Intellectual Property Rights の部分を参照のこと。Intellectual Property Rights に関する OASIS ポリシーは、http://www.oasis-open.org/who/intellectualproperty.shtml で記述されている。

Table of Contents

1. はじめに

WSS: SOAP Message Security 規定は、メッセージ層の完全性と秘匿性を実装するための SOAP 拡張の標準一式を定義する。本規定は、WSS: SOAP Message Security 規定により定義されている <wsse:Security> ヘッダ部から、セキュリティ・トークンとして、Security Assertion Markup Language (SAML) を使用する方法を定義する。

1.1. 目標

本規定の目標は、WSS: SOAP Message Security の文脈で SAML V1.1 アサーションの利用を定義することで、SOAP メッセージと SOAP メッセージ交換を安全にする目的を含む。この目標を達成するために、本プロファイルは以下を記述している：

1. SAML アサーションを<wsse:security> ヘッダによりどのように配送したり参照したりするか。
2. アサーションの記述 (例えば、申告) を、SOAP メッセージに結びつけるために、SAML アサーションを XML signature と共にどのように使うか。

1.1.1. 目標でないもの

以下のトピックは本文書の範囲外である：

3. SAML 記述構文、もしくは、セマンティクスを定義すること。
4. SOAP Message Security 以外の SAML アサーションの利用を記述すること。
5. Web Services Security (WSS): SOAP Message Security 規定における SAML V1.0 アサーションの利用を記述すること。

2. 記法と用語

本節では、本規定で利用される記法、名前空間および用語を規定する。

2.1. 記法

本文書に出てくるキーワード「しなければならない(MUST)」、「してはならない(MUST NOT)」、「要求されている(REQUIRED)」、「することになる(SHALL)」、「することはない(SHALL NOT)」、「する必要がある(SHOULD)」、「しないほうがよい(SHOULD NOT)」、「推奨される(RECOMMENDED)、「してもよい(MAY)」および「選択できる(OPTIONAL)」は RFC2119 で説明されるように解釈される。

本文書は、WS-Security SOAP Message Security 文書に定義されている記法を使用している。

(一般形式 "some-URI" の) 名前空間 URI は RFC2396 で定義されるあるアプリケーション依存または文脈依存の URI を表す。

本規定は一般の SOAP メッセージ構造及びメッセージ処理モデルと動作するよう設計されており、SOAP のどの版へも適用可能であるべきである。ここでは現在の SOAP 1.2 名前空間 URI が詳しい例を提供するために利用されているが、本規定の適用可能性を SOAP の単一の版に限定する意図はない。

読者は Internet Security Glossary の用語定義に精通していることを前提とする。

2.2. 名前空間

本規定の例に現れる以下の [XML-ns] 名前空間接頭辞は、XML 名前空間宣言が例に現れるかどうかに拘らず、(以下のテーブルから)一致する名前空間を参照していると理解されなければならない：

Prefix	Namespace
S11	http://schemas.xmlsoap.org/soap/envelope/
S12	http://www.w3.org/2003/05/soap-envelope
ds	http://www.w3.org/2000/09/xmldsig#
xenc	http://www.w3.org/2001/04/xmlenc
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-01.xsd
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
saml	**Urn: oasis:names:tc:SAML:1.0:assertion**

samlp	Urn: oasis:names:tc:SAML:1.0:protocol

Table-1 Namespace Prefixes

2.3. 用語

本規定は、WSS: SOAP Message Security 規定に定義されている用語を使用する。以下は、本規定で使われる追加された用語の定義である。

証明実体(Attesting Entity) – (SAML アサーション内の) SAML 主体ステートメントの主体と SOAP メッセージ・コンテンツの間の対応を確立するのに用いられる確認証拠を提供する実体。

確認方法識別子 –SAML 主体ステートメントの <saml:SubjectConfirmation> 要素内の値で、記述で利用される確認方法を識別する。

主体確認 – 証明実体により提供される確認証跡を検証することによって、(SAML アサーション内の)SAML 主体ステートメントの主体と SOAP メッセージ・コンテンツの間の対応を確立するのに利用される方法。

SAML アサーション・オーソリティ – アサーションを与える抽象的なシステムの実体。

主体 – SAML 主体ステートメントの申告が適用される実体の表現。

3. 利用方法

本節では、セキュリティ・トークンとして SAML アサーションを利用するための具体的な仕組みと手続きを定義する。

3.1. 処理モデル

本規定は、WSS: SOAP Message Security 規定により定義されているトークンに依存しない処理モデルを拡張している。

受信者が、SAML アサーションを含む、もしくは参照している <wsse:Security> ヘッダを処理するとき、受信者のポリシーに基づいて、処理される署名とアサーションを選択する。受信者の署名選択ポリシーが、署名の<ds:KeyInfo> 要素に出現する <wsse:SecurityTokenReference> 要素のセマンティックなラベル付け[1] に頼っても**よい(MAY)**としている。また、妥当性確認と処理のために選択されるアサーションが、選択された署名の<ds:KeyInfo> や <ds:SignedInfo> 要素から参照されたこれらを含むと仮定している。

選択されたアサーションの妥当性確認と処理の一環として、受信者は、(参照された SAML アサーションの)各 SAML 主体ステートメントの主体と、記述のために定義された確認方法を満たす証跡を提供している実体(すなわち、証明実体)との対応を確立**しなければならない(MUST)**。この対応を確立するための２つの方法、holder-of-key と sender-vouches は、以降に記述されている。本規定を実装しているシステムは、これらの主体確認方法を両方ともサポートするために必要な処理を実装**しなければならない(MUST)**。

[1] <wsse:SecurityTokenReference> 要素のオプションの Usage 属性は、(URI のような)セマンティックな利用方法ラベルの１つ以上を、参照とセキュリティ・トークンの利用へ、関連付けるために利用**してもよい(MAY)**。この属性の詳細は、WSS: SOAP Message Security を参照のこと。

3.2. セキュリティ・トークンの添付

SAML アサーションは、アサーション要素やアサーションへの参照を <wsse:Security> ヘッダ内に配置することにより、WSS: SOAP Message Security を利用して、SOAP メッセージに添付される。以下の例は、<wsse:Security> ヘッダに SAML アサーションを含んでいる SOAP メッセージを例示している。

```
<S12:Envelope>
  <S12:Header>
    <wsse:Security>
      <saml:Assertion
        AssertionID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
        IssueInstant="2003-04-17T00:46:02Z"
        Issuer=”www.opensaml.org”
        MajorVersion="1"
        MinorVersion="1"
          . . .
      </saml:Assertion>
        . . .
    </wsse:Security>
  </S12:Header>
  <S12:Body>
    . . .
  </S12:Body>
</S12:Envelope>
```

