Falsification Prevention and Protection Technologies and Products

XML Signature/Encryption — the Basis of Web Services Security

By Koji MIYAUCHI*

ABSTRACT XML is spreading quickly as a format for electronic documents and messages. As a consequence, greater importance is being placed on the XML security technology. Against this background research and development efforts into XML security are being energetically pursued. This paper discusses the W3C XML Signature and XML Encryption specifications, which represent the fundamental technology of XML security, as well as other related technologies originally developed by NEC.

KEYWORDS **XML security, XML signature, XML encryption, Distributed signature, Web services security**

1. INTRODUCTION

XML is an extendible markup language, the specification of which has been established by the W3C (WWW Consortium). It is spreading quickly because of its flexibility and its platform-independent technology, which freely allows authors to decide on document structures. Various XML-based standard formats have been developed including: ebXML and RosettaNet, which are standard specifications for e-commerce transactions, TravelXML, which is an EDI (Electronic Data Interchange) standard for travel agencies, and NewsML, which is a standard specification for new distribution formats.

As the popularity of XML becomes established, a greater importance is being placed on security technology for data the represented in XML. This means that XML needs to include features that can deal with security risks, including falsification and eavesdropping on data that is being transmitted over communication paths, such as the Internet, as well as on spoofing and repudiation.

In order to solve these problems, W3C, OASIS, and other standards organizations are working to establish standards specifications for XML security. In particular, the XML Signature and XML Encryption specifications established by the W3C can be the basis for all other XML security standards. This paper discusses these specifications and related technologies originally developed by NEC.

*System Platform Software Development Division

2. XML SIGNATURE

2.1 Overview

XML Signature is an electronic signature technology that is optimized for XML data. The practical benefits of this technology include Partial Signature, which allows an electronic signature to be written on specific tags contained in XML data, and Multiple Signature, which enables multiple electronic signatures to be written. The use of XML Signature can solve security problems, including falsification, spoofing, and repudiation.

2.2 XML Signature and Related Specifications

XML Signature was established as a formal version of W3C recommendations in Feb. 2002. W3C has also established related specifications that need to be fulfilled when XML Signature is actually used. The specifications relating to XML Signature are as follows:

- XML-Signature Syntax and Processing: W3C Recommendation 2002/2/12
- Canonical XML Version 1.0: W3C Recommendation 2001/3/15
- Exclusive XML Canonicalization Version 1.0: W3C Recommendation 2002/7/18
- XML-Signature XPath Filter 2.0: W3C Recommendation 2002/11/08

2.3 XML-Signature Syntax and Processing

This specification forms the core of XML Signature. It defines electronic signature formats using XML, the creation of electronic signatures, and rules for verification processing. **Figure 1** shows an

