EXTENDING XML SIGNATURE AND APPLYING IT TO WEB PAGE SIGNING

Takahito Tsukuba, Kenichiro Noguchi
Department of Information and Computer Science, Kanagawa University, 2946 Tsuchiya, Hiratsuka-shi 259-1293, Japan

Keywords: XML Signature, X.509 certificate, Web page signing, XML security, World Wide Web security.

Abstract: Security technologies for XML, the XML Encryption and the XML Signature developed by the World Wide Web Consortium, will play a vital role in security on the Internet. A binary X.509 certificate encoded in ASN.1 is included in the XML Signature. We propose to extend the XML Signature to fully represent X.509 certificate information in XML. We developed the specifications for extensions. We implemented a converter that transforms between the ASN.1 representation and XML representation of an X.509 certificate that was aimed to verify the validity of our proposal. World Wide Web security is an important issue on the Internet and trusted information is critical. We experimented with Web page signing, applying the extended XML Signature. We propose the scheme for signed Web pages based on the XML Signature. We conducted a test implementation of the scheme with the extended XML Signature. We verified that the proposed scheme could easily be implemented and incorporated into the current Web environment as well as the effectiveness of the extended XML Signature. The paper concludes by identifying necessary areas for future standardization.

1 INTRODUCTION

Security on the Internet has become a critical issue in today's society. Various technologies for security have been developed, and among them are the XML Encryption (W3C, 2002a) and the XML Signature (W3C, 2002b) developed by the World Wide Web Consortium. Related data are basically represented in XML in the XML Encryption and the XML Signature. However, as for an X.509 certificate, which is an important construct to convey public key information securely, a binary X.509 certificate encoded in ASN.1 is included as specified in XML Signature Recommendation. In this paper, we propose to extend the XML Signature to fully represent X.509 certificate information in XML. With our proposal, the general characteristic of XML that data described in XML are machine-processable and at the same time are human-readable is realized for XML Signature data as well. The characteristic is especially beneficial for security related data, because a human can directly read and check the raw data.

Our approach is to encode X.509 certificate data in XML, which is different to encoding ASN.1 data in XML as is done in ASN.1 XER (ITU, 2003). We developed the specifications for the extensions. We implemented a converter that transforms between the ASN.1 representation and XML representation of an X.509 certificate, aiming to verify the validity of our proposal.

An important issue on the Internet is World Wide Web security. The Web has become so extensively used in real life that trusted information on the Web is critical. If a Web page is digitally signed, its authenticity is guaranteed and users can be confident that its content has not been tampered with. We experimented with Web page signing applying the extended XML Signature, aiming to verify the effectiveness of the proposed extended XML Signature.

We propose the scheme for signed Web pages based on the XML Signature which is applicable to both HTML and XHTML. We conducted a test implementation of the scheme with the extended XML Signature. We verified that the proposed scheme could easily be implemented and incorporated into the current Web environment as well as the effectiveness of the extended XML Signature.

Areas for future standardization were identified through our study.

Tsukuba T. and Noguchi K. (2006).
EXTENDING XML SIGNATURE AND APPLYING IT TO WEB PAGE SIGNING.
In *Proceedings of the International Conference on Security and Cryptography*, pages 407-412
DOI: 10.5220/0002096204070412

2 PROPOSED EXTENSIONS TO XML SIGNATURE

We propose extensions to the XML Signature to represent X.509 certificate information in XML. We implemented a converter that transforms a binary X.509 certificate encoded in ASN.1 to one encoded in the XML form we propose and vice versa, and verified the validity of our proposal.

