XML Consortium

～ 第5回 XMLコンソーシアムWeek ～

Webサービスを支えるセキュリティ技術
WS-SXの仕様と標準化状況

2006年5月22日

XMLコンソーシアム セキュリティ部会
西村 利浩（富士通株式会社）

アジェンダ

- Webサービスを支えるセキュリティ技術
  - OASIS WSS
    - V1.1標準化後の活動
  - OASIS WS-SX
    - WS-SXを取り巻くセキュリティ仕様
    - 仕様概説
      - WS-Trust
      - WS-SecureConversation
      - WS-SecurityPolicy
    - WS-SX TCでの標準化状況
  - 関連する標準化の動き
    - W3C
    - WS-I

Webサービスを支えるセキュリティ技術

- **OASIS WSS**
  - **V1.1標準化後の活動**
- OASIS WS-SX
- 関連する標準化の動き

V1.1標準化後のWSS TCの活動

- 5月18日時点
  - Member 34組織54人 (うちVoting Member 21組織31人)
  - 日本企業では日立製作所、富士通が参加
- OTP (One Time Password) Token Profileの検討
  - 5月9日に提案取り下げ
- Minimalist Profileの検討
  - 4月4日の電話会議で、もはや必要ないということで作業項目から除外
- エラッタ更新
  - V1.0のコア、X.509プロファイルのエラッタが更新
- FAQ作成
- 5月16日の電話会議
  - “errata only mode”へ
  - 電話会議も6週間置きに変更
  - 8月の時点で未解決の作業がなければTC解散予定

Webサービスを支えるセキュリティ技術

- OASIS WSS
- **OASIS WS-SX**
  - **WS-SXを取り巻くセキュリティ仕様**
  - 仕様概説
  - WS-SX TCでの標準化状況
- 関連する標準化の動き

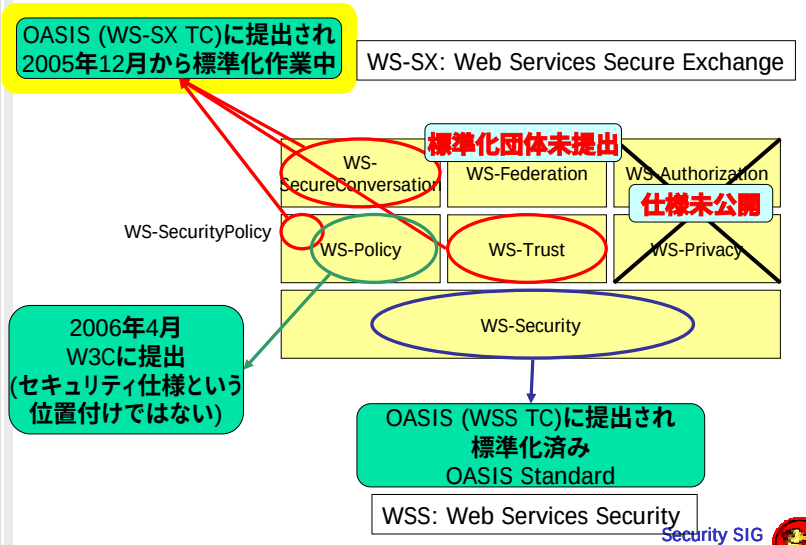
Webサービスのセキュリティ仕様(2002/04)

- 2002年4月発表のホワイトペーパー「Security in a Web Services World: A Proposed Architecture and Roadmap」

この時点では
WS-Security**のみ公開**

Security in a Web Services World: A Proposed Architecture and Roadmap
(http://msdn.microsoft.com/library/en-us/dnwssecur/html/securitywhitepaper.asp)

Webサービスのセキュリティ仕様(2006/05)



Webサービスを支えるセキュリティ技術

- OASIS WSS
- **OASIS WS-SX**
  - WS-SXを取り巻くセキュリティ仕様
  - **仕様概説**
  - WS-SX TCでの標準化状況
- 関連する標準化の動き

概要(1)

- Webサービスは、メッセージを受け取る際に、クレーム(名前、鍵、許可など)の証明を要求できる
  - **WS-SecurityPolicyで記述**
  - **+ WS-Policy, WS-PolicyAttachment**
- クレームはセキュリティ・トークンで表される