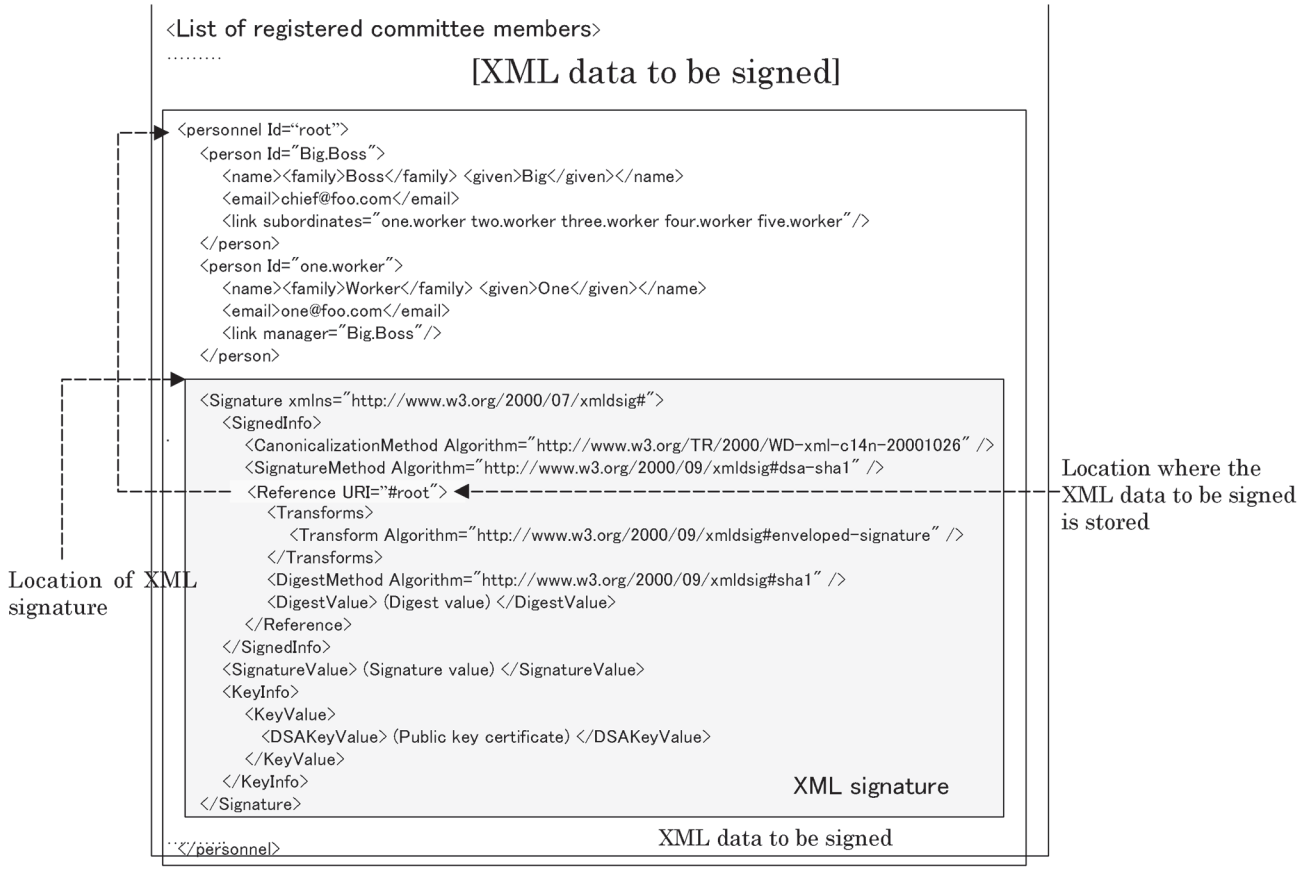

Fig. 1 XML signature format example.

example of an XML signature format and XML data that is XML-signed.

As shown in Fig. 1, an XML signature is a document structure with the <Signature> element at its top. Under the <Signature> element, lie its child elements, including a <SignedInfo> element, which contains references to the algorithm used for the XML signature creation and to the target XML data. It also holds digest value and other information, a <SignatureValue> element that contains the signature value, and a <KeyInfo> element that contains the public key certificate information to be used when the XML signature is verified. When considering the characteristics of XML Signature, the <Reference> element, which is a child element of the <SignedInfo> element is particularly important. Multiple <Reference> elements may be contained in the <SignedInfo> element. This enables any number of XML data segments at any location to be signed. This feature ensures that an extremely flexible system can be built up by using XML Signature.

2.4 Canonical XML/Exclusive XML Canonicalization

Canonical XML is an important specification relating to XML Signature. XML 1.0 is so flexible in document formats that equivalent contents can be expressed in multiple formats. An example is provided below.

(1) <document></document>
(2) <document/>

Both code fragments in (1) and (2) above represent an empty element. They are different in byte representation, but are equivalent as XML data. In addition, the XML 1.0 specification allows equivalent XML data to be expressed in multiple formats in terms of attribute occurrence sequence, blank character handling, and naming space definitions, among others.

However, the electronic signature is a technology based on hash calculation that applies to byte representations of data. The flexibility of the XML 1.0 specification could raise fatal problems in electronic

signatures. Against this background, the Canonical XML specification, which provides for canonical forms that are equivalent to XML data formats, was established ahead of XML signature specifications. Before XML data is signed and verified, it is converted to a canonical form that complies with the Canonical XML specification to ensure that the problem of format variations can be solved in order to allow the use of XML Signature.