2.1 XML Encoding of X.509 Certificates

X.509 certificates, as specified by the ITU Recommendation (ITU, 2000), are encoded according to ASN.1 (Abstract Syntax Notation 1) (ITU, 2002a) encoding rules. In the XML Signature Recommendation, information is basically encoded in XML. However, as for X.509 certificate related information, which is contained in the X509Data element, only information to identify an X.509 certificate such as the X.509 issuer serial number or the X.509 subject name is contained in XML elements. X.509 certificate information, if present, is contained as a Base 64 encoded binary value encoded in ASN.1 DER (ITU, 2002b) in the X.509Certificte element, which is the child element of the X.509Data element. Public key information can be contained in XML elements, which are separate from the X509Data element, independently of an X.509 certificate. If all information in an X.509 certificate is encoded systematically in XML, all the data of XML Signature become human-readable and a human will be able to directly read and check the data.

We extended the XML Signature to include *XML encoding of X.509 certificates*. We defined the specifications for encoding taking the current recommendation and ASN.1 encoding of X.509 certificates into account. We introduced ten new elements, which are listed in Table 1. The contents of some existing elements have been modified. The X509Data element is a root element now having two child elements, i.e., the X509Certificate and X509Signature, and the X509Certificate element now has child elements for certificate data. Our approach is to encode X.509 certificate data in XML, which is different from encoding ASN.1 data in XML as is done in ASN.1 XER (ITU, 2003).

Table 1: Newly introduced elements for XML encoding of X.509 certificates.

Element Name	Explanation
X509SignatureAlgorithm	Name of algorithm used for signature
X509Validity	Valid period of certificate
X509notBefore	Child element of X509Validity
X509notAfter	Child element of X509Validity
X509SubjectPublicKeyInfo	Subject's public key information
X509SubjectPublicKeyAlgorithm	Child element of SubjectPublicKeyInfo
X509SubjectPublicKeyExponent	Child element of SubjectPublicKeyInfo
X509SubjectPublicKeyModulus	Child element of SubjectPublicKeyInfo
X509Signature	Signature for certificate
X509SignatureValue	Child element of X509Signature

2.2 Experiment on Converting Encoding for X.509 Certificates

We experimented with automatically converting the encoding for X.509 certificates, from ASN.1 encoding to XML encoding and vice versa. The experiment had two objectives; the first was to verify the validity of the XML encoding we propose and the second was to make a prototype of the migration tool.

We introduced an intermediate format to convert the encoding, i.e., XML encoding of ASN.1 data similar to ASN.1 XER. ASN.1 specifies the structure of the data in terms of types and values, and the intermediate format is a direct representation of that structure in XML. A type represented as identifier octets and a value represented as content octets in ASN.1 are represented as an XML element with the same name and as the content of the element in the intermediate format, respectively. The binary value is Base 64 encoded in the intermediate format.

The structure of the conversion tool, the *X.509 Encoding Converter*, is outlined in Figure 1. The tool consists of four programs. ASN12IF transforms an X.509 certificate encoded in ASN.1 to one in the intermediate format. IF2XML transforms an X.509 certificate in the intermediate format to one in XML. XML2IF and IF2ASN1 perform reverse transformations of IF2XML and ASN12IF, respectively.

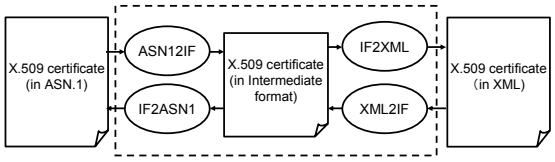

Figure 1: Structure of X.509 Encoding Converter.

The signature part of an X.509 certificate is also transformed like the other parts. Therefore, reverse conversion to ASN.1 encoding is necessary before validating the signature in XML encoding.

The converter is implemented in Java and utilizes DOM and XSLT for XML processing. The converter can transform encoding of X.509 certificates in both directions. The reverse transformation of an X.509 certificate in XML encoding can completely restore the original form in ASN.1 and the signature of the certificate can be validated.