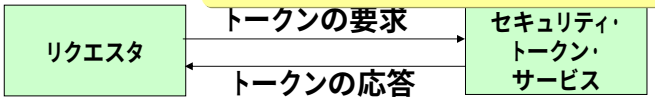

```
<sp:IssuedToken ...>
    <sp:Issuer>...</sp:Issuer>
    <sp:RequestSecurityTokenTemplate>
        <wst:TokenType>...SAML:1.1:assertion</wst:TokenType>
        <wst:Claims ...>...</wst:Claims>
    </sp:RequestSecurityTokenTemplate>
</sp:IssuedToken>
```


概要(2)

- セキュリティ・トークンはセキュリティ・トークン・サービス(STS)から取得
  - **WS-Trustを利用**

```
<wst:RequestSecurityToken Context="...">
    <wst:TokenType>...SAML:1.1:assertion</wst:TokenType>
    <wst:RequestType>...Issue</wst:RequestType>
    ...
</wst:RequestSecuri
```

+ STSでの認証にWS-Security (WSS)利用も




```
<wst:RequestSecurityTokenResponseCollection>
    <wst:RequestSecurityTokenResponse Context="...">
        <wst:TokenType>...SAML:1.1:assertion</wst:TokenType>
        <wst:RequestedSecurityToken>
            <saml:assertion>...</saml:assertion>
        </wst:RequestedSecurityToken>
        ...
    </wst:RequestSecurityTokenResponse>
</wst:RequestSecurityTokenResponseCollection>
```

概要(3)

- トークンを提示しWebサービスを利用

WS-Security(WSS)を利用

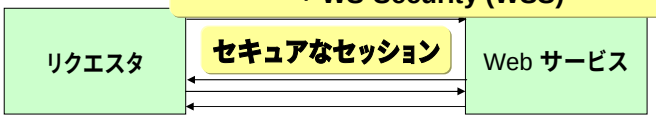

```
<S:Envelope>
    <S:Header>
        <wsse:Security>
            <saml:assertion>...</saml:assertion>
            ...
        </wsse:Security>
    </S:Header>
    <S:Body>
        ...
    </S:Body>
</S:Envelope>
```


概要(4)

- セキュアなセッションで複数メッセージ交換

WS-SecureConversationを利用

+ WS-Security (WSS)




```
<S:Envelope>
    <S:Header>
        <wsse:Security>
            <wsc:SecurityContextToken ...>
                <wsc:Identifier>uuid:...</wsc:Identifier>
            </wsc:SecurityContextToken>
            ...
        </wsse:Security>
    </S:Header>
    <S:Body>
        ...
    </S:Body>
</S:Envelope>
```

Webサービスを支えるセキュリティ技術

- OASIS WSS
- **OASIS WS-SX**
  - WS-SXを取り巻くセキュリティ仕様
  - **仕様概説**
    - **WS-Trust**
    - WS-SecureConversation
    - WS-SecurityPolicy
  - WS-SX TCでの標準化状況
- 関連する標準化の動き

注) この説明はWS-Trust V1.3 Editors Draft 01, 09 May 2006をベースにしています。最終仕様までに変更される可能性があります。

基本プロトコル

- 要求メッセージ RequestSecurityToken

```
<wst:RequestSecurityToken Context="...">
    <wst:TokenType>...</wst:TokenType>
    <wst:RequestType>...</wst:RequestType>
    ...
</wst:RequestSecurityToken>
```

トークンの型を指定

要求の型を指定

- 応答メッセージ RequestSecurityTokenResponse

```
<wst:RequestSecurityTokenResponse Context="...">
    <wst:TokenType>...</wst:TokenType>
    <wst:RequestedSecurityToken>...
                    </wst:RequestedSecurityToken>
    ...
</wst:RequestSecurityTokenResponse>
```

返却されるトークン

トークンが返却される際、<wst:RequestSecurityTokenResponse>は<wst:RequestSecurityTokenResponseCollection>に置かれる

基本的な要求のタイプ

- 要求のタイプ
  - Issue – 要求において提供/証明されたクレデンシャルに基づいて、(場合によっては新しい証明情報とともに) 新しいトークンが発行される。
  - Renew – 以前発行された有効期限付きのトークンを提示することにより、新しい期限で同じトークンが返される。
  - Cancel – 以前発行されたトークンが必要なくなったとき、トークンをキャンセルし、その利用を終了する。
  - Validate – 指定されたセキュリティトークンの有効性が評価され、その結果が返される。

