

ICS 35.040
CCS L 80



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

GB/T 17902.3-2005

**Information technology -- Security techniques -- Digital
signatures with appendix -- Part 3: Certificate-based
mechanisms**

信息技术 安全技术 带附录的数字签名 第3部分：基于证书的机制
(English Translation)

Issued on: April 19, 2005

Implemented on: October 1, 2005

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the People Republic of China, China National
Standardization Administration Committee**

Table of Contents

- Foreword
- 1 Scope
- 2 Normative references
- 3 Overview

Foreword

GB/T 17902 "Information Technology Security Technology with Digital Signature of the Appendix" consists of the following parts.

Part 1. Overview;

Part 2. Identity-based mechanisms;

Part 3. Certificate-based mechanisms.

This part is the third part of GB/T 17902, which is equivalent to the international standard ISO/IEC 14888-3.:1998 "Information Technology Safety Technology" Digital signature for appendix with appendix Part 3. Certificate-based mechanism (English version).

Appendix A and Appendix B of this part are normative appendices, and Appendix C to Appendix G are informative appendices.

This part is proposed by the Ministry of Information Industry of the People's Republic of China this part is under the jurisdiction of the National Information Security Standardization Technical Committee;

1 Scope

GB/T 17902 specifies a digital signature mechanism with an appendix for messages of any length and is suitable for providing raw data identification and non-repudiation.

And data integrity programs.

This part of GB/T 17902 specifies a certificate-based digital signature mechanism with an appendix. In particular, this section provides.

1) A general description of a certificate-based signature mechanism whose security is based on the difficulty of discrete logarithm problems on the switched groups used (see Chapter 6).

2) A general description of the certificate-based signature mechanism whose security

mechanisms are based on the difficulty of factorization (see Chapter 7).

3) Various conventional digital signature mechanisms with appendices based on the certificate mechanism using arbitrary length messages (see Appendix A and Appendix B).

2 Normative references

The terms of the following documents become the provisions of this part by reference in this part of GB/T 17902. Quotations with dated , all subsequent amendments (not including errata content) or revisions do not apply to this section, however, encouragement is achieved under this section the parties to the agreement study whether the latest versions of these documents can be used. For undated references, the latest edition applies to this section.

GB 15851-1995 Information technology security technology Digital signature scheme with message recovery (idt ISO/IEC 9796:1991) GB/T 17902.1-1999 Information technology security technology with digital signatures in appendix Part 1. Overview GB/T 17902.2-2005 Information technology security technology with digital signatures in appendix Part 2. Identity-based mechanisms (ISO/IEC 14888-2.:1999, IDT) GB/T 18238.3-2002 Information technology security techniques - Hash function - Part 3. Dedicated hash function (idt ISO/IEC 10118-3:1998) Information technology - Security techniques - Digital signature schemes with message recovery - Part 2. Using hashes Function mechanism ISO/IEC 10118-4:1998 - Information technology - Security techniques - Hash function - Part 4

3 Overview

The definitions, symbols, numerical lengths and notations given in GB/T 17902.1-1999 are used in this part of GB/T 17902.

The verification of the digital signature requires the verification key of the signature entity. Therefore, the authenticator must associate the correct authentication key with the signature entity.

stand up. For certificate-based mechanisms, this association must be provided by some kind of certificate. For example, the verification key is taken from a certificate.

The purpose of this part of GB/T 17902 is to specify the following procedures and functions of the general model described in GB/T 17902.1-1999.

- a) The process of generating a key
 - 1) Generate domain parameters
 - 2) Generate signature and verification key
- b) the process of forming a signature

- 1) (Optional) Form a pre-signature
- 2) Prepare a message for the signature GB/T 17902.3-2005/ISO/IEC 14888-3:1998