There are examples of transformation results in Figure 2, which shows an X.509 certificate in the intermediate format, and in Figure 3, which shows one in XML encoding.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <SEQUENCE>
  - <SEQUENCE>
      <INTEGER>1120683489</INTEGER>
    - <SEQUENCE>
        <OBJECTIDENTIFIER>MD5 with RSA encryption</OBJECTIDENTIFIER>
        <NULL />
      </SEQUENCE>
    - <SEQUENCE>
      - <SET>
        - <SEQUENCE>
            <OBJECTIDENTIFIER>C</OBJECTIDENTIFIER>
            <PRINTABLESTRING>JP</PRINTABLESTRING>
          </SEQUENCE>
        </SET>
        :
      - <SET>
        - <SEQUENCE>
            <OBJECTIDENTIFIER>CN</OBJECTIDENTIFIER>
            <PRINTABLESTRING>Tsukuba Takahito</PRINTABLESTRING>
          </SEQUENCE>
        </SET>
      </SEQUENCE>
    - <SEQUENCE>
        <UTCTIME>050706205809Z</UTCTIME>
        <UTCTIME>051004205809Z</UTCTIME>
      </SEQUENCE>
        :
```

Figure 2: Transformation result example: Intermediate format (part).

```
<?xml version="1.0" encoding="UTF-8" ?>
- <X509Data>
  - <X509Certificate>
      <X509SignatureAlgolithm>MD5 with RSA encryption</X509Sig
    - <X509IssuerSerial>
        <X509IssuerName>CN=Tsukuba Takahito, OU=Noguchi La
          ST=Kanagawa, C=JP</X509IssuerName>
        <X509SerialNumber>1120683489</X509SerialNumber>
      </X509IssuerSerial>
    - <X509Validity>
        <X509notBefore>050706205809Z</X509notBefore>
        <X598notAfter>051004205809Z</X598notAfter>
      </X509Validity>
      <X509SubjectName>CN=Tsukuba Takahito, OU=Noguchi Lal
        ST=Kanagawa, C=JP</X509SubjectName>
    - <X509SubjectPublicKeyInfo>
        <X509SubjectPublicKeyAlgorithm>RSA encryption</X509Sul

          <X509SubjectPublicKeyModulus>5299668950643892212
        <X509SubjectPublicKeyExponent>65537</X509SubjectPublic
      </X509SubjectPublicKeyInfo>
    </X509Certificate>
  - <X509Signature>
      <X509SignatureAlgolithm>MD5 with RSA encryption</X509Sig

        <X509SignatueValue>AEMHtDGm1cLx2+16Y4tDvCEMMkH
        ELI2VxSUsGTwlEkEnK8M3ecz8JMXY+wZvr+G/CxLhXrfR
        ypCJwSZHr5DF+tpJ18yX</X509SignatueValue>
    </X509Signature>
</X509Data>
```

Figure 3: Transformation result example: XML encoding (part).

3 APPLICATION OF EXTENDED XML SIGNATURE TO WEB PAGE SIGNING

We applied the extended XML Signature to Web page signing. We propose the scheme for signed Web pages based on the XML Signature which is applicable to both HTML and XHTML. We conducted a test implementation of the scheme with the extended XML Signature. The experiment served to verify the effectiveness of the extended XML Signature.

3.1 Scheme for Signed Web Pages

We established three principles for designing the scheme for signed Web pages:

- To comply with the XML Signature Recommendation as extended with our proposal.
- To minimize the effect on HTML/XHTML.
- To allow a page with multiple contents to be signed.

To position the signature information, we selected a detached form, instead of an enveloping or enveloped form, specified by the XML Signature Recommendation. Signature information in this form exists separately from the Web page to be

signed, so its effect on the Web page format is minimized.

A *signature file* is created for each Web page to be signed, which contains signature information in XML in accordance with the XML Signature Recommendation. The following information is stored in the file:

- A signed information element that contains reference elements. Each reference element has a reference (i.e., URI) to each file (e.g., an HTML/XHTML file and an image file) of a Web page, and contains the digest value of the content of the file.
- A signature value, which is the result of signing to the signed information element.
- Public key information, which contains an X.509 certificate in XML encoding.

We needed to establish a link between the Web page to be signed and the corresponding signature file. To attain this, we extended HTML/XHTML to include a new tag, a *sign tag*. The tag has a reference (i.e., URI) to the signature file and is inserted in the head element of an HTML/XHTML file. A sign tag for XHTML (W3C, 2002c) has the following format:

```
<sign
xmlns="http://www.nol.info.kanagawa-
u.ac.jp/sign" signref="URI"/>
```

Using an XML name space prevents names from colliding with those in XHTML.

Figure 4 outlines the scheme for signed Web pages.

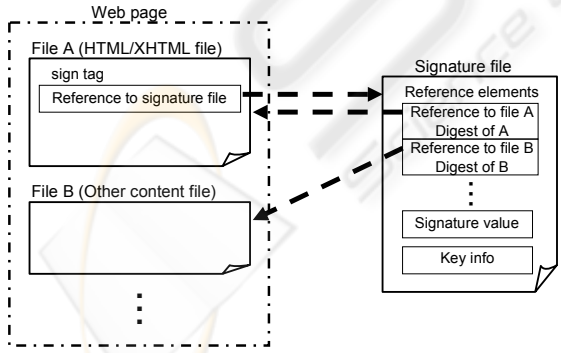

Figure 4: Scheme for signed Web pages.

3.2 Test Implementation

We conducted a test implementation of our proposed Web page signing, which included the *signing program* and the s*ignature validation program*. The latter was incorporated into the *test browser*.

The signing program accepts a list of URIs for the content files of the Web page to be signed, an X.509 certificate that contains the public key, and the corresponding private key as input. The program executes signature calculation and creates a signature file as output. This program is to be used on the Web server side. Because the program is basically an implementation of the signing phase for the extended XML Signature, it can generally be used to sign any files.

The signature validation program accepts an HTML/XHTML file for the Web page to be validated as input. The program finds the sign tag and obtains the signature file. The signature value in the signature file, which is to the signed information element, is next validated using the public key in the X.509 certificate element. If this is successful, then the digest value in each reference element is checked for whether it matches the actual digest value of each file of the Web page. If all checks are successful, the program reports validation has been successful, otherwise it reports failure.

The signature validation program was incorporated into the test browser to see whether the proposed Web page signing worked satisfactorily in a real-use environment. We utilized a sample browser described in the literature (Flanagan, 2000) as the basis of the test browser. We added a *Validate button* in the tool bar of the browser window. When the button is pressed, the signature validation program is internally invoked, and the signature for the Web page currently displayed in the browser window is validated. The validation results are displayed as a message in the status bar of the browser window. Figure 5 outlines the Web page validation process.

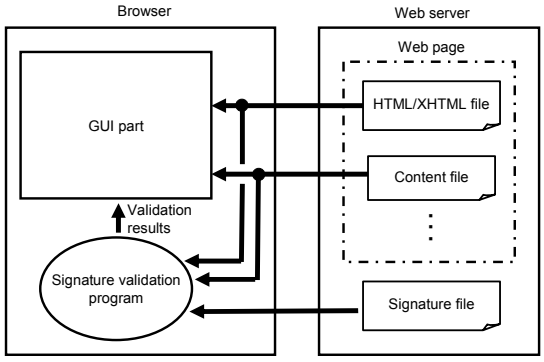

Figure 5: Flow for signature validation of signed Web page.

The test implementation is in Java. It uses RSA as the signature algorithm and SHA-1 as the digest algorithm. We omitted the canonicalization processing of XML data from the test implementation. We also omitted the validation processing of the X.509 certificate from the signature validation program. Because of this, all the processing was consistently realized as XML and HTML/XHTML processing, with no ASN.1 processing involved.

The test implementation was successful and users could verify the authenticity of Web pages with a simple action. Figure 6 shows an example Web page with a sign tag inserted, Figure 7 has its signature file created with the signing program, and Figure 8 shows the test browser window after successful validation.

