ICS 35.040
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 38647.1-2020

Information technology - Security techniques - Anonymous digital signatures - Part 1: General

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

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

Table of Contents

Foreword

GB/T 38647 "Anonymous Digital Signature of Information Technology Security Technology" is intended to be divided into two parts.

--- Part 1. General Provisions;

--- Part 2. The mechanism of using group public key.

This part is Part 1 of GB/T 38647.

This section was drafted in accordance with the rules given in GB/T 1.1-2009.

This section uses the redrafting method to modify the use of ISO /IEC .20008-1..2013 "Information Technology Security Technology Anonymous Digital Signature

Part 1. General Provisions.

Compared with ISO /IEC .20008-1..2013, this part is structurally adjusted, Chapter 2 is added, and the other article numbers are revised sequentially.

There are technical differences between this part and ISO /IEC .20008-1..2013, and the terms involved in these differences have been adopted on the outside margin

The vertical single line (|) in the blank position is marked. The specific technical differences and the reasons are as follows.

--- Added Chapter 2 normative references (see Chapter 2);

--- Removed the abbreviations "DAA" and "TPM", which is compatible with China's technical level (see ISO /IEC .20008-1..2013, section 3)

chapter);

--- End of paragraph 4 of Chapter 6 adds different types of entity authentication mechanisms supported by different types of digital signature technologies, and gives

A national standard regulating the identification mechanism of these entities has been

issued (see Chapter 6).

Please note that some content of this document may involve patents. The issuer of this document does not assume responsibility for identifying these patents.

This part is proposed and managed by the National Information Security Standardization Technical Committee (SAC/TC260).

This section was drafted. Xi'an Xidian Jietong Wireless Network Communication Co., Ltd., National Engineering Laboratory for Wireless Network Security Technology,

Zhongguancun Wireless Network Security Industry Alliance, Commercial Cryptographic Testing Center of National Cryptography Administration, National Radio Monitoring Center Testing Center, National

Information Technology Security Research Center, China General Technology Research Institute, China Electronics Technology Standardization Research Institute, Tianjin Electromechanical Products Inspection

Testing Center, Chongqing University of Posts and Telecommunications, Beijing Institute of Computer Technology and Applications, Tianjin Radio Monitoring Station, Ministry of Industry and Information Technology Broadband Wireless

IP Standards Working Group.

Introduction

The mechanism specified in GB/T 38647 uses cryptographic algorithms specified in various standards, such as.

a) You can use the anti-collision cryptographic hash function to perform cryptographic hash operations on signed messages and calculate signatures;

b) When a certificate is needed to verify the public key, a traditional digital signature mechanism can be used;

c) If an entity requires data communications to be authenticated as part of its mechanism when implementing the mechanism, it may be necessary to use traditional

Body identification mechanism;

d) If the information of some entities needs to be encrypted in the anonymous digital signature mechanism, it may be necessary to use traditional asymmetric encryption

Mechanisms to protect privacy and confidentiality.

Anonymous digital signature mechanisms can be used to provide services such as entity authentication, data source authentication, non-repudiation, and data integrity. digital signature

The mechanism can enable the owner (or holder) of the private key to generate digitally signed messages individually or jointly. Its corresponding verification key (or multiple keys)

Can be used to verify the signature validity of the message. The digital signature mechanism satisfies.

a) The attacker needs to have one or both of the following.

1) Verification key instead of signing key;

2) The signature set of a series of messages adaptively selected by the attacker.

b) The attacker is computationally infeasible under the following circumstances.

1) Generate a valid signature for the new message;

2) Recover the signature key;

3) In some cases, different valid signatures are generated on previously signed messages.

Anonymous digital signature is a special type of digital signature mechanism. In the anonymous digital signature mechanism, given a digital signature, one includes

Unauthorized entities, including the verifier, cannot recover the signer 's identity or identity. However, such a mechanism still has only legally signed

The famous party can generate a valid signature. There are four different situations for authorized entities participating in the anonymous signature mechanism.

a) The mechanism by which authorized entities can verify the signature of the signing party;

b) An authorized entity can only have the ability to connect two signatures created by the same signer but cannot verify the identity of the signer

mechanism;

c) A mechanism that contains two authorized entities and conforms to the first two situations;

d) A mechanism that contains two authorized entities that does not meet the first two conditions.

An example application of anonymous digital signature is to realize anonymous entity authentication. GB/T 34953.2 specifies an anonymous entity authentication mechanism.

Unlike the traditional digital signature mechanism, the anonymous digital signature mechanism is based on asymmetric cryptography and involves three basic operations.

a) The process of generating signature key and verification key;

b) The process of creating an anonymous digital signature using a signature key;

c) The process of verifying the anonymous digital signature using the verification key.

One of the main differences between traditional digital signatures and anonymous digital signatures is the method of using public keys for signature verification. To verify

A traditional digital signature, the verifier uses the verification key bound to the identity of the signer to verify the anonymous digital signature.

A group of public keys or multiple public keys, they are not bound to a single signer. Anonymous signatures using group public keys are often referred to as group signatures.

Anonymous signatures with multiple public keys are often called ring signatures. The strength of anonymity (that is, the degree of anonymity) provided by the anonymous signature mechanism depends on

The size of the group and the number of public keys.

In an anonymous digital signature mechanism using group public keys, three different authorization levels can be performed on an entity or a group of entities

The revocation includes the following three possibilities.

a) The entire group is withdrawn, that is, the entire group is withdrawn.

b) Revoke the membership of a group member. As a result, the revoked member can no longer authorize the representative group to create a group signature;

c) The signature verifier can revoke the permission of a certain anonymous signature type created by the group members. After such revocation, it has been applied for

The revoked member can still create other anonymous signatures on behalf of the group.

Information Technology Security Technology Anonymous Digital Signature

Part 1. General

1 Scope

This part of GB/T 38647 specifies the definition, selection and overall requirements of the anonymous signature mechanism, as well as the following two anonymous signature mechanisms

The common model, entity set and part of the process.

a) Use the signature mechanism of the group public key;

b) Use multiple public key signature mechanism.

This part is applicable to guide the design, implementation and application of anonymous digital signature mechanism.

2 Normative references