3.3. セキュリティ・トークンの識別と参照

WSS: SOAP Message Security 規定は、セキュリティ・トークンを参照するための <wsse:SecurityTokenReference> 要素を定義している。この要素によりトークン参照の３つの形式は定義されており、そして、その要素スキーマは、必要に応じて追加の参照形式を定義するための規定を含んでいる。<wsse:SecurityTokenReference> 要素により定義されるトークン参照の３つの形式は、以下のように定義される：

- 鍵識別子参照 – <wsse:EncodedString> としてセキュリティ・トークン識別子を配送して、そして、その属性で(必要に応じて)鍵識別子型(すなわち、ValueType)、識別子符号化の型(すなわち、EncodingType)や、セキュリティ・トークンを参照するために利用される他のパラメータを示す一般的要素(すなわち、<wsse:KeyIdentifier>)。
  鍵識別子が SAML アサーションを参照するために利用されるとき、その要素の値として SAML アサーションに対応する識別子を含まなければ**ならない(MUST)**。また、鍵識別子は ValueType 属性を含まなければ**ならない(MUST)**、そして、この属性の値は Table2 にある wsse:KeyIdentifier/@ValueType でなければ**ならない(MUST)**。鍵識別子は EncodingType[2] 属性を含んでは**ならない(MUST NOT)**、そして、鍵識別子の要素コンテンツは、xsi:string として、符号化されなければ**ならない(MUST)**。
  鍵識別子が、鍵識別子と同一のメッセージに含まれていない V1.1 SAML アサーションを参照するのに利用されるとき、<saml:AuthorityBinding> 要素は、鍵識別子を含んでいる <wsse:SecurityTokenReference> 要素に含まれなければ**ならない(MUST)**。<saml:AuthorityBinding> 要素のコンテンツは、意図したオーソリティから識別されたアサーションを得るために、<wsse:SecurityTokenReference> の意図した受信者にとって、不足の無い値を含まなければ**ならない(MUST)**。この目的で、<saml:AuthorityBinding> 要

[2] (http://www.oasis-open.org/committees/wss にある)Web Services Security: SOAP Message Security Version 1.0 の正誤表は、KeyIdentifier 要素の EncodingType 属性のための #Base64Binary 値からデフォルト指定を削除した。従って、このプロファイルに規定されているように、EncodingType の値を省略して、Base64 エンコーディングで処理しないように要求することは、正誤表と一致している。

素の AuthorityKind 属性の値は、"samlp:AssertionIdReference" でなければ**ならない(MUST)**。鍵識別子が、鍵識別子と同一のメッセージに含まれている V1.1 SAML アサーションを参照するのに利用されるとき、<saml:AuthorityBinding> 要素は、鍵識別子を含んでいる<wsse:SecurityTokenReference> 要素に含まれては**ならない(MUST NOT)**。

- 直接参照、URI 参照 – URI によりセキュリティ・トークンを識別する一般的要素(すなわち、<wsse:Reference>)。フラグメント識別子だけが特定されるならば、参照は、ローカル識別子(例えば、<wsu:Id> 属性)がフラグメント識別子に一致する文書内のセキュリティ・トークンになる。他の場合は、参照は、URI により識別される(潜在的に外部の)セキュリティ・トークンになる。このプロファイルでは、V1.1 SAML アサーションを参照するための、直接参照、URI 参照の使用を記述しない。
- 埋め込まれた参照 – セキュリティ・トークンをカプセル化する参照。
  埋め込まれた参照が SAML アサーションをカプセル化するのに利用されるとき、SAML アサーションは、<wsse:SecurityTokenReference> 内の <wsse:Embedded> 要素内の包含要素として、含まれなくては**ならない(MUST)**。

本規定は、４つの状況で SAML アサーションが参照されるかもしれない方法を記載する：

- SAML アサーションは、<wsse:Security> ヘッダ要素から直接参照されるかもしれない。この場合、アサーションはメッセージ内の参照によって配送される。
- SAML アサーションは、<wsse:Security> ヘッダの <ds:Signature> 要素の <ds:KeyInfo> 要素から参照されるかもしれない。この場合、アサーションは、署名の検証に利用する鍵を識別する <saml:SubjectConfirmation> 要素の主体ステートメントを含んでいる。
- SAML アサーション参照は、<wsse:Security> ヘッダ内の <ds:Signature> 要素の <ds:SignedInfo> 要素内の <ds:Reference> 要素から参照されるかもしれない。この場合、二重に参照されたアサーションは、含まれている署名により 、署名される。
- SAML アサーション参照は、<xenc:ReferenceList> 要素内の <xenc:DataReference> 要素から参照された <xenc:EncryptedData> 要素内の暗号化されたコンテンツとして存在するかもしれない。この場合、(埋め込まれたアサーションを含んでいるかもしれない)アサーション参照は、暗号化される。

これらの状況はそれぞれ、参照されたアサーションは以下のどちらでもよい：

- ローカル – このケースでは、参照を含んでいる <wsse:Security> ヘッダに含まれている。
- リモート – このケースでは、参照を含んでいる <wsse:Security> ヘッダに含まれていないが、SOAP メッセージの別の部分に現れても良いし、もしくは、参照により識別されたアサーション・オーソリティでありうる参照により識別される場所にあってもよい。

（リモート参照の場合）<saml:AuthortyBinding> 要素をサポートする <wsse:SecurityTokenReference> 形式の SAML 鍵識別参照が、SAML アサーションの参照を表現するのに現在最も適している。次期バージョンの [SAMLCore] は、直接参照 URI によるリモート 参照を容易にすることが期待されている。直接 <wsse:SecurityTokenReference> 参照により、ローカル SAML アサーションを参照する使用法は、識別子として <saml:AssertionID> 属性識別子を認識する必要があり、ローカル直接参照の解釈にトークンに依存する処理を強いるのでこのプロファイルには含まれていない。

属性	値
wsse:KeyIdentifier/@ValueType	http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID

Table-2 ValueType 属性値

3.3.1. ヘッダや要素から参照された SAML アサーション

全ての準拠した実装は、対応するアサーションを得るために、 <wsse:Security> ヘッダの中か、または署名以外のヘッダ要素に現れる SAML アサーション参照を処理できなければ**ならな**

い**(MUST)**。準拠した実装は、参照されたアサーションの確認方法に関わらずどのような参照も処理しなければ**ならない(MUST)**。

SAML アサーションは、<wsse:Security> ヘッダ、もしくは、ヘッダ内の（署名以外の）要素から参照されるかもしれない。以下の例は、ローカルの SAML アサーションを参照するための、<wsse:Security> ヘッダ内の鍵識別子の利用を例示している。

```
<S12:Envelope>
  <S12:Header>
    <wsse:Security>
      <saml:Assertion
        AssertionID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
        IssueInstant="2003-04-17T00:46:02Z"
        Issuer=”www.opensaml.org”
        MajorVersion="1"
        MinorVersion="1"
          . . .
      </saml:Assertion>
      <wsse:SecurityTokenReference wsu:Id=”STR1”>
        <wsse:KeyIdentifier wsu:Id=”…”
          ValueType=”http://docs.oasis-open.org/wss/oasis-wss-saml-
token-profile-1.0#SAMLAssertionID”>
          _a75adf55-01d7-40cc-929f-dbd8372ebdfc
        </wsse:KeyIdentifier>
     </wsse:SecurityTokenReference>
    </wsse:Security>
  </S12:Header>
  <S12:Body>
    . . .
  </S12:Body>
</S12:Envelope>
```