```
<HTML>
<HEAD>
<SIGN signref="http://www.nol.info.kanagawa-u.ac.jp/test/Sign01.xml">
</HEAD>
<BODY>
<H1>Signed Web Page with Extended XML Signature</H1>
<P>This page is signed with the Extended XML Signature.</P>
<P>This page has multiple contents.</P><BR>
<IMG src="http://www.nol.info.kanagawa-u.ac.jp/test/Fuji.jpg">
</BODY>
</HTML>
```

Figure 6: An example of source text for signed Web page in HTML (sign tag format is for HTML).

```
<?xml version="1.0" encoding="UTF-8" ?>
- <Signature>
  - <SignedInfo>
      <CanonicalizationMethod />
      <SignatureMethod />
    - <Reference URI="http://www.nol.info.kanagawa-u.ac.jp/test/Test.h
        <DigestMethod />
        <DigestValue>b5992da40c11345de330e18780ed3b108b5094e8</D
      </Reference>
    - <Reference URI="http://www.nol.info.kanagawa-u.ac.jp/test/Fuji.jp
        <DigestMethod />
        <DigestValue>0458e3600ea2376b826b56a68f43345df2a87bc7</Dig
      </Reference>
    </SignedInfo>

    <SignatureValue>GRncPBEpwe3OY9BG8CS0ST0rDP3ZdaAxDVuwqVNd
    zBGTPM9MxHmlixbkp1OWJuuWP4uGmcbxnaQ9fLno/mFjDJFEBPWC
    W5VA2kFlAogRtiBT1IA=</SignatureValue>
  - <KeyInfo>
    - <X509Data>
      - <X509Certificate>
          <X509SignatureAlgolithm>MD5 with RSA encryption</X509Signature
        - <X509IssuerSerial>
            <X509IssuerName>CN=Tsukuba Takahito, OU=NOL, O=KU, L=Hir
              C=JP</X509IssuerName>
            <X509SerialNumber>1133929580</X509SerialNumber>
          </X509IssuerSerial>
        - <X509Validity>
            <X509notBefore>051207042620Z</X509notBefore>
            <X598notAfter>060307042620Z</X598notAfter>
          </X509Validity>
          <X509SubjectName>CN=Tsukuba Takahito, OU=NOL, O=KU, L=Hir
            C=JP</X509SubjectName>
        - <X509SubjectPublicKeyInfo>
            <X509SubjectPublicKeyAlgorithm>RSA encryption</X509SubjectPu
```

Figure 7: An example of signature file of signed Web page (part).

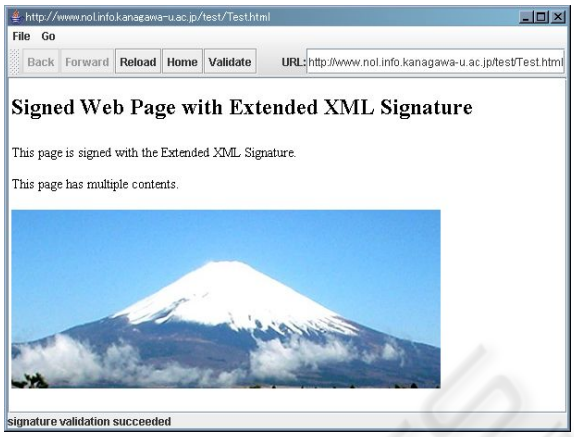

Figure 8: Test browser window (After successful signature validation).

If users access the signature file with their usual browsers, the content of the file is displayed as XML text. It is an advantage of representing information in XML that users can read and check the content of the signature file including X.509 certificate information.

4 DISCUSSION

We proposed extensions to the XML Signature to include XML encoding of X.509 certificates. Our proposal means all information in an X.509 certificate is encoded in XML, which simplifies the processing of the XML Signature without involving ASN.1 processing. One exception is the handling of the signature of a certificate. It is strongly recommended that the new XML based certificate format with a signature to XML encoded information be standardized.

Our proposal for XML encoding of X.509 certificates is for the version 1 format of X.509 certificates. Further work to cover version 2 and 3 formats is necessary.

A study to represent X.509 certificates in XML was reported (Imamura et al., 2000). However, their approach was to represent them in a format similar to our intermediate format.

We proposed the scheme for signed Web pages based on the XML Signature. The scheme has little effect on the current Web scheme. The test implementation revealed that the proposed scheme could easily be implemented and incorporated into the current Web environment. Users can verify the authenticity of Web pages with a simple action.

The benefits of XML, whereby programs can easily handle XML encoded information and users

can also read the information, were attained by applying XML encoding to X.509 certificates in the test implementation for signing Web pages.

