GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 36624-2018

Information Technology - Security Techniques - Authenticated Encryption

信息技术 安全技术 可鉴别的加密机制

(ISO/IEC 19772:2009, MOD)

Issued on: September 17, 2018 **Implemented on: April 1, 2019**

Issued by: State Administration for Market Regulation;

Standardization Administration of the People's Republic of China.

Table of Contents

Foreword

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

This Standard adopts the re-drafting law to modify the adoption of ISO/IEC 19772:2009 *Information Technology - Security Techniques - Authenticated Encryption*.

In comparison with ISO/IEC 19772:2009, the technical differences and the causes for these differences are as follows:

---In regard to normative references, this Standard makes adjustments with technical differences, so as to adapt to the technical conditions of China. The adjustments are concentratedly reflected in Chapter 2 “Normative References”. The specific adjustments are as follows:

- GB/T 15852.1-2008, which equivalently adopts the international standard, is used to replace ISO/IEC 9797-1 (see 8.4);
- GB/T 17964-2008 is used to replace ISO/IEC 10116 (see 9.3);
- GB/T 32907-2016 is used to replace ISO/IEC 18033-3 (see Chapter 5);
- GB/T 25069-2010 is added to the references (see Chapter 3);

---In Chapter 3, terms and definitions that have already been defined in the current national standards are directly adopted; some common definitions are deleted.

In comparison with ISO/IEC 19772:2009, there are relatively significant adjustments in structure. See the details below:

---The content of Scope in ISO/IEC 19772:2009 is modified; some content is transferred to Chapter 5 Overview;

---In consideration of the practical application scope of China’s national conditions technology, this Standard adopts the five authenticated encryption mechanisms specified in Chapter 7 ~ Chapter 11 in ISO/IEC 19772:2009; deletes the authenticated encryption mechanism specified in Chapter 6 in ISO/IEC 19772:2009;

---Normative Appendix C in ISO/IEC 19772:2009 is adjusted to Appendix A, correspondingly, Informative Appendix A and Appendix B in ISO/IEC 19772:2009 are respectively adjusted to Appendix B and Appendix C;

---The data example provided in Appendix C is modified to use SM4 algorithm as an example.

This Standard makes the following editorial modification:

Information Technology - Security Techniques - Authenticated Encryption

1 Scope

This Standard specifies five authenticated encryption mechanisms, which achieve the following security objectives by defining the methods of processing a data string:

---Data confidentiality, which protects against unauthorized disclosure of data;

---Data integrity, which ensures that the data recipient can verify whether the data has been modified;

---Data source authentication, which ensures that the data recipient can verify the identity of data originator.

This Standard provides ASN.1 definition of the five authenticated encryption mechanisms.

This Standard is appliable to applications and systems that require data confidentiality, integrity protection and data source authentication.

2 Normative References

The following documents are indispensable to the application of this document. 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 15852.1-2008 *Information Technology - Security Techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms Using a Block Cipher* (ISO/IEC 9797-1:1999, IDT)

GB/T 17964-2008 *Information Technology - Security Techniques - Modes of Operation for a Block Cipher*

GB/T 25069-2010 *Information Security Technology - Glossary*

GB/T 32907-2016 *Information Security Technology - SM4 Block Cipher Algorithm*

3 Terms and Definitions

What is defined in GB/T 15852.1-2008, GB/T 17964-2008 and GB/T 25069-2010, and the following terms and definitions are applicable to this document.

3.1 Authenticated Encryption

Authenticated encryption refers to a reversible data conversion that uses cipher algorithm to generate a ciphertext corresponding to the data. Unauthorized entities cannot modify the ciphertext without being detected. Meanwhile, it also provides data confidentiality, data integrity and data source authentication.

3.2 Authenticated Encryption Mechanism

Authenticated encryption mechanism refers to a cryptographic technique used to implement data confidentiality protection and provide data integrity and data source authentication. It includes two processing processes, namely, encryption and decryption.

3.3 Data Integrity

Data integrity refers to the characteristic that data has not been altered or destroyed in an unauthorized mode.

[GB/T 25069-2010, Definition 2.1.36]

3.4 Block Cipher

Block cipher, also known as block cipher algorithm, is a symmetric cipher algorithm that partitions plaintext into fixed-length blocks for encryption.

[GB/T 17964-2008, Definition 3.1.2]

3.5 Encryption System

Encryption system refers to the cryptographic technique used to protect data confidentiality. It includes three processing processes, namely, encryption algorithm, decryption algorithm and key generation.

3.6 Message Authentication Code; MAC

Message authentication code refers to data item derived from the message using symmetric cryptographic technique and secret key. Any entity holding this secret key may utilize message authentication code to check the integrity of the message and the originator.

[GB/T 15852.1-2008, Definition 3.2.5]

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------