

ICS 35.040



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

**GB/T 34953.1-2017**

---

**Information technology -- Security techniques -- Anonymous  
entity authentication -- Part 1: General**

信息技术 安全技术 匿名实体鉴别 第1部分：总则

**(English Translation)**

**Issued on: November 1, 2017**

**Implemented on: May 1, 2018**

---

**Issued by: SAMR; SAC**

## Table of Contents

|                                         |
|-----------------------------------------|
| Foreword                                |
| Introduction                            |
| 1 Scope                                 |
| 2 Terms and definitions                 |
| 3 Symbols and abbreviations             |
| 4 Anonymous entity identification model |
| 5 General requirements and restrictions |
| 6 Anonymous management                  |
| Reference                               |

## Preface

GB/T 34953 "Information Technology Security Technology Anonymous Entity Identification" is divided into four parts.

---Part 1: General Provisions;

---Part 2: Mechanism based on group public key signature;

---Part 3: Mechanism based on blind signature;

---Part 4: Mechanism based on weak secrets.

This part is Part 1 of GB/T 34953.

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

The translation method used in this part is equivalent to the ISO /IEC 20009-1:2013 "Information Technology Security Technology Anonymous Entity Authentication No. 1 Part. General Provisions.

Please note that certain contents of this document may involve patents. The issuing agency of this document is not responsible for identifying these patents.

## Introduction

Verifying the legitimacy of communication participants is one of the most important cryptographic services. There are multiple encryption mechanisms to support this service, for example, The entity authentication mechanism specified by ISO /IEC 9798 and the digital signature mechanism specified by ISO /IEC 9796 and ISO /IEC 14888.

Anonymous authentication communication includes hiding the identity of the authenticated entity from the correspondent and/or third party, while retaining the ability to enable the verifier to determine its identity.

The communication peer is a legal attribute. An anonymous entity authentication mechanism is designed to support these anonymous communications. This mechanism is defined as inter-entity The exchange of information, when needed, these exchanges will involve a trusted third party.

In the anonymous entity authentication mechanism, the authenticated entity (the claimant) provides evidence to the verifier, which proves that the claimant knows the secret and does not It will disclose the identity of the claimant to any unauthorized entity, that is, through the complete information exchanged between the claimant and the verifier, the The right entity cannot discover the identity of the entity to be verified (that is, the claimant). At the same time, the verifier can have certain attributes of the claimant (such as scheduled Group membership) to ensure the authenticity of the claimant. However, even an authorized verifier cannot be authorized to obtain The identity of other entities. The anonymous entity authentication mechanism allows the authorized party to perform the opening process, which enables the authorized party to obtain the generated signature.

The identity of the entity of the name. The mechanism that allows it to be opened is called the partial anonymous entity authentication mechanism.

Anonymous entity authentication can be applied in many scenarios, such as e-commerce, e-voting, and e-identity (e.g., e-driving license, e-health Certificates and e-passports), social networks, mobile payments, and trusted computing. In many such services, the customer's personally identifiable information (PII) is disclosed to the service provider as part of the authentication process. As a result, service providers may use PII for other purposes, But not necessarily interested in PII itself. One way to restrict service providers from obtaining PII is to use an anonymous authentication mechanism. Anonymous entity authentication See ISO /IEC 29191 Appendix A for other use cases.

GB/T 34953 is composed of multiple parts, which respectively stipulate the general model and mechanism of anonymous entity authentication. This part mainly stipulates the secret The model of name entity authentication, the details of the anonymous entity authentication mechanism and the authentication interaction message are not within the scope of this part, and will be carried out by other parts specification. Information technology security technology anonymous entity authentication Part 1: General

## 1 Scope

This part of GB/T 34953 specifies the model, requirements and agreement of an anonymous entity authentication mechanism used to verify the legitimacy of an entity. Bundle condition.

## 2 Terms and definitions

The following terms and definitions apply to this document.

### 2.1 Anonymity strength

An unauthorized entity can determine the probability of the true signer from a given signature.

**Note:** The anonymity strength of  $n$  means that the probability that an unauthorized entity can correctly guess the real signer from a signature is  $1/n$ . [ISO /IEC 20008-1:2013]

### 2.2 Anonymous entity authentication

Prove that an entity has certain properties, but not distinguish the entity from other entities that have the same properties come out.

### 2.3 Anonymous digital signature

It can be verified using a group public key or multiple public keys, and it is not chased by unauthorized entities including the verifier of the signature. The signature of the distinguishable identifier traced to the signer. [ISO /IEC 20008-1:2013]

### 2.4 Question

A data item randomly selected by the verifier and sent to the claimant, and the claimant uses this data item together with the secret information it possesses to generate it to The verifier's response. [ISO /IEC 9798-1:2010]

## 4 Anonymous entity identification model

Figure 1 shows the general model of the anonymous entity authentication mechanism. The entity and message interaction in this model is not for all authentication mechanisms. Both are required.

For the anonymous entity authentication mechanism described in other parts of GB/T 34953, such as one-way anonymous authentication, entity A is used as the claim Party, entity B is the verifier. In the two-way anonymous authentication mechanism, entity A and entity B simultaneously assume the roles of claimant and verifier.

In the one-way anonymous two-way authentication mechanism, entity A and entity B assume the roles of claimant and verifier at the same time. The difference is that the authentication mechanism It is anonymous in one direction and non-anonymous in the other direction (for example, A verifies the valid identity of B, and B only verifies that A belongs to one Member of a predefined entity group.)

The role of TTP depends on the type of mechanism that uses it. Some mechanisms may not use trusted third parties. As an option, TTP Can participate in the authentication process in an offline manner, for example, before using a mechanism, provide one or both of A and B for authentication Information to support the use of this mechanism. As an optional third party, TTP may actively pass and identify one of the entities or The two parties exchange information to participate in the authentication mechanism. TTP may also participate in the opening process or linking process. If TTP participates, no matter Online or offline, both parties participating in the anonymous authentication mechanism must trust it.

In order to achieve the purpose of anonymous entity identification, entities generate and exchange standardized messages, which are called tokens. One-way anonymous authentication At least one token needs to be exchanged, and at least two tokens need to be exchanged for two-way anonymous authentication. If a challenge must be used to initiate an anonymous entity authentication Otherwise, additional message interaction may be required. If a trusted third party participates in authentication, additional message interaction may also be required.

In Figure 1, the arrows indicate the potential flow of information. Entity A and Entity B can interact directly, or they can use trusted third parties respectively. Information issued by the party.

The anonymous entity authentication mechanism is composed of a message exchange, and the verifier is based on the certain attributes (such as predefined (Group membership) as evidence to identify the authenticity of the claimant. The evidence is obtained by examining secret information that only real entities can possess.

Obtained after changing the line password. In addition, some mechanisms also allow the claimant to indicate to the verifier that it possesses in addition to being owned by a truly authorized entity. Some attributes other than some attributes.

The specific details of the GB/T 34953 anonymous entity authentication mechanism will be regulated in the subsequent part.

## 5 General requirements and restrictions

In order for one entity (i.e. verifier) to anonymously identify another entity (i.e. claimant), both the claimant and the verifier should use Use a public collection of cryptographic techniques and parameters.

In the process of using the key, the value of all time-varying parameters cannot be repeated (such as timestamp, sequence number, and random number), or at least pressure The inverted probability will not repeat.

Assume that in the process of using the anonymous entity authentication mechanism, both