Current browsers such as Microsoft Internet Explorer (Microsoft) and Mozilla Firefox (Mozilla) have capabilities to handle signed resources. However, they do not provide an easy way of signing a whole Web page, and their capabilities are browser-specific. A method of signing Web pages using PGP was proposed (Bell, 1996) and is used on the Web. Our proposal has advantages in that because it is based on the XML Signature, it matches Web technology (HTML/XHTML) and any browser can implement it.

We tentatively proposed adding a new tag to HTML/XHTML for a signed Web page to refer to the signature information of the page. In the future, such capabilities will need to be specified to conform with the meta-information capabilities of the Semantic Web.

5 CONCLUSION

We proposed extensions to the XML Signature Recommendation to include XML encoding of X.509 certificates. With our proposal, full X.509 certificate information can be represented in XML. We implemented an encoding converter that transforms between the ASN.1 encoding and XML encoding of X.509 certificates and verified the validity of our proposal.

We applied the extended XML Signature to Web page signing. We proposed the scheme for signed Web pages based on the XML Signature and conducted a test implementation. We verified that the proposed scheme could easily be implemented and incorporated into the current Web environment, as well as the effectiveness of the extended XML Signature. Users can verify the authenticity of Web pages with a simple action as we did in the test implementation.

Areas for future standardization were identified through our study. These are a fully XML based digital certificate format with a signature to XML encoded information, an enhanced XML Signature Recommendation incorporating the fully XML based digital certificate, and an scheme for XML Signature based Web page signing with possible extensions to HTML/XHTML. Another area is a unified Web page signing scheme and the Semantic Web scheme. We believe this study will help accelerate standardization in these areas.

REFERENCES

W3C, 2002a. XML Encryption Syntax and Processing. W3C Recommendation 10 December 2002. http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

W3C, 2002b. XML-Signature Syntax and Processing. W3C Recommendation 12 February 2002. http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

W3C, 2002c. XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition). W3C Recommendation 26 January 2000, revised 1 August 2002. http://www.w3.org/TR/2002/REC-xhtml1-20020801

ITU, 2000. Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. ITU-T Recommendation X.509.

ITU, 2002a. Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation. ITU-T Recommendation X.680.

ITU, 2002b. Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). ITU-T Recommendation X.690.

ITU, 2003. Information technology – ASN.1 encoding rules: XML Encoding Rules (XER). ITU-T Recommendation X.693.

Flanagan, D., 2000. Java Examples in a Nutshell, Second Edition. Oreilly & Associates Inc.

Imamura, T. , Maruyama, H., 2000. ASN.1/XML Translator and Its Application to Certification Authorities. In *SCIS2000 (Symposium on Cryptography and Information Security 2000)* (in Japanese)

Mozilla. Network Security Services (NSS). Mozilla org. http://www.mozilla.org/projects/security/pki/nss/

Microsoft. ActiveX Controls. Microsoft Corporation. http://msdn.microsoft.com/workshop/components/activex/activex_node_entry.asp

Bell, N., 1996. PGP signed web-pages. http:// members.aol.com/EJNBell/pgp-www.html