<wsse:Security> ヘッダの外部に存在している SAML アサーションは、SAML アサーション・オーソリティや応答者において識別されたアサーションを得るためのロケーション、バインディングとクエリを定義している（<wsse:SecurityTokenReference> 内の）<saml:AuthorityBinding> 要素を含むことにより、<wsse:Security> ヘッダ要素から参照されるかもしれない。

```
<wsse:SecurityTokenReference wsu:Id=”STR1”>
  <saml:AuthorityBinding>
    Binding=”urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding”
    Location=”http://www.opensaml.org/SAML-Authority”
    AuthorityKind= “samlp:AssertionIdReference”
  </saml:AuthorityBinding>
  <wsse:KeyIdentifier
    wsu:Id=”…”
    ValueType=”http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID”>
    _a75adf55-01d7-40cc-929f-dbd8372ebdfc
  </wsse:KeyIdentifier>
</wsse:SecurityTokenReference>
```

3.3.2. KeyInfo から参照された SAML アサーション

全ての準拠した実装は、holder-of-key 確認方法に定義されているような、<wsse:Security> ヘッダ内の <ds:Singnature> 要素の <ds:KeyInfo> 要素内に現れる SAML アサーション参照を処理できなければ**ならない(MUST)**。

以下の例は、<ds:KeyInfo> からローカルのアサーションを参照するための鍵識別子の利用を表している。

```
<ds:KeyInfo>
```

```
  <wsse:SecurityTokenReference wsu:Id=”STR1”>>
    <wsse:KeyIdentifier wsu:Id=”…”
      ValueType=”http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID”>
      _a75adf55-01d7-40cc-929f-dbd8372ebdfc
    </wsse:KeIdentifier>
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
```

以下の例は、鍵識別子と、識別された SAML アサーション・オーソリティや応答者により識別されたアサーションを得るための十分な情報（ロケーション、バインディングやクエリ）を通信するための <saml:AuthortyBinding> を含む<wsse:SecurityTokenReference> の利用を例示している。

```
<ds:KeyInfo>
  <wsse:SecurityTokenReference wsu:Id=”STR1”>
    <saml:AuthorityBinding>
   Binding=”urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding”
      Location=”http://www.opensaml.org/SAML-Authority”
      AuthorityKind= “samlp:AssertionIdReference”
    </saml:AuthorityBinding>
    <wsse:KeyIdentifier wsu:Id=”…”
      ValueType=”http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID”>
_a75adf55-01d7-40cc-929f-dbd8372ebdfc
    </wsse:KeyIdentifier>
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
```

<ds:KeyInfo> 要素は、<xenc:EncryptedData> と<xenc:EncryptedKey> 要素に現れてもよく、その場合暗号鍵を識別するという役割をもつ。 <ds:KeyInfo> 要素は、主体ステートメント(複数)に対応した主体を確認するために証明されなければ**ならない(MUST)** 鍵を識別する <saml:SubjectConfirmation> 要素に現れてもよい。このプロファイルに準拠した実装は、<xenc:EncryptedData> 、<xenc:EncryptedKey> や <saml:SubjectConfirmation>[3] 要素内の <ds:KeyInfo> 要素に現れる SAML アサーション参照の処理を要求しない。

3.3.3. SignedInfo から参照された SAML アサーション

参照されたアサーションの確認方法に関係なく、全ての準拠した実装は、<wsse:Security> ヘッダ内の <ds:Signature> 要素の <ds:Signednfo> 要素内の <ds:Reference> 要素から、<wsse:SecurityTokenReference> により参照される SAML アサーションを処理できなければ**ならない(MUST)**。埋め込まれた参照は直接ダイジェストされる場合があり、これによって、カプセル化されたアサーションを効果的にダイジェストする。他の <wsse:SecurityTokenReference> 形式は、ダイジェストされる参照されたアサーションのために参照解決されなければならない。

中核となる規定、WSS: SOAP Message Security は、<wsse:SecurityTokenReference> を（ダイジェスト・ストリーム中で）参照されたトークンのコンテンツに置き換える STR Dereference 変換を定義している。STR Dereference 変換は、埋め込まれた参照ではない <wsse:SecurityTokenReference> により参照されたいかなる SAML アサーションもダイジェストするためにも規定され、そして、適用されなければ**ならない(MUST)**。STR Dereference 変換は、埋め込まれた参照に適用**しない方がよい(SHOULD NOT)**。

[3] <saml:SubjectConfirmation> 要素内で <ds:KeyInfo> 要素から参照される SAML アサーションは、１つ以上の holder-of-key で確認される主体 statements を含まなければ**ならず(MUST)**、その主体 statement のそれぞれは主体と参照している記述の他の申告を確認するのに利用**してもよい(MAY)**鍵を識別する。

以下の例は、ダイジェスト操作が参照ではなくセキュリティ・トークンに対して遂行されるよう、SAML アサーション(すなわち、セキュリティ・トークン)への参照を参照解決するために STR Dereference 変換の利用を例示している。

```
<wsse:SecurityTokenReference wsu:Id=”STR1”>
  <saml:AuthorityBinding>
 Binding=”urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding”
    Location=”http://www.opensaml.org/SAML-Authority”
    AuthorityKind= “samlp:AssertionIdReference”
  </saml:AuthorityBinding>
  <wsse:KeyIdentifier wsu:Id=”…”
    ValueType=”http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID”>
    _a75adf55-01d7-40cc-929f-dbd8372ebdfc
  </wsse:KeyIdentifier>
</wsse:SecurityTokenReference>
  . . .
<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="#STR1">
    <Transforms>
      <ds:Transform
        Algorithm="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-soap-message-security-1.0#STR-Transform”/>
        <wsse:TransformationParameters>
          <ds:CanonicalizationMethod
            Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </wsse:TransformationParameters>
      </ds:Transform>
    </Transforms>
    <ds:DigestMethod
      Algorithm= "http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>...</ds:DigestValue>
  </ds:Reference>
</ds:SignedInfo>
```

<ds:Reference> 要素に現れる URI が wsu:Id の値により <wsse:SecurityTokenReference> 要素を識別する点に注意すること。STR Dereference 変換は、(参照されたアサーションの)入力ノードセットをシリアライズするために利用されるアルゴリズムを定義している<ds:CanonicalizationMethod> を（<wsse:TransformationParameters> 内に）含まなければ**ならない(MUST)**点にも注意すること。