On the other hand, Exclusive XML Canonicalization is one of the XML canonicalization specifications. It has been established considering special situations. For example, in consideration that XML-signed XML data A will be added to a child element of XML data B. When XML data B is converted in accordance with the Canonical XML specification, the naming space of XML data A changes because of canonicalization. This will lead to failure in XML signature verification for XML data A. This situation generally occurs when XML-signed XML data is embedded in a SOAP message. To avoid this problem, the Exclusive XML Canonicalization was established as a specification that is based on Canonical XML and excludes naming space and other contexts for the target of canonicalization. This specification is particularly important for Web Services Security, which specifies XML-signed SOAP messages.

3. XML ENCRYPTION

3.1 Overview

XML Encryption is an encryption technology that is optimized for XML data. Its practical benefits include partial encryption, which encrypts specific tags contained in XML data, multiple encryption, which encrypts data multiple times, and complex encryption, such as the designation of recipients who were permitted to decrypt respective portions of data. The use of XML Encryption also helps solve security problems, including XML data eavesdropping.

3.2 XML Encryption and Related Specifications

XML Encryption was established by the W3C as a formal version of W3C recommendations in Dec. 2002. The W3C also established related specifications that solve problems raised when XML Encryption and XML Signature are used in combination. The specifications relating to XML Encryption are as follows:

- XML Encryption Syntax and Processing: W3C Recommendation 2002/12/10
- Decryption Transform for XML Signature: W3C Recommendation 2002/12/10

3.2.1 XML Encryption Syntax and Processing

This specification provides for encryption formats using XML and processing rules regarding encryption and decryption. **Figure 2** shows an XML encryption format and an example of XML-encrypted XML data.

As shown in Fig. 2, XML-encrypted data is of a document structure with the <EncryptedData> element at its top. Under the <EncryptedData> element, lie its child elements, including the <EncryptionMethod> element, which contains information on the algorithm used for encryption, the <KeyInfo> element, which contains information on the decryption key to be used for decryption, and the <CipherData> element, which contains the cipher data. If hybrid encryption is used, the structure can also include the <EncryptedKey> element, which contains the key-encryption key. In addition to XML signatures and in order to ensure that multiple encryption and designation of multiple recipients are possible URIs can also be used to specify what is to be encrypted. This feature enables users to build extremely flexible systems using XML Encryption.

3.2.2 Decryption Transform for XML Signature

The Decryption Transform for XML Signature specification was established to solve problems that are raised when XML Signature and XML Encryption are used at the same time. It provides for a method used to determine whether XML encryption has been applied before or after the XML signature creation. This has been established by the W3C's XML encryption working group as an additional specification with regard to the conversion processing that is performed on XML signatures.

4. NEC'S ORIGINAL TECHNOLOGIES RELATED TO XML SECURITY

The most important point in the field of XML security is to guarantee inter-operability with other products, or to place precedence on compliance with standard specifications. This means that vendors find difficulty in developing discriminating points for their products in this field. NEC has developed the original technologies, Distributed Signature and HTML Signature; has applied for patents of these technologies, and considers that the technologies are discriminating points for the NEC products range. This paper discusses Distributed Signature. It is a technology developed to allow the use of XML Signature on thin clients. NEC's products are being employed in

