NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

GB/T 34953.4-2020

Information technology - Security techniques - Anonymous entity authentication - Part 4: Mechanisms based on weak secrets

Issued on: April 28, 2020 **Implemented on: November 1, 2020**

Issued by: SAMR; SAC

Table of Contents

Foreword

GB/T 34953 "Information technology - Security techniques - Anonymous entity authentication" is divided into 4 parts:

- Part 1: General;
- Part 2: Mechanisms based on signatures using a group public key;
- Part 3: Mechanisms based on blind signatures;
- Part 4: Mechanisms based on weak secrets.

This Part is Part 4 of GB/T 34953.

This Part is drafted in accordance with the rules given in GB/T 1.1-2009.

This Part uses the redraft law to modify and adopt ISO/IEC 20009-4:2017 "Information technology - Security techniques - Anonymous entity authentication - Part 4: Mechanisms based on weak secrets".

Compared with ISO/IEC 20009-4:2017, this Part has structural adjustments. Adjust 6.3 to 6.2. The other clause numbers are revised in turn.

The technical differences between this Part and ISO/IEC 20009-4:2017 and the reasons are as follows:

- As for the normative references, this Part has made adjustments with technical differences, to adapt to the technical conditions of China. The adjustments are reflected in Clause 2 "Normative references". The specific adjustments are as follows:

? Replace ISO/IEC 9797-2 with GB/T 15852.2 which modifies and adopts the international standard; stipulate that the hash algorithm used shall follow relevant national standards and industry standards;

? Replace ISO/IEC 29000-1 with GB/T 34953.1 which is identical to the international standard;

? Replace ISO/IEC 19772:2009 with GB/T 36624-2018 which modifies and adopts the international standard;

? Delete ISO/IEC 10118-3; ISO/IEC 10118-3 specifies the hash algorithm used in mechanisms of this Part. Stipulate that the hash algorithm used shall follow relevant national standards and industry standards;

Information technology - Security techniques - Anonymous entity authentication - Part 4: Mechanisms based on weak secrets

1 Scope

This Part of GB/T 34953 specifies anonymous entity authentication

mechanisms based on weak secrets. The precise operation of each mechanism is specified, together with details of all inputs and outputs.

This Part is applicable to situations in which the server only verifies that the user belongs to a certain user group without obtaining any information that can be used to identify the user later on.

2 Normative references

The following documents are indispensable for the application of this document. For the dated references, only the editions with the dates indicated are applicable to this document. For the undated references, the latest edition (including all the amendments) are applicable to this document.

GB/T 15852.2 Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function (GB/T 15852.2-2012, ISO/IEC 9797-2:2002, MOD)

GB/T 34953.1 Information technology - Security techniques - Anonymous entity authentication - Part 1: General (GB/T 34953.1-2017, ISO 20009-1:2013, IDT)

GB/T 36624-2018 Information technology - Security techniques - Authenticated encryption (ISO/IEC 19772:2009, MOD)

ISO/IEC 11770-4:2006 Information technology - Security techniques - Key management - Part 4: Mechanisms based on weak secrets

3 Terms and definitions

For the purposes of this document, the terms and definitions given in GB/T

34953.1 and the following apply.

.....