トークン発行要求

```
<wst:RequestSecurityToken>
    <wst:TokenType>...</wst:TokenType>
    <wst:RequestType>...Issue</wst:RequestType>
    ...
    <wsp:AppliesTo>...</wsp:AppliesTo>
    <wst:Claims Dialect="...">...</wst:Claims>
    <wst:Entropy>
        <wst:BinarySecret>...</wst:BinarySecret>
    </wst:Entropy>
    <wst:Lifetime>
        <wsu:Created>...</wsu:Created>
        <wsu:Expires>...</wsu:Expires>
    </wst:Lifetime>
</wst:RequestSecurityToken>
```

Issueを指定

トークンの有効範囲を指定

トークンに含まれるべきクレームを指定

鍵生成用のエントロピーを指定

トークンの有効期限を指定

トークン発行要求

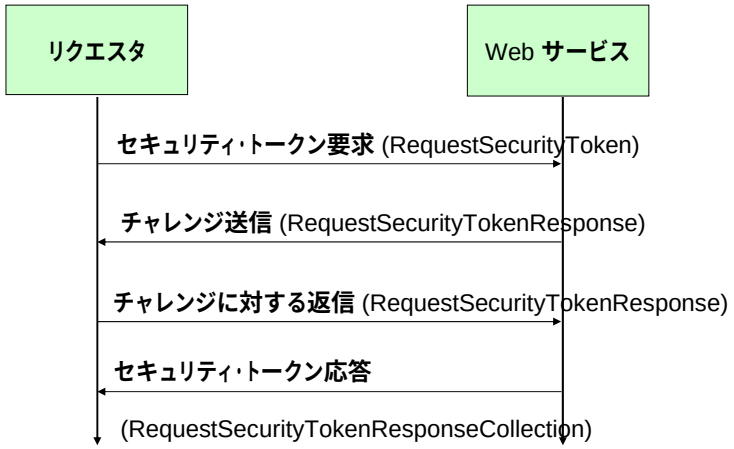
```
<wst:RequestSecurityTokenResponse>
    <wst:TokenType>...</wst:TokenType>
    <wst:RequestedSecurityToken>...
                              </wst:RequestedSecurityToken>
    ...
    <wsp:AppliesTo>...</wsp:AppliesTo>
    <wst:RequestedAttachedReference>
        ...
    </wst:RequestedAttachedReference>
    <wst:RequestedUnattachedReference>
        ...
    </wst:RequestedUnattachedReference>
    <wst:RequestedProofToken>...</wst:RequestedProofToken>
    <wst:Entropy>
        <wst:BinarySecret>...</wst:BinarySecr
    </wst:Entropy>
    <wst:Lifetime>...</wst:Lifetime>
</wst:RequestSecurityTokenResponse>
```

トークンの参照方法を指定

要求されたトークンに関係する所有証明トークンを返す

交渉/チャレンジ

- 複数メッセージ交換による交渉/チャレンジも許す



その他の拡張

- 誰か他人の代わりにトークンを要求していることを示して、トークンを要求
- 鍵や暗号化の詳細を指定してトークンを要求
- 誰かに委任することを指定、もしくは転送/委任可能であることを指定してトークンを要求
- ポリシー(WS-Policy)を指定してトークンを要求
- リクエスタ以外に返却されるトークンを利用することが許されるParticipantsを指定して、トークンを要求
- 鍵交換トークン(KET)

Webサービスを支えるセキュリティ技術

- OASIS WSS
- **OASIS WS-SX**
  - WS-SXを取り巻くセキュリティ仕様
  - **仕様概説**
    - WS-Trust
    - **WS-SecureConversation**
    - WS-SecurityPolicy
  - WS-SX TCでの標準化状況
- 関連する標準化の動き

注) この説明はWS-SecureConversation V1.3 Editors Draft 01, 18 April 2006をベースにしています。最終仕様までに変更される可能性があります。

WS-SecureConversation概要

- WSS (WS-Security)では、単一メッセージの認証手段を提供
- 複数メッセージの交換を行なう場合に、パーティ間でセキュリティ・コンテキスト(セッション)を確立手段を提供→WS-SecureConversation
- 新たな2つのトークン・タイプを規定
  - SecurityContextToken
  - DerivedKeyToken
- コンテキストを確立するためにWS-Trustを利用する方法を規定