3.3.4. 暗号化されたデータ参照から参照された SAML アサーション

参照されたアサーションの確認方法に関わらず、全ての準拠した実装は、<xenc:ReferencedList> 要素の <xenc:DataReference> 要素から Id により参照された <xenc:EncryptedData> 要素内の暗号化されたコンテンツとして現れる SAML アサーション参照を処理できなければ**ならない(MUST)**。<xenc:ReferencedList> 要素は、Security ヘッダの最上位の要素として現れても、<xenc:EncryptedKey> 要素に埋め込まれて現れてもよい。どちらの場合も、<xenc:ReferencedList> は、暗号化されたコンテンツを識別する。

STR Dereference 変換が適用されないことを除くと、この参照は、<ds:Signednfo> 要素内の <ds:Reference> 要素に現れ**てもよい(MAY)**参照と形式上は似ている。以下の例に表すように、<xenc:DataReference> 内の暗号化された <wsse:SecurityTokenReference> を含む <xenc:EncryptedData> 要素の識別子を含めることにより、(埋め込まれたアサーショ

ンを含むかもしれない)暗号化された <wsse:SecurityTokenReference> は、<xenc:DataReference> から参照される。

```
<xenc:EncryptedData Id=”EncryptedSTR1”>
  <ds:keyInfo>
  . . .
  </ds:KeyInfo>
  <xenc:CipherData>
    <xenc:CipherValue>...</xenc:CipherValue>
  </xenc:CipherData>
/xenc:EncryptedData>
<xenc:ReferenceList>
  <xenc:DataReference URI="#EncryptedSTR1"/>
</xenc:ReferenceList>
```

3.4. SAML アサーションの主体確認

WSS: SOAP Message Security の SAML プロファイルは、システムが、主体確認の方法として holder-of-key と sender-vouches をサポートすることを要求する。メッセージと添付されたアサーションの主体ステートメントとの間の対応を確立するために、XML Signature を使用することを、強く**推奨する(RECOMMENDED)**。このことは、保護されていないトランスポートで SOAP メッセージ交換をするときには、特に**推奨する(RECOMMENDED)**。

SAML アサーションのどんな処理機構も、アサーション署名の妥当性確認、そして、アサーション内の <saml:Condition> 要素の処理を含む SAML 規定 [SAMLCore] に定義されている必須の妥当性確認や処理ルールに従わなければ**ならない(MUST)**。

以下の表は、必須の主体の確認方法を列挙して、関連する処理モデルを要約している：

メカニズム	推奨される(RECOMMENDED) 処理ルール
urn:oasis:names:tc:SAML:1.0:cm:holder-of-key	証明実体は、署名により keyInfo として参照された SAML アサーションの主体ステートメントの <saml:ConfirmationMethod> 内の鍵情報で検証され得る XML Signature を含む。
urn:oasis:names:tc:SAML:1.0:cm:sender-vouches	(恐らくは)主体とは異なる証明実体が、主体の証明を保証する。受信者は、証明実体と既存の信頼関係を有していなければ**ならない(MUST)**。証明実体は、第三者による改ざんに備えて、メッセージ・コンテンツと共に(主体ステートメントを含む)アサーションを保護し**なければならない(MUST)**。４章を参照すること。

以下の節に記述されている高度な処理モデルは、再送攻撃に備えて保護するために必要となるであろう、証明実体とメッセージ送信者の区別をしないことに注意すること。高度な処理モデルは、送信者による受信者の認証、もしくは、メッセージまたはアサーションの機密性の要求を考慮していない。これらの懸案事項は、高度な処理モデルに記述されている以外の方法で対処されなければならない(すなわち、3.1)。

3.4.1. Holder-of-key 主体確認方法

以下の節では、SOAP メッセージと本規定に準じて SOAP メッセージに追加された SAML アサーションとの対応を確立する holder-of-key 方法を記述している。

3.4.1.1 証明実体

証明実体は、 holder-of-key <saml:SubjectConfirmation> 要素を含んでいる SAML 主体ステートメントの主体としてふるまう権限をもっていることを証明するために holder-of-key 確認方法を使う。holder-of-key 方法により確認される主体ステートメントは、以下の<saml:SubjectConfirmation> 要素を含まなければ**ならない(MUST)**：

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

<saml:SubjectConfirmation> 要素は、主体のアイデンティティを確認するために利用される公開鍵や秘密鍵[4] を識別する <ds:KeyInfo> 要素を含まなければ**ならない(MUST)**。

メッセージ受信者によって実行される関連した確認方法の処理を満たすため、証明実体は、確認用の鍵の知識を証明しなければ**ならない(MUST)**。証明実体は、メッセージに含まれるコンテンツに署名するために確認鍵を使用し、<wsse:Security> ヘッダ内に結果の <ds:Signature> 要素を含めることで、完遂**してもよい(MAY)**。この目的のために形成された <ds:Signature> 要素は、WSS: SOAP Message Security 規定に定義されている正規化(canonicalization)や、トークンの先頭追記ルール(token pre-pending rule）に適合しなければ**ならない(MUST)**。

holder-of-key <saml:SubjectConfirmation> 要素を含んでいる SAML アサーションは、アサーション・オーソリティにより確立された確認用 <ds:KeyInfo> の完全性を保護する <ds:Signature> 要素を含む**必要がある(SHOULD)**。

SAML アサーションの完全性を保護するために使われる <ds:Signature> 要素を形成するのに使用する正規化方法は、署名が計算されたコンテキスト以外（<wsse:Security> ヘッダなど）においても、これらの <ds:Signature> 要素の検証をサポートしなければ**ならない(MUST)**。

3.4.1.2 受信者

処理するために選択した SAML アサーションについて、受信者がアサーションの完全性を検証して、証明実体が <saml:SubjectConfirmation> 要素の <ds:KeyInfo> 要素によって、識別された鍵の知識を証明していない限り、メッセージ受信者は holder-of-key <saml:SubjectConfirmation> 要素を含んでいるアサーションを承認しては**ならない(MUST NOT)**。
もし、受信者が、証明実体は主体確認鍵の知識を証明していると判断した場合、そのとき、確認鍵を含む SAML アサーションは証明実体に起因すると**してよい(MAY)**、そして、主体確認方法により保護されたメッセージのどんな要素も、主体により提供されているとみなし

[4] [SAMLCore] は、「主体により保持されている暗号鍵」を含んでいる主体確認方法の KeyInfo を定義している。この鍵の証明は、誰が主体であるか(または、主体として動作するか)を立証するのに十分である。さらに、それがアイデンティティを確立した主体により確認鍵が知られている(または、主体だけに知られている)ことは証明できないため、鍵が主体により保持されていることを要求することは、テスト不可能であり確認方法 にいかなる強度も加えない。OASIS Security Services Technical Committee は、SubjectConfirmation の KeyInfo の定義から、「主体により保持されている」という文章を削除することを決議した。

