XML署名 (電子署名ツール) 検証報告

2009年5月12日 XMLコンソーシアムWeek

セキュリティ部会
宮地 直人 (ラング・エッジ)

XML署名/検証報告
活動の概要

- 標準でXML署名に対応したフレームワークを検証/調査
  - 1) Sun Java6 / XMLSignature に関する調査
    環境：Windows XP SP3 + Sun JDK 6 Update 13 + Eclipse 3.4.2
  - 2) MS .NET Framework / SignedXml に関する調査
    環境：Windows XP SP3 + .NET Framework 3.5 SP1 + Visual Studio 2005 C#
- 主な検証/調査項目
  - XML署名で一般的な各署名方式による相互運用性の確認
  - SHA-2 (SHA-256/384/512) への対応状況の確認
  - 署名で重要なXML正規化 (C14N) の単独利用の確認
  - PKCS#12ファイルやWindows証明書ストアの利用方法確認
  - その他XML署名の基本的なオプションへの対応状況を確認

XML署名/検証報告
相互運用性の確認1

- 署名方式1：別ファイルへのDetached (外包)
  - .NET Framework / Java6 間での相互運用性：OK

```
<Signature xmlns="http:.../xmldsig#">
   <SignedInfo>
      <Reference URI="target.xml">
   </SignedInfo>
   ...
</Signature>
```

DetachedOut.xml

```
<MyData xmlns="">
   <Data>...</Data>
</MyData>
```

Target.xml

※ ただしJava6ではDOMValidateContext.setBaseURI()が必要だった

XML署名/検証報告
相互運用性の確認2

- 署名方式2：同一ファイル内のDetached（外包）
  - .NET Framework / Java6 間での相互運用性：OK

```
<MyData xmlns="">
   <Data Id="D1">...</Data>
   <MySign>
      <Signature xmlns="http:.../xmldsig#">
         <SignedInfo>
            <Reference URI="#D1">
         </SignedInfo>
         ...
      </Signature>
   </MySign>
</MyData>
```

DetachedIn.xml

XML署名/検証報告
相互運用性の確認3

- 署名方式3：**Enveloped**（埋め込み）
  - .NET Framework / Java6 間での相互運用性：**OK**

Enveloped.xml

```
<MyData xmlns="">
  <Data>...</Data>
  <Signature xmlns="http:.../xmldsig#">
    <SignedInfo>
      <Reference URI="">
        ...<Transform Algorithm="...#enveloped-signature">...
      </Reference>
    </SignedInfo>
    ...
  </Signature>
</MyData>
```

XML署名/検証報告
相互運用性の確認4

- 署名方式4：**Enveloping**（内包）
  - .NET Framework / Java6 間での相互運用性：一部問題あり

```
<Signature xmlns="http:.../xmldsig#">
   <SignedInfo>
      <Reference URI="#MyObjId">
   </SignedInfo>
   ...
   <Object  Id="MyObjId">
      <MyData xmlns="">
         <Data>...</Data>
      </MyData>
   </Object>
</Signature>
```

Enveloping.xml

XML署名/検証報告
XMLへのEnvelopingの問題

- Envelopingの署名対象XMLに名前空間名指定が無い
  - .NET Framework と Java6 間で検証に失敗する

```
<MyData xmlns="">
   <Data>...</Data>
</MyData>
```

相互運用性が無い例

- Envelopingの署名対象XMLに名前空間名指定がある
  - .NET Framework と Java6 間で検証は成功する

```
<MyData xmlns="http://xmlconsortium.org/MyTest">
   <Data>...</Data>
</MyData>
```

相互運用性がある例

XML署名/検証報告
XMLへのEnvelopingの問題確認

- .NET Framework の Envelopingの正規化結果
  - 署名後のダイジェスト値で確認、正しいと思われる

```
<Object xmlns="http://www.w3.org/2000/09/xmldsig#" Id="MyObjectId">
 <MyData xmlns="">
  <Data>...</Data>
 </MyData>
</Object>
```