セキュリティ・コンテキスト・トークン

- セキュリティ・コンテキスト
  - 確立された認証状態と合意された鍵を参照するための抽象概念
- SecurityContextToken
  - セキュリティ・コンテキストの具体的表現
  - コンテキストはURIで識別される

```
<wsse:Security>
    <wsc:SecurityContextToken wsu:Id="MyID">
        <wsc:Identifier>uuid:...</wsc:Identifier>
    </wsc:SecurityContextToken>
    <ds:Signature>
        ...
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#MyID" />
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
</wsse:Security>
```

署名に使う鍵としてセキュリティ・コンテキスト・トークンを指定

セキュリティ・コンテキストの確立

- WS-Trustを利用して、セキュリティ・コンテキスト・トークンの発行(Issue)、修正(Amend)、更新(Renew)、キャンセル(Cancel)する方法を規定

鍵の導出

- 鍵の交換、同じ鍵の使いまわしはセキュリティ上好ましくない
→鍵の導出して利用する方法を規定
- RFC 2246 (TLS)で規定する擬似乱数関数P_SHA-1を利用
- <DerivedKeyToken>要素

“#CTX1”で参照されるセキュリティ・コンテキスト・トークンで識別される共有鍵から3世代目の導出鍵を表す

```
<wsc:DerivedKeyToken>
    <wsse:SecurityContextReference>
        <wsse:Reference URI=“#CTX1” />
    </wsse:SecurityTokenReference>
    <wsc:Generation>2</wsc:Generation>
</wsc:DerivedKeyToken>
```

Webサービスを支えるセキュリティ技術

- OASIS WSS
- **OASIS WS-SX**
  - WS-SXを取り巻くセキュリティ仕様
  - **仕様概説**
    - WS-Trust
    - WS-SecureConversation
    - **WS-SecurityPolicy**
  - WS-SX TCでの標準化状況
- 関連する標準化の動き

注) この説明はWS-SecurityPolicy V1.2 Editors Draft 01, 27 April 2006**をベースにしています。最終仕様までに変更される可能性があります。**

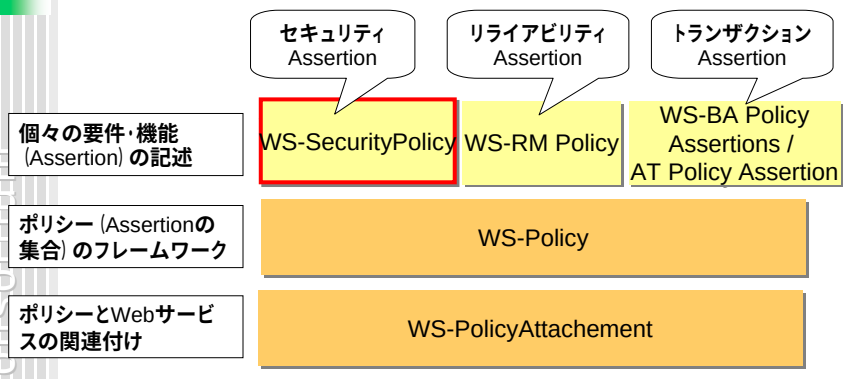
Webサービスポリシーの概要

- Webサービスのポリシーとは
  - Webサービスの要件や機能
    - 例1）WebサービスAを利用するためには、SOAPリクエストに署名がされていなければならない
    - 例2）WebサービスBはAESアルゴリズムによる暗号化をサポートしている
  - WSDLでは記述されないが、Webサービスを利用するためには必要な情報
- ポリシーの利用例
  - Webサービスの要件や機能をポリシーとして記述し公開
  - クライアントは、送信メッセージがポリシーを満たすように処理
  - Webサービスは、受信メッセージがポリシーを満たしているか検証

ポリシーの標準仕様を策定することで、Webサービスの相互接続性向上が期待できる

SOAP：Simple Object Access Protocol　AES：Advanced Encryption Standard
WSDL：Web Services Description Language