547 てよい(MAY)。

548 #### 3.4.1.3 例

549 以下の例は、SOAP メッセージと <wsse:Security> ヘッダにおける SAML アサーションの
550 主体との間の対応を確立するための holder-of-key 主体確認方法の利用を例証している：

```
551 <?xml:version="1.0" encoding="UTF-8"?>
552 <S12:Envelope>
553   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
554   xmlns:xsd="http://www.w3.org/2001/XMLSchema">
555   <S12:Header>
556
557     <wsse:Security>
558       <saml:Assertion
559         AssertionID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
560         IssueInstant="2003-04-17T00:46:02Z"
561         Issuer=”www.opensaml.org”
562         MajorVersion="1"
563         MinorVersion="1"
564         xmlns="urn:oasis:names:tc:SAML:1.0:assertion">
565         <saml:Conditions>
566           NotBefore="2002-06-19T16:53:33.173Z"
567           NotOnOrAfter="2002-06-19T17:08:33.173Z"/>
568         <saml:AttributeStatement>
569           <saml:Subject>
570             <saml:NameIdentifier
571               NameQualifier="www.example.com"
572               Format="…">
573               uid=joe,ou=people,ou=saml-demo,o=baltimore.com
574             </saml:NameIdentifier>
575             <saml:SubjectConfirmation>
576               <saml:ConfirmationMethod>
577                 urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
578               </saml:ConfirmationMethod>
579               <ds:KeyInfo>
580                 <ds:KeyValue>…</ds:KeyValue>
581               </ds:KeyInfo>
582             </saml:SubjectConfirmation>
583           </saml:Subject>
584           <saml:Attribute
585             AttributeName="MemberLevel"
586             AttributeNamespace="http://www.oasis.open.
587             org/Catalyst2002/attributes">
588             <saml:AttributeValue>gold</saml:AttributeValue>
589           </saml:Attribute>
590           <saml:Attribute
591             AttributeName="E-mail"
592             AttributeNamespace="http://www.oasis.open.
593               org/Catalyst2002/attributes">
594             <saml:AttributeValue>joe@yahoo.com</saml:AttributeValue>
595           </saml:Attribute>
596         </saml:AttributeStatement>
597         <ds:Signature>…</ds:Signature>
598       </saml:Assertion>
599
600       <ds:Signature>
601         <ds:SignedInfo>
602           <ds:CanonicalizationMethod
603             Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
604           <ds:SignatureMethod
605             Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
606           <ds:Reference
```

```
            URI="#MsgBody">
            <ds:DigestMethod
              Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>GyGsF0Pi4xPU...</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>HJJWbvqW9E84vJVQk…</ds:SignatureValue>
        <ds:KeyInfo>
          <wsse:SecurityTokenReference wsu:Id=”STR1”>
            <wsse:KeyIdentifier wsu:Id=”…”
              ValueType=”http://docs.oasis-open.org/wss/oasis-wss-saml-
token-profile-1.0#SAMLAssertionID”>
              _a75adf55-01d7-40cc-929f-dbd8372ebdfc
            </wsse:KeyIdentifier>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
    </wsse:Security>
  </S12:Header>

  <S12:Body wsu:Id="MsgBody">
    <ReportRequest>
      <TickerSymbol>SUNW</TickerSymbol>
    </ReportRequest>
  </S12:Body>
</S12:Envelope>
```

3.4.2. Sender-vouches 主体確認方法

以下の節は、SOAP メッセージと WSS: SOAP Message Security の SAML プロファイルに準じて SOAP メッセージに追加された SAML アサーションとの間の対応を確立する sender-vouches 方法を記述している。

3.4.2.1 証明実体

証明実体は、sender-vouches <saml:SubjectConfirmation> 要素を含む SAML 主体ステートメントの主体に代わって振舞っていることを表明するために sender-vouches 確認方法を利用する。証明実体が sender-vouches 方法によって確認するであろう主体ステートメントは、以下の <saml:SubjectConfirmation> 要素を含まなければ**ならない(MUST)**：

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

受信者側の対応する確認方法の処理を満たすために、証明実体は、第三者によって変更されたときに受信者が判断できるように、保証される SOAP メッセージ・コンテンツを保護しなければ**ならない(MUST)**。また、証明実体は、権限のない改ざんを発見することができるように、(必要に応じて)保証される主体ステートメントとメッセージ・コンテンツへの結び付けもまた保護しなければ**ならない(MUST)**。証明実体は、関連したメッセージ・コンテンツとアサーションに署名するために鍵を利用することにより準備した<ds:Signature> 要素を対応した <wsse:Security> ヘッダに含めることで、これらの要求を満た**してよい(MAY)**。XML Signature 規定により定義されているように、証明実体は、<ds:Signature> 要素内に <ds:KeyInfo> 要素を含めることによって鍵を識別**してよい(MAY)**。

この目的のために形成された <ds:Signature> 要素は、正規化とWSS: SOAP Message Security 規定に定義されているトークンの先頭追記ルールに準拠しなければ**ならない(MUST)**。

3.4.2.2 受信者

処理するために選択した SAML アサーションについて、アサーションの主体に代わって振舞うことを受信者によって信頼された実体証明により、保証されたアサーションと SOAP メッセージ・コンテンツが(上記のように)保護されない限り、メッセージ受信者は sender-vouches <saml:ConfirmationMethod> を含むアサーションを容認しては**ならない(MUST NOT)**。

3.4.2.3 例

以下の例は、アイデンティティを確立し、そして、“STR1” によって参照されたアサーションの主体（複数）に代わってメッセージ本体を送信したことを表明するための関連した <ds:Signature> 要素とともに、証明実体による sender-vouches 主体確認方法の利用を例証している。

“STR1” により参照されたアサーションは、メッセージには含まれない。“STR1” は、<ds:SignedInfo> から<ds:reference> により参照される。<ds:reference> は、<SecurityTokenReference>ではなくアサーションがダイジェスト計算において含まれるようにするため、STR-transform を含む。“STR1” は、3.3.3 節の例で説明したリモート・アサーション参照技術を利用する <AuthorityBinding> 要素を含む 。

