

ICS 35.040
CCS L 80



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

GB/T 31503-2015

**Information security technology -- Encryption and signature
message syntax for electronic document**

信息安全技术 电子文档加密与签名消息语法

(English Translation)

Issued on: May 15, 2015

Implemented on: January 1, 2016

Issued by: Standardization Administration of China

Table of Contents

Preface	
Introduction	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Abbreviations	
5 Universal Grammar	
6 Data content type	
7 Signed data content type	
8 Package data content type	
9 Summary data content type	
10 Encrypted data content types	
Identification data content types	11
Useful 12 Type	
13 22 Useful Properties	
14 ASN.1 module	
15 33 safety matters	

Foreword

This standard was drafted in accordance with GB/T 1.1-2009 given rules.

This standard by the National Safety Standardization Technical Committee (SAC/TC260) and focal points.

This standard was drafted. CAS data protection and Communication Research and Education Center, Beijing digital certification Co., Ltd., Shanghai Pu China Information Technology Co., Ltd. integrity, Chan Ka Electronic Technology Co., Ltd.

Introduction

This standard reference IETF (Internet Engineering Task Force) RFC5652 document developed.

This standard specifies the syntax for packaging an electronic document is password protected. It supports digital signatures and encryption. This syntax allows multiple letters

Installed, a package can be nested within another envelope of the package, the same party may previously been encapsulated data is then digitally signed name. It also allows arbitrary attributes, such as time signature, together with the message content, and to provide other properties such as joint signature associated with a signature Together.

This standard describes the electronic document encryption and signature message syntax supports a variety of certificate-based key management architecture. The abstract syntax Syntax Notation ASN.1, and BER-encoded value is generated. These values \u200b\u200bare often expressed as a byte string form. While many systems can Reliable transmission byte string, but there are still a lot of e-mail system does not work. This standard does not provide a mechanism to ensure that the byte stream of encoded this environment Reliable transmission.

Information Security Technology Electronic document encryption and signature Message Syntax

1 Scope

This standard specifies the electronic document encrypting and signing messages Syntax, which can be used to digitally sign any message content, abstracts, Identification or encrypted.

This standard applies to e-commerce and e-government electronic documents generated for encrypting and signing messages, processing and verification.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version suitable for use herein Member. For undated references, the latest edition (including any amendments) applies to this document.

GB/T 16262.1-2006 Information technology - Abstract Syntax Notation - (ASN.1) - Part 1. Specification of basic notation GB/T 16263.1-2006 Information technology - ASN.1 encoding rules Part 1. Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) specification GB/T 16264.2-2008 Information technology - OSI Directory - Part 2. Models GB/T 16264.8-2005 Information technology - OSI Directory - Part 8. a public key and attribute certificate frameworks GB/T 19714-2005 Information technology - Security techniques Public Key Infrastructure Certificate Management Protocol GB/T 20518-2006 Information security technology - Public key infrastructure - Digital certificate format Internet attribute certificate frameworks (AnInternetAttributeCertificateProfileforAu- RFC3281 for authorization thorization) RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List contour (InternetX.509PublicKeyIn-frastructureCertificateandCertificateRevocationList (CRL) Profile)

3 Terms and Definitions

GB/T 19714-2005, GB/T 20518-2006 define the following terms and definitions apply to this document.

Algorithm identifier by object type identification algorithm identifier.

Property attribute

Including property type, and one or more attribute values, attribute type specified by the object identifier.

4 Abbreviations

The following abbreviations apply to this document.

ASN.1. Abstract Syntax Notation - (AbstractSyntaxNotationone) BER. Basic Encoding Rules (BasicEncodingRules)