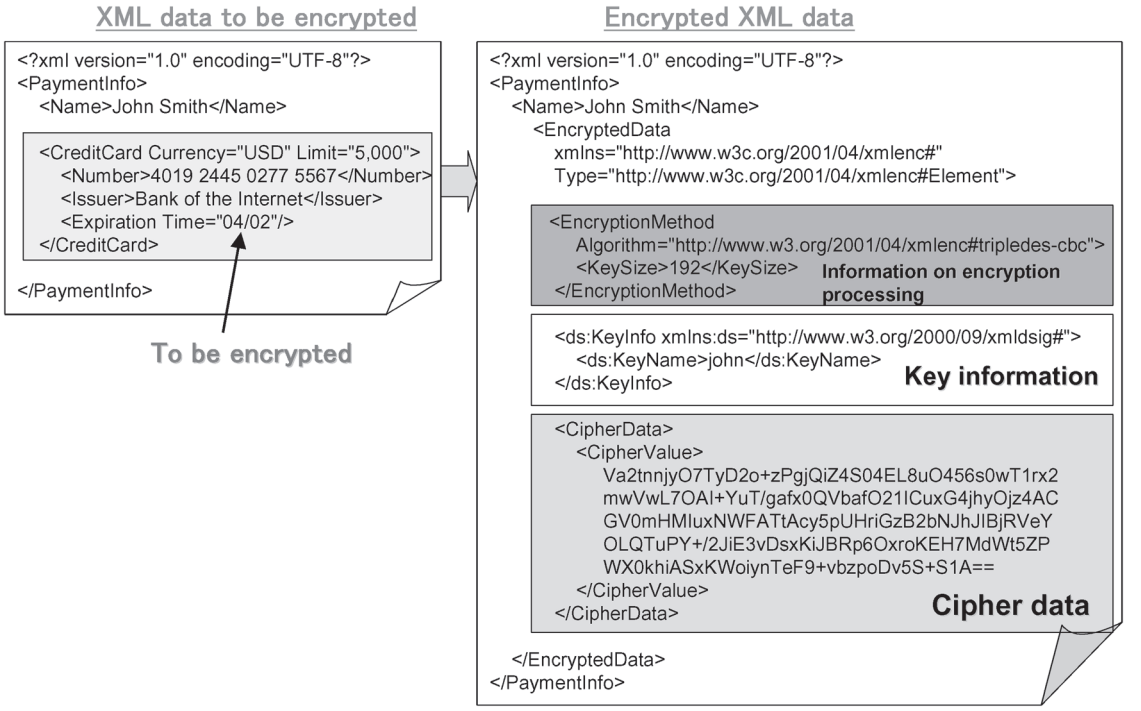

Fig. 2 XML encryption format example.