ヘッダに埋め込まれて、そして、<ds:KeyInfo> の“STR2” により参照された SAML アサーションは、証明実体に対応している。アサーションに現れる公開確認鍵に対応する私有鍵は、メッセージ本体と “STRI” により参照されたアサーションを一緒に署名するために利用される。

```
<?xml:version="1.0" encoding="UTF-8"?>
<S12:Envelope>
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <S12:Header>
    <wsse:Security>

      <saml:Assertion
        AssertionID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
        IssueInstant="2003-04-17T00:46:02Z"
        Issuer=”www.opensaml.org”
        MajorVersion="1"
        MinorVersion="1"
        xmlns="urn:oasis:names:tc:SAML:1.0:assertion">
        <saml:Conditions>
          NotBefore="2002-06-19T16:53:33.173Z"
          NotOnOrAfter="2002-06-19T17:08:33.173Z"/>
        <saml:AttributeStatement>
          <saml:Subject>
            <saml:NameIdentifier
              NameQualifier="www.example.com"
              Format="…">
              uid=proxy,ou=system,ou=saml-demo,o=baltimore.com
            </saml:NameIdentifier>
            <saml:SubjectConfirmation>
              <saml:ConfirmationMethod>
                urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
              </saml:ConfirmationMethod>
              <ds:KeyInfo>
                <ds:KeyValue>…</ds:KeyValue>
              </ds:KeyInfo>
            </saml:SubjectConfirmation>
          </saml:Subject>
          <saml:Attribute
            . . .
          </saml:Attribute>
            . . .
        </saml:AttributeStatement>
```

```
      </saml:Assertion>

      <wsse:SecurityTokenReference wsu:Id=”STR1”>
        <saml:AuthorityBinding>
          saml:Binding=”urn:oasis:names:tc:SAML:1.0:bindings:SOAP-
binding”
          saml:Location=”http://www.opensaml.org/SAML-Authority”
          saml:AuthorityKind= “samlp:AssertionIdReference”
        </saml:AuthorityBinding>
        <wsse:KeyIdentifier wsu:Id=”…”
          ValueType=”http://docs.oasis-open.org/wss/oasis-wss-saml-
token-profile-1.0#SAMLAssertionID”>
          _a75adf55-01d7-40cc-929f-dbd8372ebdbe
        </wsse:KeyIdentifier>
      </wsse:SecurityTokenReference>

      <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="#STR1">
            <Transforms>
              <ds:Transform
                Algorithm="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-soap-message-security-1.0#STR-Transform"/>
                <wsse:TransformationParameters>
                  <ds:CanonicalizationMethod
                    Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
                </wsse:TransformationParameters>
              </ds:Transform>
            </Transforms>
            <ds:DigestMethod
              Algorithm= "http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>...</ds:DigestValue>
          </ds:Reference>
          <ds:Reference URI="#MsgBody">
            <ds:DigestMethod
              Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>...</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>HJJWbvqW9E84vJVQk…</ds:SignatureValue>
        <ds:KeyInfo>
          <wsse:SecurityTokenReference wsu:Id=”STR2”>
            <wsse:KeyIdentifier wsu:Id=”…”
              ValueType=”http://docs.oasis-open.org/wss/oasis-wss-saml-
token-profile-1.0#SAMLAssertion-1.1”>
              _a75adf55-01d7-40cc-929f-dbd8372ebdfc
            </wsse:KeyIdentifier>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
    </wsse:Security>
  </S12:Header>

  <S12:Body wsu:Id="MsgBody">
    <ReportRequest>
      <TickerSymbol>SUNW</TickerSymbol>
    </ReportRequest>
  </S12:Body>
```

```
</S12:Envelope>
```

3.5. エラー・コード

セキュリティヘッダの処理において検出されるエラーのため、WSS: SOAP Message Security の SAML トークン・プロファイルを実装するシステムが通常の処理を行わない場合、SOAP フォールト機構を利用して、エラーの原因を報告することを選択**してよい(MAY)**。WSS: SOAP Message Security の SAML トークン・プロファイルは、そのようなエラーに対して SOAP フォールトが返されることを必要とせず、そして、フォールトを返すことを選択したシステムは、エラー応答により戻される情報の結果として、どのようなセキュリティの脆弱性も生じないよう考慮する**必要がある(SHOULD)**。

フォールトを戻すことを選択したシステムは、WSS: SOAP Message Security 規定に定義されているエラー・コードを返す**必要がある(SHOULD)**。一般的なアサーション処理の失敗とWSS: SOAP Message Security 規定に定義されているエラー・コードとの**推奨(RECOMMENDED)**される対応が以下の表に定義される：

Assertion Processing Error (faultString)	RECOMMENDED Error(Faultcode)
参照された SAML アサーションを獲得できなかった。	`wsse:SecurityTokenUnavailable`
受信者が理解できない`<saml:Condition>`要素がアサーションに含まれる。	`wsse:UnsupportedSecurityToken`
アサーション内の署名またはアサーションの参照が無効である。	`wsse:FailedCheck`
受信者がアサーションの発行者を受け入れられない。	`wsse:InvalidSecurityToken`
受信者がアサーションで使われている拡張スキーマを理解できない。	`wsse:UnsupportedSecurityToken`

上記のテーブルは、SOAP 1.1 と共に使用されることが適している形式で、フォールトの文字列とコードを定義している。WSS: SOAP Message Security 規定は、SOAP 1.1 のフォールトを SOAP 1.2 のフォールトへマッピングする方法を記述している。

4. 脅威モデルと対応策 (参考)

本文書は、SAML アサーションを、SOAP メッセージへ安全に添付するためのメカニズムと手順を定義している。SOAP メッセージはさまざまな状況で使われ、特にメッセージが有効なセッションなしで配送されたり、メッセージが永続化されたり、または、メッセージが何人かの仲介者を経由したりするケースを含む。そのような使用における一般的な利用状況は、このプロファイルのユーザがいろいろな脅威に関心をもたなければならないことを示唆する。

一般に、WSS: SOAP Message Security と共に SAML アサーションを利用することは、SAML またはWSS: SOAP Message Security セキュリティ規定によって識別されるもの以上の新しい脅威を生じない。以下の節では、脅威モデルの特性の概要、そして、各々の認知されている脅威のために採用される**必要がある(SHOULD)** 対応策を提供する。

4.1. 盗聴

盗聴は、どんなネットワーク・プロトコルに対しても脅威であると同様に、WSS: SOAP Message Security の SAML トークン・プロファイルに対しても脅威である。仲介者を通した SOAP メッセージのルーティングは、盗聴の潜在的発生率を増やす。SOAP メッセージが永続化されるとき、盗聴の更なる機会が存在する。

盗聴からの最大の保護を提供するために、アサーション、アサーション参照と機密メッセージ・コンテンツは、意図された受信者だけが、それらの内容を見ることができるように、暗号化**する必要がある(SHOULD)**。このアプローチは配送中に盗聴の脅威を取り除くが、受信者の保管、または、脆弱な取り扱いに関連する危険を取り除かなく**てもよい(MAY)**。

トランスポート層のセキュリティが、メッセージとそれに含まれるアサーションや参照を配送中の盗聴から保護するのに用いられ**てもよい(MAY)**が、仲介者による盗聴から保護するのであれば、メッセージ・コンテンツは、トランスポート層の上層で、暗号化されなければ**ならない(MUST)**。