ポリシー関連仕様



：OASISで標準化中の仕様
：W3Cに提出された仕様

WS-RM：WS-ReliableMessaging
WS-BA：WS-BusinessActivity
WS-AT：WS-AtomicTransaction

(トランザクションに関するAssertionは個別仕様書ではなく本仕様の中で規定)

WS-SecurityPolicy概要

- WS-SecurityPolicyとは
  - Webサービスのセキュリティに関するAssertionの記述方法を規定した仕様
  - WS-Security、WS-Trust、WS-SecureConversation、トランスポートレベルセキュリティに関するAssertionの記述方法を規定

◆ **Assertionの例**

SOAPボディの秘匿性が確保されていなければならない

```
<sp:EncryptedParts>
  <sp:Body/>
</sp:EncryptedParts>
```

メッセージには常にUsernameTokenが含まれていなければならない

```
<sp:UsernameToken
  sp:IncludeToken="../IncludeToken/Always" />
```

WS-SecurityPolicyが規定するアサーション

- Protection Assertions
  - メッセージ保護に関するアサーション
- Token Assertions
  - メッセージで利用されるトークンを指定するアサーション
- Security Binding Assertions
  - セキュリティがどのような機構(トランスポート層、メッセージ層)で提供されるかを指定するアサーション
- Supporting Tokens Assertions
  - サービスが複数クレームを要求するような場合に、メッセージに含めるべき追加のトークンを指定するアサーション
- Protocol Assertions
  - WSS (1.0, 1.1)、WS-Trustのオプションを指定するアサーション

(参考)WS-Policy概要

- WS-Policyは、ポリシー表記のフレームワークを規定した仕様

◆ **ポリシー表記の例**

```
<wsp:Policy>
  <wsp:ExactlyOne>
    <wsp:All>
      Assertion A
      Assertion B
    </wsp:All>
    <wsp:All>
      Assertion C
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>
```

※ Normal Formで記述した場合

Policy Expression

ポリシーの表記。Alternativeの集合。ポリシーを満たすには、下位のAlternativeのどれか一つを満たす必要がある

Policy Alternative

Assertionの集合。Alternativeを満たすには、下位のAssertionをすべて満たす必要がある

Policy Assertion

個々の要件や機能の表記。Assertionのスキーマは別仕様で規定する

(参考)WS-PolicyAttachment概要

- WS-PolicyAttachmentは、ポリシーとWebサービスを関連付ける方法を規定した仕様

◆ **WSDLへの関連付けの例**

WSDL

```
<wsdl:definitions>
  <wsp:UsingPolicy>
  <wsdl:message
    wsp:PolicyURIs="http://example.com/wsp#ABC" />
  ...
</wsdl:definition>
```

WS-PolicyAttachment を使っていることを宣言

URIによりポリシーを参照

ポリシー

```
<wsp:Policy
    xml:base="http://example.com/wsp"
    wsu:Id="ABC">
  ...
</wsp:policy>
```

ポリシーのURIを定義

Webサービスを支えるセキュリティ技術

- OASIS WSS
- **OASIS WS-SX**
  - WS-SXを取り巻くセキュリティ仕様
  - WS-SX仕様概説
  - **WS-SX TCでの標準化状況**
- 関連する標準化の動き

これまでの状況

- 2005年7月
  - WSS TC電話会議の中で3仕様をOASISに提出することが表明される
- 2005年10月
  - OASISからWS-SX TC設立のアナウンス
- 2005年12月
  - Redmond, WAにおいて最初のF2F (標準化作業開始)
  - 日本からは西村(富士通)が参加
  - Member 37組織73人 (うちVoting Member 32組織62人)
- 2006年4月
  - Austin, TXにおいて2回目のF2F
- 2006年5月18日現在
  - Member 49組織97人 (うちVoting Member 19組織41人)
  - 日本企業では富士通、リコーが参加

今後の予定

- 相互運用テストなどで問題点を洗い出し、その結果を反映した仕様をCommittee Draftに
- 2006年10月 第3回F2F (Ottawa, Ontario? Burlington, MA? San Jose, CA?)
- 60日以上のPublic Review (OASISプロセス)
- 2007年6月(最初のF2Fから18ヶ月)までにCommittee Specification (当初予定)

