

ICS 35.040
CCS L 80



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

GB/T 17902.2-2005

**Information technology -- Security techniques -- Digital
signatures with appendix -- Part 2: Identity-based mechanisms**

信息技术 安全技术 带附录的数字签名 第2部分：基于身份的机制

(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
- 4 Terms and definitions

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 second part of GB/T 17902, which is equivalent to the international standard ISO/IEC 14888-2.:1999 "Information Technology Safety Technology" Digital signatures with appendix Part 2. Identity-based mechanisms (English version).

Appendix A and Appendix B of this section are informative annexes.

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 various digital signature mechanisms with appendices for messages of any length. It is suitable for providing entity authentication, data A scheme for initial identification, non-repudiation and data integrity.

This part of GB/T 17902 specifies the signature and verification of an identity-based digital signature mechanism with an appendix for messages of any length.

The overall structure and basic process of the process.

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

3 Overview

The verification of the digital signature requires the verification key of the signature entity. Therefore, the authenticator must put the correct verification key with the signature entity, or Specifically, it is associated with the (partial) identification data of the signature entity. If this connection is inherent to the verification key itself, this scheme it is called "identity-based." the key generation process for the identity-based scheme defined in this section includes a trusted third party. This trusted third party has a secret Parameter---Key generation index, which is used to derive the signature key of other entities. The secretness of the signature key unconditionally depends on the key generation the secret of indexing.

In the verification of identity-based signatures, two parameters are required. The first parameter is the domain validation index, which is common to all entities.

The second parameter is the verification key of the signing entity, which is specific to each entity. Identity-based mechanisms defined in this section the entity's authentication key is obtained directly from the entity's identification data using a public function.

The identity-based signature mechanism with an appendix is an example of a randomization mechanism, as described in GB/T 17902.1-1999. Digital sign the name and verification process description follows the general procedure defined in Chapter 10 of GB/T 17902.1-1999. In particular, this standard uses General requirements conditions, definitions and symbols provided in GB/T 17902.1-1999.

An identity-based digital signature mechanism with an appendix is defined in the detailed description of the following process. They are.

- a) the key generation process;
- b) the signature process;
- c) Verification process.

4 Terms and definitions

The following terms and definitions apply to this part of GB/T 17902.

GB/T 17902.2-2005/ISO/IEC 14888-2:1999