4.2. 再送

holder-of-key 主体確認メカニズムをもつ、オーソリティに保護された(例えば、署名された)アサーションに依存することは、鍵の保有者以外がアサーションを SOAP メッセージに結び付けるのを妨げる。このメカニズムが効果的にデータの起源を確認鍵の保有者に制限するけれども、それは、単独では、第三者によるメッセージの獲得と再送信を検出する手段を提供しない。

もし、アサーションが、アサーションの利用や再利用する実体を規制しないならば、sender-vouches 確認メカニズムを含むアサーションは、別の面で、再送への脆弱性を招くことになる。

メッセージの送信者が、起源で保護されたメッセージ・コンテンツ内に追加のメッセージ識別情報（例えば、タイムスタンプ、ナンス、受信者識別子など）を含めて、そして、受信者がこの情報を以前に受信した値と照合すれば、再送攻撃は受信者により検出することができる。

4.3. メッセージの挿入

WSS: SOAP Message Security の SAML トークン・プロファイルは、メッセージ挿入攻撃に対して脆弱ではない。

4.4. メッセージの削除

WSS: SOAP Message Security の SAML トークン・プロファイルは、メッセージ削除攻撃に対して脆弱ではない。

4.5. メッセージの改ざん

もし、受信者が関連したメッセージ・コンテンツの未許可の変更を検出できるならば、この規定に従って作成されるメッセージはメッセージの改ざんから保護されている。したがって、全ての関連する、変えられないメッセージは、証明実体によって署名することが強く**推奨される(RECOMMENDED)**。受信者は、SAML アサーションの主体と SOAP メッセージとの間の対応が、別の実体による改ざんに対して証明実体によって保護されたメッセージの部分に対して確立されていることだけを考慮する**必要がある(SHOULD)**。

受信したアサーションが発行されてから偽造され、変更されていないことをメッセージ受信者が確信できることを確実にするために、`<wsse:Security>` ヘッダ要素に現れている、もしくは、参照されている SAML アサーションは発行オーソリティまたは(保証されるなら)証明実体によって、許可されていない変更に対して保護(例えば、署名)されなければ**ならない(MUST)**。証明実体は、それが証明していて発行オーソリティによる署名がないどのような`<saml:Assertion>` 要素に対しても署名することが強く**推奨される(RECOMMENDED)**。

トランスポート層のセキュリティが、メッセージとそれに含まれるアサーションや参照を配送中の改ざんから保護するのに利用**されてもよい(MAY)**が、そのような保護を仲介者を介して拡張するために署名が要求される。

4.6. 中間者攻撃

holder-of-key 主体確認方法のアサーションは、中間者(MITM)攻撃に対して脆弱ではない。sender-vouches 主体確認方法のアサーションは、受信者が、証明実体のアイデンティティに、鍵の結び付けを信頼してないのと同じ程度に、中間者攻撃に弱い。

5. 参考文献

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

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

[SAMLBind] Oasis Committee Specification 01, E. Maler, P.Mishra, and R. Philpott (Editors), *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1*, September 2003.

[SAMLCore] Oasis Committee Specification 01, E. Maler, P.Mishra, and R. Philpott (Editors), *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1*, September 2003.

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

W3C Working Draft, Nilo Mitra (Editor), SOAP Version 1.2 Part 0: Primer, June 2002.

W3C Working Draft, Martin Gudgin, Marc Hadley, Noah Mendelsohn, Jean-Jacques Moreau, Henrik Frystyk Nielsen (Editors), SOAP Version 1.2 Part 1: Messaging Framework, June 2002.

W3C Working Draft, Martin Gudgin, Marc Hadley, Noah Mendelsohn, Jean-Jacques Moreau, Henrik Frystyk Nielsen (Editors), SOAP Version 1.2 Part 2: Adjuncts, June 2002.

[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-SAML] Contribution to the WSS TC, P. Mishra (Editor), WS-Security Profile of the Security Assertion Markup Language (SAML) Working Draft 04, Sept 2002.

[WSS: SOAP Message Security] Oasis Standard, A. Nadalin, C.Kaler, P. Hallem-Baker, R. Monzillo (Editors), Web Services Security: SOAP Message Security 1.0 (WS-Security 2004), August 2003.

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

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

[XML Token] Contribution to the WSS TC, Chris Kaler (Editor), WS-Security Profile for XML-based Tokens, August 2002.

886 Appendix A: 改訂履歴

Rev	Date	What
01	19-Sep-02	Initial draft produced by extracting SAML related content from [XML token]
02	23-Sep-02	Merged in content from SS TC submission
03	18-Nov-02	Resolved issues raised by TC
04	09-Dec-02	Refined confirmation mechanisms, and added signing example
05	15-Dec-02	Results of Baltimore F2F
06	21-Feb-03	Changed name to profile
07	05-May-03	Acknowledged contributors
07	05-May-03	Throughout document, Refined terminology to distinguish attesting entity from subject and sender, and to distinguish assertions from statements within assertions. Also modified sender-vouches to support traced vouching (by allowing for the use of a confirmation key)
08	09-Jun-03	Indicated reliance on conventions of core in “Notational Conventions”
08	09-Jun-03	In “Terminology”, added definitions of new terms (attesting entity and confirmation method identifier), edited definition of Subject Confirmation, and replaced definition of sender with subject.
08	09-Jun-03	In “Subject Confirmation of SAML Assertions”, added requirement that an attesting entity must protect unsigned sender-vouches confirmed assertions.
08	25-Nov-03	Added SAM v1.1 version distinction to “Abstract”
08	25-Nov-03	Editorial changes to “Introduction”
08	25-Nov-03	Reorganized non-normative text of requirements and goals sections
08	25-Nov-03	Removed Identification, Contact Information, Description, and Updates from “Usage”.
08	25-Nov-03	Updated schema URIs and corrected namespace prefixes in “Namespaces”
08	25-Nov-03	Updated SAML document references in “References” to point to v1.1. specs.
08	25-Nov-03	In Error codes, changed error processing such that it is optional and consistent with the recommendations in core.
08	25-Nov-03	Qualified “Threat Model and Counter-measures” as non-normative.
08	30-Nov-03	In “Identifying and Referencing Security Tokens”, removed keyname references and added embedded references. Also removed editorial comment regarding using artifacts to reference assertions.