Webサービスを支えるセキュリティ技術

- OASIS WSS
- OASIS WS-SX
- 関連する標準化の動き
  - **W3C**
  - **WS-I**

W3CへのWS-Policy提出

- 2002年12月の仕様公開
  - 以降、なかなか標準化の場に出ない→IPRの懸念など
- 2006年4月
  - 19社がWS-PolicyとWS-PolicyAttachmentをW3Cに提出
  - 提出物をベースにWeb Services PolicyのためのW3C Recommendationを作るWorking Groupの創設を提案
  - 特許については、W3C Royalty-Free licensing requirementsにしたがったライセンスを提供することが明記

(http://www.w3.org/Submission/2006/06/)

WS-Policy提出の影響

- WS-SecurityPolicyが深く関係
- WS-Trustからも参照
- WS-SX TCのチャータでは、非標準仕様の排除を明記

> If any of the above specifications is outside of a standardization process at the time this TC moves to ratify its deliverables, or is not far enough along in the standardization process, any normative references to it in the TC output will be expressed in an abstract manner, and the incarnation will be left at that time as an exercise in interoperability.

(http://www.oasis-open.org/committees/ws-sx/charter.php)

- WS-AddressingのW3C Recommendation化(2006/5/9)もあり、WS-SXでの標準化における懸念の1つは取り除かれそう

WS-Policyの関連仕様であるWS-MetadataExchangeは、まだ標準化団体に提出されていない点には今後も注意が必要

WS-I Basic Security Profile

- Basic Security Profile 1.0
  2006年3月に、1文書にしたWorking Group Draftを公開

SWA Profile (V1.1)	Kerberos Token Profile (V1.1)
Username Token Profile (v1.0)	REL Token Profile (V1.0)
X.509 Token Profile (V1.0)	SAML Token Profile (V1.0)
OASIS Web Services Security (V1.0)	
Transport Security (HTTP over TLS)	

- Basic Security Profile 1.1はOASIS Web Services Security V1.1をカバー

WS-I Reliable Secure Profile

- 2006年5月1日発表
- セキュアで高信頼なメッセージングのためのガイダンスを提供
- Reliable Secure Profile (RSP) 1.0は次の仕様をカバー
  - OASIS WS-ReliableMessaging 1.1
  - OASIS WS-SecureConversation 1.3

WS-I Announces New Profile Work for 2006

(http://www.ws-i.org/docs/press/20060501wsipr.doc)

WS-I Reliable Secure Profile

- WS-RMでは曖昧になっている下位層とのバインディングについて、相互運用性を確保できるよう、オープンな標準プロトコルへのバインディングを示すことをチャータに明記

> RSP 1.0 must list or denote the different options for binding to the underlying open standard protocol the various kinds of messages and their patterns of exchange, described in the specifications directly referenced by this charter - e.g. how the back-channel of a 2-way protocol may be used.
> (Working Group Charter: Reliable Secure Profile 1.0の4. Scope of Effortより
> http://www.ws-i.org/docs/charters/RSP_Charter1-0.pdf)

Working Group Charter:

Reliable Secure Profile 1.0

(http://www.ws-i.org/docs/charters/RSP_Charter1-0.pdf)

まとめ

- OASIS WSS TCでのWS-Securityの標準化に続いて、OASIS WS-SX TCにおいてWS-Trust、WS-SecureConversation、WS-SecurityPolicyの標準化が進行中
  - WS-Trustはセキュリティ・トークン・サービスにアクセスするためのプロトコルを提供
  - WS-SecureConversationは安全なセッションでのメッセージ交換を提供
  - WS-SecurityPolicyはセキュリティに関するポリシー・アサーションの記述手段を提供
- W3C、WS-Iにも関連する動きがあり、特にWS-PolicyがW3Cに提出されたことでWS-SXでの標準化における懸念の1つは取り除かれそう
  - WS-Federation、WS-MetadataExchangeなど注意が必要な仕様もまだある
- Webサービスのセキュリティ仕様の標準化が進むことにより、誰でも安心して利用できる、相互運用可能で安全なWebサービスが実現可能になる

参考

- OASIS
  (Organization for the Advancement of Structured Information Standards)
  http://www.oasis-open.org
  - WSS TC
    http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
  - WS-SX TC
    http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ws-sx
- W3C
  (World Wide Web Consortium)
  http://www.w3.org/
- WS-I
  (Web Services Interoperability Organization)
  http://www.ws-i.org/