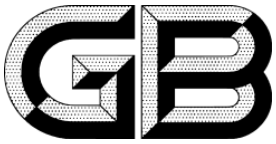

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

GB/T 15843.6-2018

Information technology -- Security techniques -- Entity authentication -- Part 6: Mechanisms using manual data transfer

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

Issued by: SAMR; SAC

Table of Contents

Foreword

GB/T 15843 consists of the following parts, under the general title Information Technology - Security Techniques - Entity Authentication.

--- Part 1.General;

--- Part 2.Mechanisms Using Symmetric Encipherment Algorithms;

--- 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 Part is Part 6 of GB/T 15843.

This Part was drafted as per the rules specified in GB/T 1.1-2009.

This Part uses translation method to equivalently adopt ISO/IEC 9798-6.2010 Information Technology - Security Techniques - Entity Authentication - Part 6. Mechanisms Using Manual Data Transfer.

Please note that some contents of this document may involve patents. The issuing agency of this document does not assume the responsibility to identity these patents.

This Part was proposed by and under the jurisdiction of National Technical Committee

for Standardization of Information Security (SAC/TC 260).

Drafting organizations of this Part. Data Assurance and Communication Security Research Center, Chinese Academy of Sciences; Beijing Certificate Authority Co., Ltd.; and Feitian Technologies Co., Ltd.

Chief drafting staffs of this Part. Xia Luning, Zhang Guozhu, Zhang Qionglu, Lin Xueyan, and Zhu Pengfei.

1 Scope

This Part of GB/T 15843 specifies eight entity authentication mechanisms based on manual data transfer between authenticating devices. This Part indicates how these mechanisms can be used to support key management functions, and provides guidance on secure choices of parameters for the mechanisms. For these 8 mechanisms, this Part gives their ASN.1 definitions, and analyzes and compares their security levels and efficiency.

2 Normative References

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are 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

For the purposes of this document, the terms and definitions given in GB/T 15843.1-

2017 and the following apply.

Function f which maps a string of bits and a short secret key, i.e. a key that can readily be entered into or read from a user device, to a fixed-length string of bits, i.e. a b-bit check-value, satisfying the following properties.

4 Symbols and Abbreviated Terms

A, B - Labels used for the two devices engaging in a manual entity authentication mechanism.

5 Overall Requirements

This Clause specifies the general requirements that the authentication mechanisms 1~8 should meet. In addition to these general requirements, each authentication mechanism shall also meet the specific requirements specified in Clauses 6, 7, and 8.

6 Mechanisms Using a Short Check-Value

In the manual authentication mechanism 1, no authentication information is transmitted through non-secure channels. Therefore, if the random key K and check value are transferred from the device A to the device B before the device B obtains the data string D, it shall not affect the security of mechanism 1.

7 Mechanisms Using a Short Digest-Value or a Short

User compares the random key K and check-value outputted from the two devices; and input the

Accept or Reject signal to the two devices through their simple input interfaces

8 Mechanisms Using a Message Authentication Code (MAC)

This mechanism has two variants (7a and 7b). Mechanism 7a, specified in clause 8.2.3, requires fewer interactions between the two devices, whereas mechanism 7b, specified in clause 8.2.4, requires less manual user interaction.

Annex A

(Normative)

ASN.1 Definition

Annex B

(Informative)

Using Manual Authentication Protocols for the Exchange of

Secrete Keys

This annex describes the method of using the manual authentication mechanism in this Part to perform key exchange so that two communicating entities share a secret key.

Annex C

(Informative)

Using Manual Authentication Protocols for the Exchange of Public Keys

In this annex methods are described that enable devices to reliably exchange a public key using one of the manual authentication mechanisms specified in the body of this Part. The context of the description is between a Certification Authority (CA) and a client of the CA. The CA needs to reliably transfer its public key to the client, and the client needs to reliably transfer its public key to the CA.

.....