

ICS 35.040
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 25061-2010

**Information security technology -- Public key infrastructure --
XML digital signature syntax and processing specification
(English Translation)**

Issued on: September 2, 2010

Implemented on: February 1, 2011

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine**

Table of Contents

Foreword...	3
Introduction...	4
1 Scope...	5
2 Normative References...	5
3 Terms, Definitions and Abbreviations...	6
4 Overview of XML Signature...	7
5 Processing Rules...	9
6 Core Signature Syntax...	10
7 Additional Signature Syntax...	29
Appendix A (Normative) Definition of XML Digital Signature Document Type	33
Appendix B (Normative) Definition of XML Digital Signature Schema... ..	44
Appendix C (Informative) Algorithms... ..	51
Appendix D (Informative) Examples of XML Digital Signature... ..	60
Bibliography...	67

1 Scope

This Standard specifies the syntax and processing rules of establishing and representing XML digital signature. XML digital signature provides integrity, message authentication and signer authentication services to any type of data.

This Standard is applicable to application programs, systems or services of establishing and processing XML digital signature.

2 Normative References

Through the reference in this Standard, clauses in the following documents become clauses of this Standard. In terms of references with a specific date, all the subsequent modification lists (excluding corrected content) or revised editions are not applicable to this Standard. However, all parties that reach an agreement in accordance with this

Standard are encouraged to explore the possibility of adopting the latest version of these documents. In terms of references without a specific date, the latest version is applicable to this Standard.

GB/T 1988 Information Technology - 7-bit Coded Character Set for Information

Interchange (GB/T 1988-1998, eqv ISO/IEC 646-1991)

GB 13000.1 Information Technology - Universal Multiple-Octet Coded Character Set (UCS)
- Part 1.Architecture and Basic Multilingual Plane (GB 13000.1-1993, idt

ISO/IEC 10646-1.1993)

GB/T 16264.8 Information Technology - Open Systems Interconnection - The Directory

- Part 8.Public-key and Attributed Certificate Frameworks (GB/T 16264.8-2005,

ISO/IEC 9594-8.2001, IDT)

GB/T 18793-2002 Information Technology - Extensible Markup Language (XML) 1.0 (W3C
RFC-xml. 1998, NEQ)

RFC 2253 Lightweight Directory Access Protocol (v3). UTF-8 String Representation of

Distinguished Names

RFC 2396 Uniform Resource Identifiers (URI). Generic Syntax

Signature application refers to an application program, which implements the indispensable parts requested in this Standard, and whose structure and substructure of Signature element type comply with the requirements in this Standard.

3.1.7 Signature validation

Signature validation refers to the core validation of whether the SignedInfo result processed through the canonicalization method appointed by CanonicalizationMethod and the signature method appointed by SignatureMethod matches with the value in

SignatureValue.

3.1.8 Signer authentication

Signer authentication is used to declare and identify the attribute of the signer.

Signature shall indicate the signer of a document, message or record, and without authorization, it is extremely difficult for others to generate it. Signer authentication shall be implemented through application. This Standard supports signer authentication. However, the specific mode of such authentication shall be stipulated by relevant authentication standards.

3.1.9 Transform

Transform refers to the processing of a piece of data from original state to export state.

Typical transform includes XML normalization, XPath and XSLT.

3.2 Abbreviations

The following abbreviations are applicable to this Standard.

CRL. Certification Revocation List

DN. Distinguished Name

URI. Universal Resource Identifier

XML. Extensible Markup Language

XSL. Extensible Stylesheet Language

XSLT. XSL Extensible Stylesheet Language Transformations

4.1 Overview

This Chapter describes XML digital signature structure. Chapter 5 provides processing rules. Chapter 6 provides core signature syntax. Chapter 7 provides signature syntax of additional elements.

Core validation shall include.

- a) Reference validation. validate digest included in every Reference in SignedInfo;
- b) Signature validation. use cryptographic method to conduct signature validation of the signature obtained through SignedInfo calculation.

5.2.2 Reference validation

Reference validation has the following steps.

- a) In accordance with canonicalization method appointed by CanonicalizationMethod in SignedInfo, canonicalize SignedInfo element;
- b) In terms of every Reference in SignedInfo.
 - 1) Obtain data object for digest processing;
 - 2) Use digest algorithm appointed in Reference to calculate the digest value of the result data object;
 - 3) Compare the digest value generated in the previous step and the content of DigestValue element in SignedInfo; if there is any difference, then, the validation is failed.

NOTE: SignedInfo is canonicalized in the first step; the application program shall guarantee that CanonicalizationMethod would not lead to any error.

5.2.3 Signature validation

Signature validation has the following steps.

- a) From KeyInfo or other modes, obtain key information;
- b) Use CanonicalizationMethod to obtain canonicalization form of

SignatureMethod. Then, use the obtained result and the key information obtained above to compare with the signature value on SignedInfo element.

6.1 Overview

This Chapter stipulates the specific syntax of core signature elements. If it is not particularly declared, elements involved in this Chapter shall be supported. Signature syntax shall be defined through document type definition and XML schema definition.

All document type definitions and XML schema definitions shall use the following XML preamble, declaration and internal entity.

identified by URI points to identical-document reference or when the application does not request transform, signature application program does not need to resolve it.

If fragment emerges in front of an absolute or relative URI, the connotation of the fragment shall be defined by MIME type of resources. In terms of XML document, a proxy may also be used to complete signature program's URI parsing (including the fragment processing). Thus, if fragment processing is not reference validation through standardized processing, it might fail. Therefore, this Standard suggests that URI attribute shall not include fragment identifier, instead, it shall consider this processing process as an additional XPath transform to explain.

When fragment does not emerge in front of URI, XML signature program shall support a null-URI and unknown XPointer. If application program still hopes to support any normalized operation of annotation saving, then, it is suggested to provide support to

XPointer of the same document. Since it might be impossible for application program to control fragment generation, all the other supports for XPointer are all optional; all the supports for unknown XPointer and externally quoted XPointer are also optional.

6.4.4.4 Same document URI reference

Parsing same document reference shall generate a XPath node set which is suitable for normalized XML application. Particularly speaking, parsing a null-URI shall generate a XPath node set, which contains every non-annotated node of XML document, which has URI attribute. In fragment URI, characters behind # shall comply with XPointer syntax. When processing XPointer the application program shall use the root node of XML document, which contains URI attribute, to initialize XPointer processing document. If the