.NET Framework 正規化例

- Java6 の Envelopingの正規化結果
  - 署名後のダイジェスト値で確認、xmlns=“” が省略されている

```
<Object xmlns="http://www.w3.org/2000/09/xmldsig#" Id="MyObjectId">
 <MyData>
  <Data>...</Data>
 </MyData>
</Object>
```

Java6 正規化例

※ 見やすくする為に改行や空白文字を加えています。

XML署名/検証報告
SHA-2への対応の確認

- **Reference要素のダイジェスト方式としてSHA512を指定**
  - .NET Framework / Java6 の両方で対応していた
- **XML署名方式としてRSA-SHA512を指定**
  - .NET Framework / Java6 の両方で未対応であった
- **XML以外の署名方式としてRSA-SHA512を指定**
  - .NET Framework では未対応であった
    - IEのSSL等ではRSA-SHA2証明書等には対応済み
  - Java6 では対応していた

➢ システムでは対応済みでもXML署名機能では使えない？

➢ XML署名機能は追加であり対応が遅いのかもしれない？

XML署名/検証報告
その他機能の確認

- XML正規化（C14N 1.0）の単独利用
  - .NET Framework / Java6 の両方で利用可能だった
  - ただし C14N 1.1 には未対応のようだ（W3CのUpdateで追加）
- PKCS#12ファイルやWindows証明書ストアを利用
  - .NET Framework / Java6 の両方で利用可能だった
- KeyInfoのIdをReference先に含める
  - .NET Framework ではうまく使えない？ → 今後の課題
  - Java6 では利用可能だった
- 同一ファイル内の複数署名や複数Referenceの指定
  - .NET Framework / Java6 の両方で利用可能だった

XML署名/検証報告
.NET Framework (SignedXml) の考察

- MSDNにサンプルも多く利用手順もJava6より容易か
  - 個人的にはWindows環境に限れば使いやすいように感じた
  - XML暗号を行う EncryptedXml クラスも提供されている
- 今後CryptoAPIはCNG (Cryptography Next Generation) に移行
  - Vista/Server2008 からサポートが開始された新API
  - CNGでXML署名やXML暗号の機能はあるのか？要調査
  - SignedXml等のAPIは今後もサポートされるのか？
- 新しいアルゴリズムへの対応 (SHA-2等)
  - SHA-2はダイジェストとしては提供されているので対応して欲しい
  - 新規格にはオープンソース系やベンダー系の方が対応が早い？

XML署名/検証報告
Java6 (XMLSignature)の考察

- SignedXmlに比べるとやや行数が多くなる傾向があり面倒
  - ただしこれは慣れの問題でありJava中心のプログラマなら問題ない
  - もっとサンプルが提供されると良いと感じた
- Java6にて標準で提供されたことは評価できる
  - IBM版Java6での対応と相互運用性も期待したい
- 新しいアルゴリズムへの対応 (SHA-2等)
  - SHA-2はダイジェストとしては提供されているので対応して欲しい
  - 新規格にはオープンソース系やベンダー系の方が対応が早い？
  - Apache版XML署名ではRSA-SHA2に対応しているようだ
- Base64変換の機能が標準で欲しい
  - XMLを使ったPKI実装ではバイナリをBase64化する事が多い

XML署名/検証報告
まとめ

- Envelopingの名前空間名無しの相互運用性問題
  - どちらかが間違っている？XML正規化（C14N）の問題か？
  - 今回の実装の問題なら良いが間違いがあれば修正を期待したい
  - 安全策を取るなら署名対象には名前空間名を指定しておくべき
- 新アルゴリズムへの対応
  - RSA2048bit/SHA2対応は米国2010年/日本2013年目標
  - PKIでは新アルゴリズム対応は重要であり早期対応を願う
- Java6も善戦している（実は今回初めて使った）
  - 初めて標準実装されたAPIだが必要な基本機能は揃っていた
- 今回実装した.NET Framework/Java6のサンプルプログラム
  - セキュリティ部会のSNSに置いてあります