

ICS 35.040



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

GB/T 15843.2-2024

**Cybersecurity technology-Entity authentication-Part 2:
Mechanisms using authenticated encryption**

网络安全技术 实体鉴别 第2部分：采用鉴别式加密的机制

(English Translation)

Issued on: January 1, 1970

Implemented on: January 1, 1970

Issued by: SAMR; SAC

Table of Contents

Foreword	
Introduction	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Symbols and abbreviations	
5 Requirements	
6 Mechanisms that do not involve trusted third parties	
6.1 One-way authentication	
6.1.1 Mechanism 1-Single Pass Authentication	
6.1.2 Mechanism 2-Two-pass authentication	
6.2 Mutual authentication	
6.2.1 Mechanism 3-Two-pass authentication	
6.2.2 Mechanism 4-Three pass authentication	
7 Mechanisms involving trusted third parties	
7.1 Mechanism 5-Four-pass authentication	
7.2 Mechanism 6-Five pass authentication	
Appendix A (normative appendix) OID and ASN.1 syntax	
Appendix B (informative appendix) Use of text fields	
Appendix C (informative appendix) Nature of entity authentication mechanism	
Reference	

Preface

GB/T 15843 "Information Technology Security Technology Entity Identification" has currently or plans to publish the following parts.

- Part 1: General Provisions;
- Part 2: The mechanism of using symmetric encryption algorithms;
- Part 3: The mechanism of using digital signature technology;
- Part 4: Using the mechanism of password verification function;
- Part 5: The mechanism of adopting zero-knowledge technology;

---Part 6: Using the mechanism of manual data transfer.

This part is Part 2 of GB/T 15843.

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

This Part replaces GB/T 15843.2-2008 "Information Technology Security Technology Entity Authentication Part 2: Using Symmetric Encryption Compared with GB/T 15843.2-2008, the main changes are as follows.

---In Chapter 3, a description of seven terms other than those defined in ISO/IEC 9798-1:1997 was added;

--- Separate the "symbols" in Chapter 3 into Chapter 4 "symbols and abbreviations";

---In Chapter 5 "Requirements", the requirements for verifying time-varying parameters have been added;

---Added two appendices. Appendix A and Appendix C.

The translation method used in this part is equivalent to ISO/IEC 9798-2:2008 "Information Technology Security Technical Entity Authentication Part 2.

Mechanism using symmetric encryption algorithm.

The Chinese documents that have consistent correspondence with the international documents cited in this section are as follows.

---GB/T 15843.1-2017 Information technology security technology entity identification Part 1: General (ISO/IEC 9798-1.

2010, IDT)

This section has made the following editorial changes.

---Include the content of ISO/IEC 9798-2:2008 TECHNICAL CORRIGENDUM 3:2013;

---The number of parallel items is changed from "(1), (2)" to "a), b)".

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

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

Drafting organizations of this section. Data and Communication Protection Research and Education Center of Chinese Academy of Sciences, Beijing Jiangnan Tianan Technology Co., Ltd., PwC Letter Information Technology Co., Ltd.

Introduction

This part is equivalent to ISO/IEC 9798-2:2008 and its errata document ISO/IEC 9798-2:2008 TECHNICAL COR-RIGENDUM 3, which is a subcommittee SC27 (Information Security Technology) of the ISO/IEC Joint Technical Committee JTC1 (Information Technology) Drafted.

This part specifies the entity authentication mechanism using symmetric encryption algorithm, including one-way authentication mechanism and mutual authentication mechanism, and does not involve trusted Third-party authentication mechanisms and authentication mechanisms involving trusted third parties, and provide requirements for these authentication mechanisms.

In the case of not involving a trusted third party, the one-way authentication mechanism includes one-pass authentication and two-pass authentication.

The system includes two pass authentication and three pass authentication. If a trusted third party is involved, the mutual authentication mechanism needs to be carried out four times or Five passes.

All relevant content related to cryptographic algorithms in this section shall be implemented in accordance with relevant national regulations.

Information technology security technology entity authentication Part 2: Mechanisms using symmetric encryption algorithms

1 Scope

This part of GB/T 15843 specifies an entity authentication mechanism using a symmetric encryption algorithm. Four of them are inaccessible between two entities Trust the third-party authentication mechanism. Two of the four mechanisms are one-way authentication by one entity against another entity, and the other two are two-way authentication mechanisms.

Two entities authenticate each other. The rest of the mechanisms require a trusted third party to participate in order to establish a public secret key to achieve mutual or single Entity identification.

The mechanisms specified in this section use time-varying parameters such as timestamps, serial numbers, or random numbers to prevent previously valid authentication information from being Accepted or accepted multiple times.

If there is no trusted third party involved and a timestamp or serial number is used at the same time, the information only needs to be transmitted once for one-way authentication.

Mutual authentication needs to be sent twice. If there is no trusted third party involved and

the challenge-response method using random numbers is used, one-way authentication Don't need to transmit information twice, and for mutual authentication, you need to transmit three times. If there is a trusted third party involved, between an entity and the trusted third party any additional communication of the need to add two transfers in the communication exchange.

2 Normative references

The following documents are indispensable for the application of this document. For dated reference documents, only the dated version applies to this article Pieces. For undated references, the latest version (including all amendments) applies to this document.

ISO/IEC 9798-1 Information Technology Security Technical Entity Authentication Part 1: General Rules

3 Terms and definitions

ISO/IEC 9798-1 and the following terms and definitions apply to this document.

Authenticated encryption the (reversible) transformation of data through a cryptographic algorithm, once the generated ciphertext is replaced by an unauthorized entity, it can be detected Come, that is to say, it provides protection of data confidentiality, data integrity and data origin authentication.

[ISO/IEC 19772:2009] 3.2 Ciphertext Transformed data to hide its information content.

[ISO/IEC 10116:2006] 3.3 Claimant an entity whose identity can be authenticated, including its functions and private data necessary for authentication interaction.

[ISO/IEC 9798-5:2004] 3.4 Message authentication code Use the output bit string generated by the message authentication code algorithm.

Note: The message authentication code is sometimes called the password check value.

[GB/T 15852.1-2008]

Message authentication code algorithm an algorithm that calculates bit strings and keys to obtain a fixed-length bit string has the following characteristics.

---For any key and any input string, it can be calculated effectively;

---For any fixed key, without any prior knowledge about this key, calculate the message of any new input string the authentication code is computationally infeasible.

Note 1: The message authentication algorithm is sometimes called a password verification function (see the example of ISO 7498-2).

Note 2: The specific safety requirements and environment of the user since the feasibility of the calculation.