



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

GB/T 15843.4-2024

Replacing GB/T 15843.4-2008

**Information technology - Security techniques - Entity
authentication - Part 4: Mechanisms using a cryptographic
check function**

网络安全技术 实体鉴别 第4部分：采用密码校验函数的机制

(English Translation)

Issued on: March 15, 2024

Implemented on: October 1, 2024

Issued by: SAMR; SAC

Table of Contents

Foreword	3
Introduction	6
1 Scope	7
2 Normative References	7
3 Terms and Definitions	7
4 Symbols and Abbreviations	7
5 Security Requirements	8
6 Authentication Mechanism	9
6.1 General	9
6.2 Unilateral Authentication	10
6.3 Bidirectional Authentication	11
Appendix A (informative) Object Identifiers	15
Appendix B (informative) Use of Text Fields	16
Bibliography	17

Foreword

This document was drafted in accordance with the rules provided in GB/T 1.1-2020 Directives for Standardization - Part 1: Rules for the Structure and Drafting of Standardizing Documents.

This document is Part 4 of GB/T 15843 Cybersecurity Technology - Entity Authentication.

GB/T 15843 has issued the following parts.

---Part 1: General;

---Part 2: Mechanisms Using Symmetric Encipherment Algorithm;

---Part 3: Mechanisms Using Digital Signature Techniques;

---Part 4: Mechanisms Using a Cryptographic Check Function;

---Part 5: Mechanisms Using Zero Knowledge Techniques;

---Part 6: Mechanisms Using Manual Data Transfer.

This document serves as a replacement for GB/T 15843.4-2008 Information Technology - Security Techniques - Entity Authentication - Part 4: Mechanisms Using a Cryptographic Check Function. In comparison with GB/T 15843.4-2008, apart from structural adjustments

and editorial modifications, the main technical changes are as follows.

- a) The Scope in Chapter 1 is modified (see Chapter 1);
- b) The concatenation symbols are added (see Chapter 4);
- c) The security requirements for authentication keys and cryptographic check values are added [see d) and e) of Chapter 5];
- d) The specific content of Step a) and Step b) of the two-transfer bidirectional authentication mechanism is added (see 6.3.1);
- e) The description of Step b) in the three-transfer bidirectional authentication mechanism process is modified into. A generates a random number RA, generates and sends a token TokenAB to B (see 6.3.2).

This document modifies and adopts ISO/IEC 9798-4:1999 Information Technology - Security Techniques - Entity Authentication - Part 4: Mechanisms Using a Cryptographic Check Function.

In comparison with ISO/IEC 9798-4:1999, this document makes the following structural adjustments.

- a) Chapter 4 "Symbols and Abbreviations" is added, and the subsequent chapters will have their numbers continued in sequence;

1 Scope

This document specifies entity authentication mechanisms using a cryptographic check function, including unilateral authentication and bidirectional authentication mechanisms.

This document is applicable to the design, development, implementation and testing, etc. of entity authentication using a cryptographic check function.

The mechanisms specified in this document use time variant parameters, such as time stamps, sequence numbers or random numbers to prevent the problem that previously valid authentication information is accepted again after it has expired.

If time stamps or sequence numbers are used, unilateral authentication requires only one transfer, while bidirectional authentication requires two transfers. If the challenge-response method of random numbers is used, unilateral authentication requires two transfers, and bidirectional authentication requires three transfers.

For examples of cryptographic check function, see GB/T 15852 (all parts).

2 Normative References

The contents of the following documents constitute indispensable clauses of this document through the normative references in the text. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 15843.1-2017 Information Technology - Security Techniques - Entity Authentication - Part 1: General (ISO/IEC 9798-1:2010, IDT)

3 Terms and Definitions

The terms and definitions defined in GB/T 15843.1-2017 are applicable to this document.

4 Symbols and Abbreviations

The symbols and abbreviations defined in GB/T 15843.1-2017 and the following apply to this document.

$X||Y$. the result of concatenating data items "X" and "Y" in the order of "X" on the left and "Y" on the right.

NOTE: when the concatenation of two or more data items is used as the input of a cryptographic check function, it is guaranteed that the concatenation result is uniquely parsed back to the original data item, that is, there is no ambiguous interpretation. This feature can be implemented in a variety of ways, and the specific implementation is application-dependent. For instance, it can be implemented in the following ways. a) fix the length of the concatenated data item and maintain this length throughout the execution of the authentication mechanism; b) use a decoding-unique encoding method to process the concatenated data item sequence, for example, using the encoding rules defined in GB/T 16263.1.

5 Security Requirements

In the authentication mechanism specified in this document, the entity to be authenticated verifies its identity by indicating that it possesses a certain key. This can be achieved by the entity using its key and the cryptographic check function to calculate a cryptographic check value for the specified data. The cryptographic check value can be verified by any other entity that possesses the entity's key. The method of checking is to re-calculate the cryptographic check value and compare it with the received value. If they are consistent, the result is pass, otherwise it fails.

The authentication mechanism specified in this document has the following security requirements. If any one of them is violated, then, the authentication process may be attacked or cannot be successfully completed.

- a) The claimant who verifies its identity to the verifier shares the key used for authentication with the verifier; before the authentication mechanism is officially started, this key shall be grasped by the relevant parties. The method of distributing the key to the relevant entities is not within the scope of this document;
- b) The authentication key shared by the claimant and the verifier shall only be grasped by these two entities and other entities trusted by both parties;
- c) Parameters, such as key length and cryptographic check value length shall be carefully selected to achieve the required security strength. The method of parameter selection and its corresponding security strength can be clearly specified in the security policy;
- d) The key used to implement any authentication mechanism in this document shall be different from the keys used for other purposes;
- e) In the authentication mechanism, it shall be ensured that the cryptographic check value used for different occasions cannot be exchanged.

NOTE: in order to ensure that the cryptographic check value cannot be exchanged, the following