Rev	Date	What
08	30-Nov-03	Made editorial changes to “Processing Model”, including clarification (by footnote) of “semantic labeling”
08	30-Nov-03	Removed “Acknowledgments” as it duplicated preceding sections of the document
08	12-15-03	Added high level goals and non-goals
08	12-15-03	Added support for the use of (fragment) URI references to section 3.3
08	12-15-03	Specified default encoding type for SAML and fragment UR references to be xsi:string
08	12-15-03	Added two more contexts in which SAML assertions may be referenced; from within SubjectConfirmation elements and as encrypted data.
08	12-15-03	Made it a requirement of conformant implementations that they support the various methods of referencing SAML assertions
08	12-15-03	Added new sections to describe SAML assertion referenced from SubjectConfirmation and SAML assertion referenced from Encrypted Data reference.
09	01-27-04	Changed document identifier and location
09	01-27-04	Modified namespace table of section 2.2 to differentiate SOAP 1.1 and SOAP 1.2
10	02-05-04	Changed all instances of wsu:id to wsu:Id
10	02-05-04	In section 3.4.2.1 beginning around line 705, removed the distinction of the “typical case where the assertion authority has NOT securely bound a key…” because we no longer expect sender-vouches to use a confirmation key.
10	3-29-04	Corrected STR transform URL to match change in core.
10	3-29-04	Removed from section 3.3.2 mention of use of KeyInfo with sender-vouches confirmation method.
10	3-29-04	Modified footnote in section 3.2 regarding usage attribute to reflect change from QNAMES to URIs.
10	3-29-04	Corrected signature algorithm in examples.
10	3-29-04	Corrected transforms syntax of example in section 3.3.3.
10	3-29-04	In section 3.3.3 recommended that STR dereference transform not be applied to embedded token references.
10	3-29-04	Removed requirement (from section 4.5 of Security Considerations) that assertion references be protected from unauthorized modification.

Rev	Date	What
10	4-02-04	Removed namespace qualification from ValueType, URI, EncodingType, and Usage Attributes (mostly in examples). Also removed angle brackets.
10	4-05-04	Reworded initial paragraph of section 2.2 Namespaces such that it is not normative, and affords more flexibility in the form of the examples.
10	4-05-04	Removed namespace declarations from examples.
10	4-05-04	Corrected misspelling of “Authorty” in examples.
10	4-05-04	Modified processing rule for sender-vouches in Table of section 3.4 (to allow sender to vouch for itself).
10	4-05-04	Editing changes to the error codes section. In particular, replaced the word “generated” with “returned”, and rewrote the description of the mapping to 1.2 constructs.
10	4-05-04	Removed unused SAMLreqs and SAMLSecure from the references section.
10	4-06-04	Added footnote to explain optional support for SAML V1.0 assertions.
10	4-06-04	Removed section 3.3.4 “SAML Assertion referenced from SubjectConfirmation”, as SAML is evolving in a manner that will make it unlikely that authorities will need to produce such assertions. Moved the description of SAML Assertions references occurring within KeyInfo of SubjectConfirmation to section 3.3.2 “SAML assertion referenced from KeyInfo”
10	4-06-04	From Section 3.3 “Identifying and referencing Security Tokens”, removed referencing a SAML assertion from KeyInfo of SubjectConfirmation from the five contexts in which SAML assertions may be referenced.
10	4-06-04	Moved description of SAML Assertion references occurring within KeyInfo of SubjectConfirmation to section 3.3.2.
10	4-06-04	Added footnote to description of holder-of-key semantics in section 3.4.1.1 to describe interpretation of “held by the subject” phrase appearing in definition in [SAMLCore].
10	4-06-04	Updated contributors list
11	5-21-04	Moved “http://…documents.php” URL from “Location” to “Document Repository (temporary):” which will be removed when document is available from “Location”.
11	5-21-04	In section “1.1.1 Non-Goals”, added new bullet to indicate that describing support for V1.0 assertions is

Rev	Date	What
		outside the scope of the profile.
11	5-21-04	Changed SAMLAssertion-1.0 wsse:Reference/@ValueType to SAMLAssertion-1.1 in examples (lines 366, 611, and 752)
11	5-21-04	Updated document, specification, and schema URL's to accommodate change to OASIS document URLs (i.e. www.docs.oasis-open.org changed to docs.oasis-open.org)
11	5-21-04	Removed SAMLAssertion-1.0 wsse:Reference/@ValueType from "Table-2 ValueType Attribute Values." Also removed footnote on table title.
11	5-21-04	Editorial correction made to the attributes of the NameIdentifier element in the examples (see lines 564 and 684).
11	5-21-04	In section 3.4, "Subject Confirmation of SAML Assertions" (line 485), changed the reference to be to [SAMLCore] for the definition of the validation and processing rules that apply to SAML assertions. Also (as the resolution to issue 275), extended the stated reliance (on [SAMLCore]) with "including the validation of assertion signatures, and the processing of <saml:Condition> elements within Assertions"
12	6-25-04	In section 3.4.2.3, clarified the description of the sender-vouches example.
13	6-30-04	Modified section 3.3 to describe the use of KeyIdentifiers as apposed to Direct references to reference SAML assertions.
13	6-30-04	In section 3.3 and 3.3.4 clarified the use of STRs from <xenc:DataReference>
13	6-3--04	Removed wsse:Reference/@ValueType from Table 2 of section 3.3, as the change to KeyIdentifiers rendered the ValueType unnecessary.
13	6-30-04	Changed the examples in sections 3.3.1, 3.3.2, 3.3.4, 3.4.1.3, and 3.4.2.3 to reflect the change from Direct references to KeyIdentifiers.
14	7-12-04	Corrected KeyIdentifier syntax of examples at lines 338, 376, 627, and 780.
15	7-19-04	Added clarification to sections 3.3.1, 3.3.2, and 3.3.4 to address issue 295b; that the profile include provision for the use of "Bearer" confirmed assertions.
CD 02	9-08-04	Renamed as committee draft, added reference to errata, updated contributor lists, modified status to CD, and added footnote to description of KeyIdentifier to direct reader to clarification in errata.

Rev	**Date**	What
CD 03	9-21-04	Removed version qualification (i.e. “Version 2 of ”) from the reference to the Errata occurring in the footnote (of section 3.3).
CD 04	10-21-04	Updated OASIS logo (bitmap). Changed Appendix B Copyright to 2004.
OASIS Standard	12-01-04	Updated document title, identifier, location, and status to reflect new status.

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 ma y be required to implement this specification. Please address the information to the OASIS Executive Director.

This document and the information contained herein is provided on an “AS IS” basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT N OT 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.

OASIS は、本文書で記述された技術の実装や利用に関して主張される可能性がある知的財産や他の権利の正当性や範囲についてや、そのような権利のライセンスが利用可能または不可能かもしれないことについて、何の立場もとらないし、そのような権利を確認するために努力してきたとも主張しない。OASIS 仕様の権利に関する OASIS の手続き情報は OASIS ウェブサイトで見

924 ることができる。公表のために利用可能となっている権利の主張の写しと利用可能となるであろ
925 うライセンスの保証、または、本規定の実装者または利用者がそのような財産権を利用するため
926 の一般的なライセンスまたは許可を取得しようとした試みの結果は、OASIS Executive Direct
927 or から取得することができる。

928 OASIS は、関心のあるものは誰でも、本規定を実装するために必要とされる技術を対象とする
929 著作権、特許または特許申請、または、他の財産権についての注意をうながしてもらうようお願
930 いする。このような情報については、OASIS Executive Director に連絡してほしい。

945 本節は参考である。