NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

GB/T 36624-2018

Information technology -- Security techniques -- Authenticated encryption

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

Issued by: SAMR; SAC

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.

---The content of the corrected version of ISO/IEC 19772.2009 is included.

Please be noted that certain content of this document might involve patents. The institution issuing this document does not undertake the responsibility of identifying these patents.

This Standard was proposed by and shall be under the jurisdiction of National Technical Committee 260 on Information Technology Security of Standardization Administration of China (SAC/TC 260).

The drafting organizations of this Standard. Data Assurance & Communications Security Center; Institute of Software Chinese Academy of Sciences; Beijing JN TASS Technology Co., Ltd.

1 Scope

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

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)

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.

4 Symbols

The following symbols are applicable to this document.

5 Overview

The five authenticated encryption mechanisms specified in this Standard are all based on the block cipher algorithm. Meanwhile, the data originator and data recipient are required to share keys.

6 Authenticated Encryption Mechanism 1

The block cipher algorithm used in this mechanism shall be a 128-bit block cipher algorithm, namely, n = 128.This mechanism requires that the protected data D shall at least contain 128 bits, and the data length shall be an integer multiple of 64 bits [namely, len(D) = 64m, m > 1].

7 Authenticated Encryption Mechanism 2

Before using this authenticated encryption mechanism, the data originator and data recipient shall firstly negotiate and determine the following matters.

8 Authenticated Encryption Mechanism 3

Before using this authenticated encryption mechanism, the data originator and recipient shall firstly determine the standard length t, in which, 0 < t <= n.

The recipient shall execute the following steps to decrypt and verify the authenticated encrypted data C.

9 Authenticated Encryption Mechanism 4

Before using this authenticated encryption mechanism, the data originator and data recipient shall firstly negotiate and determine the following matters.

10 Authenticated Encryption Mechanism 5

Before using this authenticated encryption mechanism, the data originator and recipient shall firstly negotiate and determine the tag length t. The value of t shall be an integer multiple of 8 and satisfy 96 <= t <= 128 (under specific circumstances, the value of t may also be 32 or 64).

Appendix A

(normative)

ASN.1 Module

The five authenticated encryption mechanisms specified in this Standard are respectively corresponding to ae-mechanism2, ae-mechanism3, ae-mechanism4, ae-mechanism5 and ae-mechanism6 in the above ASN.1 definition.

.....