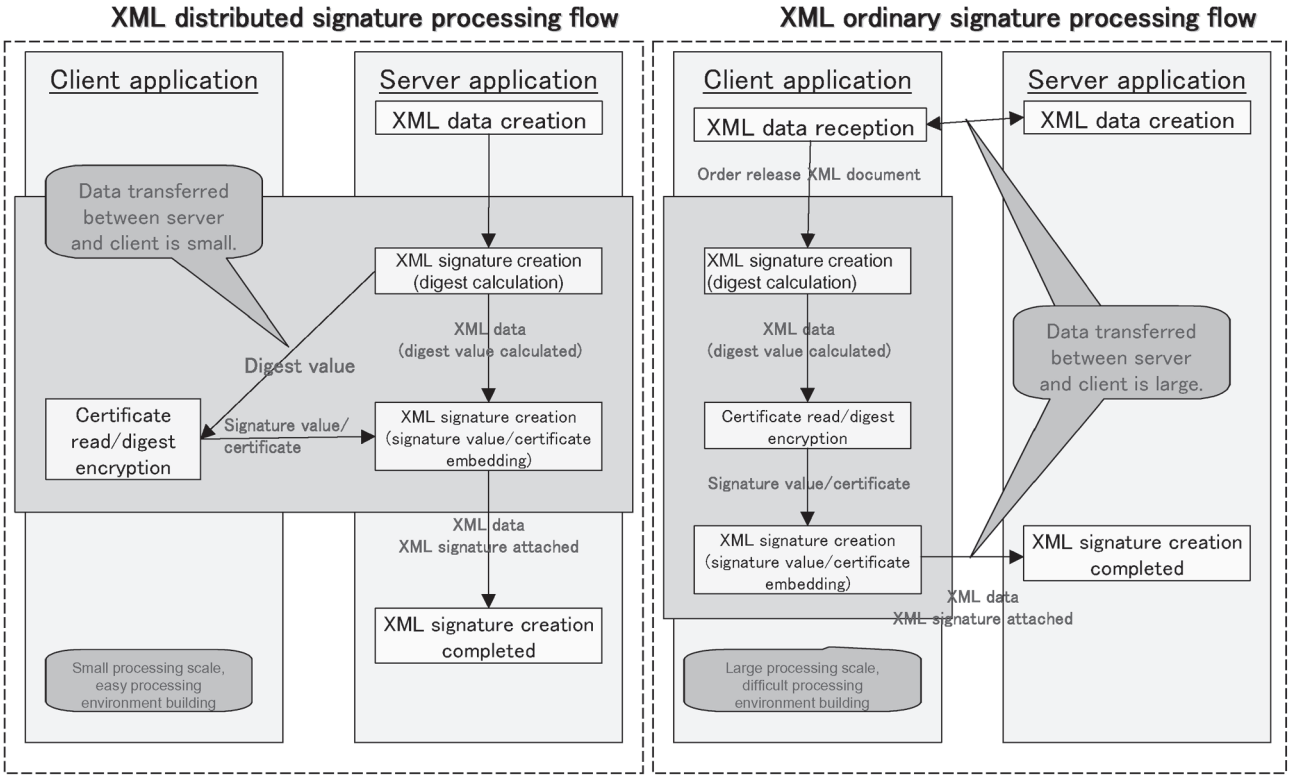

Fig. 3 Comparison between XML distributed signature processing flow and XML ordinary signature processing flow.

multiple system integration projects as a result of this Distributed Signature technology.

4.1 What Is Distributed Signature

Principal problems involved in implementing XML Signature on a thin client are as follows:

- For XML processing, an execution environment, including an XML parser, an XSLT (XML Stylesheet Language Transformations) engine, and Java Runtime, needs to be installed in advance.
- Since XML processing causes relatively high loads, the client machine specification needs to be to a certain extent, a high one.
- If a general Web client is used, it may sometimes be difficult to send/receive XML documents to/from the server because XML documents are likely to be large because of transmission speed restrictions.

Distributed Signature has been developed to solve these problems. With this technology, XML signature creation processing steps are divided into those for the server and the client to ensure that the server and the client cooperate to perform XML signature creation processing.

4.2 Distributed Signature Processing Flow

Figure 3 compares a distributed signature processing flow and an ordinary processing flow.

As shown in this figure, processing performed on the client is limited to the creation of the signature value based on digest value encryption using a secret key and the acquisition of a public key certificate. Therefore, it is not necessary to build a special environment for XML signature creation on the client. In addition, data that is transferred between the server and the client is limited to the digest value, signature value, and public key certificate. Therefore, the amount of data transferred is extremely small. Since the processing steps are distributed to the server and the client computer in this way, the client computer is truly thin in a Web application system that handles electronic applications, electronic contracts, or others.

5. CONCLUSION

XML Signature and XML Encryption, which are the basis for XML security, have been discussed. NEC has continued to be a member of the W3C working group for these technologies since the stage of deciding on the specifications. It has also contributed to the establishment of these technologies by conducting interoperability tests. As a consequence, NEC assumes that a competitive advantage is ensured by high compliance with the specification and its ability to develop original technologies. At present, NEC is undertaking research and development efforts for ID Federation technologies such as Web Services Security, SAML (Security Assertion Markup Language), Liberty Alliance, and other technologies based on this technical advantage. In the future, it is planned to integrate the results of our efforts into an XML security solution.

REFERENCES

[1] XML-Signature Syntax and Processing: W3C Recommendation 2002/2/12, http://www.w3.org/TR/xmldsig-core/
[2] Canonical XML Version 1.0: W3C Recommendation 2001/3/15, http://www.w3.org/TR/xml-c14n
[3] Exclusive XML Canonicalization Version1.0: W3C Recommendation 2002/7/18, http://www.w3.org/TR/xml-exc-c14n/
[4] XML-Signature XPath Filter 2.0: W3C Recommendation 2002/11/08, http://www.w3.org/TR/xmldsig-filter2/
[5] XML Encryption Syntax and Processing: W3C Recommendation 2002/12/10, http://www.w3.org/TR/xmlenc-core/
[6] Decryption Transform for XML Signature: W3C Recommendation 2002/12/10, http://www.w3.org/TR/xmlenc-decrypt

Received November 30, 2004

* * * * * * * * * * * * * * * * *

Koji MIYAUCHI graduated from the Master Course, Information Engineering Department, Engineering Faculty, Nagoya University Graduate School in 1991 and then joined NEC Corporation where he studied GUI implementation and visual programming environments. At present, he is engaged in research and development activities for general XML security. He is a member of the Information Processing Society of Japan.