

ICS 35.030
CCS L 80



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

GB/T 17903.3-2024

Replacing GB/T 17903.3-2008

**Information technology - Security techniques - Non-repudiation
- Part 3: Mechanisms using asymmetric techniques
(English Translation)**

Issued on: March 15, 2024

Implemented on: October 1, 2024

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

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms and Definitions
4 Symbols
5 Requirement
6 Involvement of trusted third parties
7 Digital Signature
8 Non-repudiation Token
9 Mechanisms for generating evidence by end entities
9.1 General Rules
9.2 Non-repudiation of origin mechanism
9.3 Delivery Non-Repudiation Mechanism
10 Mechanisms for generating evidence by delivery agencies
10.1 General Rules
10.2 Submission Non-Repudiation Mechanism
10.3 Transmission Non-Repudiation Mechanism
11 Time Guarantee Mechanism
11.1 General Rules
11.2 Timestamp mechanism
11.3 Mechanisms for using time notarization services
Reference

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 3 of GB/T 17903 "Information Technology Security Technology Non-Repudiation". GB/T 17903 has been published in the following parts.

--- Part 1: Overview;

--- Part 2: Mechanisms using symmetric techniques;

--- Part 3: Mechanisms using asymmetric techniques.

This document replaces GB/T 17903.3-2008 "Information technology security technology non-repudiation part 3.using asymmetric technology Compared with GB/T 17903.3-2008, in addition to structural adjustments and editorial changes, the main technical changes are as follows.

a) Added security requirements for digital signatures (see Chapter 5);

b) Added a time guarantee mechanism (see Chapter 11).

This document is modified to adopt ISO/IEC 13888-3:2020 "Information security non-repudiation part 3.Mechanisms using asymmetric techniques".

The technical differences between this document and ISO/IEC 13888-3:2020 and their reasons are as follows.

a) Added normative reference GB/T 20520 (see Chapter 3), citing the terms of this standard;

b) Deleted the definition of "3.2 Timestamp service" in Chapter 3 of ISO/IEC 13888-3:2020.This term has been included in the normative references.

The definition is given in GB/T 20520;

c) The normative reference GB/T 17903.1 replaces ISO/IEC 13888-1 (see Chapter 3 and Chapter 4) to adapt to my country's Technical conditions;

d) The requirements for collision-resistant hash functions have been modified to adapt to my country's technical conditions (see Chapter 5);

e) The normative references GB/T 15851 (all parts) replaced ISO/IEC 9796 (all parts), and the normative references GB/T 15851 (all parts) replaced ISO/IEC 9796 (all parts).

GB/T 17902 (all parts) replaced ISO/IEC 14888 (all parts) (see Chapter 7) to adapt to my country's technical requirements.

Technical conditions;

f) ISO/IEC 18014 (all parts) (see 11.2) has been replaced by the normative reference GB/T 20520 to adapt to the technical requirements of my country.

Technical conditions.

The following editorial changes were made to this document.

a) To coordinate with the existing standards, the name of the standard is changed to "Information Technology Security Technology Non-Repudiation Part 3.

Mechanisms using asymmetric techniques";

b) deleted the informative references to ISO/IEC 10118 (all parts) in ISO/IEC 13888-3:2020;

c) ISO/IEC 9594-8 is replaced by the informative reference GB/T 16264.8-2005 (see Chapter 6).

Introduction

Non-repudiation services are designed to generate, collect, maintain, utilize, and verify evidence about claimed events or actions in order to resolve disputes regarding such events.

GB/T 17903 aims to describe the model of the anti-repudiation mechanism and the use of symmetric cryptographic technology and non-the specific anti-repudiation mechanism of symmetric encryption technology is planned to consist of three parts.

--- Part 1: Overview. The purpose is to give a general model of the non-repudiation mechanism as specified in other parts of GB/T 17903 A general model for non-repudiation mechanisms using cryptographic techniques.

--- Part 2: Mechanisms using symmetric technology. The purpose is to provide specific non-repudiation mechanisms using symmetric cryptographic technology.

--- Part 3: Mechanisms using asymmetric technology. The purpose is to provide specific non-repudiation mechanisms using asymmetric cryptographic technology.

Information technology security technology non-repudiation Part 3: Mechanisms using asymmetric techniques

1 Scope

This document defines several specific non-repudiation mechanisms to provide non-repudiation of origin, non-repudiation of delivery, non-repudiation of transmission, and non-repudiation of submission.

deny.

This document applies to the design, implementation and testing of message non-repudiation related applications implemented using asymmetric technology.

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document.

For referenced documents without a date, only the version corresponding to that date

applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to this document.

GB/T 15851 (all parts) Information technology security techniques Digital signature schemes with message recovery [ISO/IEC 9796 (all parts) Some]

Note 1: GB/T 15851.3-2018 Information technology security techniques Digital signature schemes with message recovery Part 3: Mechanisms based on discrete logarithms (ISO/IEC 9796-3:2006,MOD) GB/T 17902 (all parts) Information technology security techniques Digital signatures with appendix [ISO/IEC 14888 (all parts)]

Note 2: GB/T 17902.1-2023 Information technology security techniques Digital signatures with appendices Part 1: Overview (ISO/IEC 14888-1.

2008, IDT)

GB/T 17902.2-2023 Information technology security technology Digital signature with appendix Part 2: Identity-based mechanism (ISO/IEC 14888-2:1999, IDT) GB/T 17902.3-2023 Information technology security techniques Digital signatures with appendix Part 3: Certificate-based mechanisms (ISO/IEC 14888-3:1998, IDT) GB/T 17903.1 Information technology security technology non-repudiation Part 1: Overview (GB/T 17903.1-2024, ISO/IEC 13888-1:2020,MOD) GB/T 20520 Network security technology public key infrastructure timestamp specification ISO/IEC 29192-4 Information technology security techniques Lightweight cryptography Part 4: Mechanisms using asymmetric techniques (In-

3 Terms and definitions

The terms and definitions defined in GB/T 17903.1 and GB/T 20520 and the following terms and definitions apply to this document.

Time-marking service A service that provides evidence that a record occurred before a specific point in time.

NOTE: The evidence contains a hash code and an identifier of the hash function used.