ICS 35.030
CCS L 80



# NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

# GB/T 17902.1-2023

Replacing GB/T 17902.1-1999

## Information technology - Security techniques - Digital signatures with appendix - Part 1: General

**Issued on: March 17, 2023** **Implemented on: October 1, 2023**

**Issued by: State Administration for Market Regulation, China National Standardization Administration**

# Table of Contents





## foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for Standardization Work Part 1.Structure and Drafting Rules for Standardization Documents" drafting.

This document is Part 1 of GB/T 17902 "Information Technology Security Technology Digital Signature with Appendix". GB/T 17902 has

The following parts have been published.

--- Part 1.Overview;

--- Part 2.Identity-based mechanisms;

--- Part 3.Certificate-based mechanism.

This document replaces GB/T 17902.1-1999 "Information Technology Security Technology Digital Signature with Appendix - Part 1.Overview

Compared with GB/T 17902.1-1999, except for structural adjustment and editorial changes, the main technical changes are as follows.

--- Adjust the original "Overview" part to Chapter 5 (see Chapter 5, Chapter 3 of the.1999 edition);

--- Removed "Assignment" "Collision-Free Hash Function" "Deterministic" "Hash Token" "Hash Code" "Pre-Signed" "Randomize" "Random

Terms such as "value", "signature equation", "signature function" and "assignment" (see Chapter 4 of the.1999 edition), added "collision-resistant hash function

terms such as "number", "data element", "field", "hash code", "key pair" and "message" (see Chapter 3);

---Deleted symbols such as "recalculated hash token", "prepared partial message", "assignment", "pre-signature", "recalculated pre-signature"

number and the legend of "comparison" (see Chapter 5 of the.1999 edition), added the legend of "optional data" (see 4.3), and added

"Usual" content (see 4.2);

---Added the chapter "Binding Options of Signature Mechanism and Hash Function", which describes several types of options for binding signature mechanism and hash function

(see Chapter 7);

--- Merge the content of the signature process into Chapter 9, and use a general model to describe the existing mechanism uniformly, which is more universal than the original content (see

Chapter 9, Chapter 8 and Chapter 9 of the.1999 edition);

--- Merge the verification process into Chapter 10, and update the general model to describe the existing mechanism, which is more universal than the original content (see Chapter 10

Chapter 10, Chapter 9 of the.1999 edition).

This document is equivalent to ISO /IEC 14888-1.2008 "Information Technology Security Technology Digital Signature with Appendix Part 1.

Overview".

The following minimal editorial changes have been made to this document.

---Chapter 10 The signature verification section adds a note for easy understanding.

Please note that some contents of this document may refer to patents. The issuing agency of this document assumes no responsibility for identifying patents.

## Introduction

Digital signature mechanism is a kind of asymmetric cryptographic mechanism, which is widely used in entity authentication, data source authentication, data integrity and non-repudiation.

Serve. There are two digital signature mechanisms.

--- If a message is required as part of the input during the verification process, this type of mechanism is called "digital signature with appendix", and the appendix counts

The calculation needs to use the hash function;

---If all or part of the message is disclosed during the verification process, this type of mechanism is called "digital signature with message recovery", and the signature generates

Completion and verification also use hash functions.

Digital signatures with appendices are regulated in GB/T 17902, digital signatures with message recovery are regulated in ISO 10118

Specifications, hash functions are specified in GB/T 18238 (all parts).

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

--- Part 1.Overview. The purpose is to standardize the general framework and general model of digital signature with appendix.

--- Part 2.Identity-based mechanisms. The purpose is to standardize the identity-based digital signature mechanism with appendices.

--- Part 3.Certificate-based mechanism. The purpose is to standardize the digital signature mechanism based on the certificate.

Information technology security technology digital signature with appendix

Part 1.Overview

## 1 Scope

GB/T 17902 specifies several digital signature mechanisms with appendices for signing messages of arbitrary length.

This document includes the general principles and requirements of digital signatures with appendices, as well as the definitions and definitions used in various parts of GB/T 17902.

symbol.

Related technologies such as certificate and key management are outside the specification scope of this document. For more information of this kind, see GB/T 16264.8-

2005[2], ISO /IEC 11770-3[8] and ISO /IEC 15945.2002[9].

## 2 Normative references

This document has no normative references.

## 3 Terms and Definitions

The following terms and definitions apply to this document.

3.1

appendix appendix

A bitstring consisting of a signature and an optional text field.

3.2

Anti-collision hash function colision-resistanthash-function

Collision Resistant Hash Function

A hash function that satisfies the property that it is computationally infeasible to find any two different inputs that map to the same output.

Note. Whether the calculation is feasible depends on the specific security requirements and the environment.

[Source. ISO /IEC 10118-1.2016, 3.1]

3.3

Data element dataelement

Integer, bitstring, set of integers, or set of bitstrings.

3.4

domain domain

A group of entities operating under a single security policy.

Example. A public key certificate created by a single authority or a group of authorities adopting the same security policy.

3.5

Domain parameter domainparameter

A data element that is common and known or accessible to all entities in the domain.