

ICS 35.030
CCS L80



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

GB/T 15843.3-2023

**Information technology-Security techniques-Entity
authentication-Part 3: Mechanisms using digital signature
techniques**

信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

(English Translation)

Issued on: March 17, 2023

Implemented on: October 1, 2023

**Issued by: State Administration for Market Regulation;
Standardization Administration of China**

Table of Contents

1 Scope	1
2 Normative references	1
3 Terms, definitions and symbols	1
4 Requirements	1
5 Mechanism	2
5.1 Overview	2
5.2 One-way authentication	2
5.3 Mutual authentication	3
6 Mechanism for introducing online trusted third parties	6
6.1 Overview	6
6.2 Five passes to authenticate TePA-A (initiated by entity A).....	6
6.3 Five passes to authenticate TePA-B (initiated by entity B).....	8
Appendix A (informative appendix) Use of text fields	10
Appendix B (Normative Appendix) OID and ASN.1 Notation	11
B.1 Formal definition	11
B.2 Use of subsequent object identifiers	11
B.3 Coding example based on basic coding rules	11

Preface

GB/T 15843 "Information Technology Security Technical Entity Identification" is currently divided into five parts.

---Part 1.Overview;

---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.

This part is Part 3 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 15843.3-2008 "Information Technology Security Technology Entity Authentication Part 3.Using Digital Signature Technology

The mechanism of technology. Compared with GB/T 15843.3-2008, the main technical changes in this part are as follows.

---Added an authentication mechanism for introducing online trusted third parties (see Chapter 6);

---Added OID and ASN.1 syntax (see Appendix B).

Among them, the relevant chapters and articles involved in the amendment of GB/T 15843.3-2008 are as follows.

Modified item number GB/T 15843.3-2008 chapter number modification description

5 Add Appendix B after Appendix A

The translation method used in this part is equivalent to the ISO /IEC 9798-3:1998 "Information Technology Security Technical Entity Authentication Part 3.

The Mechanism of Using Digital Signature Technology and Amd.1:2010 "Information Technology Security Technology Entity Authentication Part 3.Using Digital

The mechanism of signature technology No. 1 amendment. the introduction of an online trusted third-party authentication mechanism", only editorial changes.

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

The main drafting units of this section. Xi'an Xidian Jietong Wireless Network Communication Co., Ltd., and the State Cryptography Administration

Center, State Key Laboratory of Information Security, China Electronics Standardization Institute, National Radio Monitoring Center Testing Center, Xi'an Electronics

University of Technology, Xi'an University of Posts and Telecommunications, Guangzhou Jiesai Technology Co., Ltd., Shenzhen Minghua Aohan Technology Co., Ltd., China Information Security

Certification Center, National Information Security Engineering Technology Research Center, National Computer Network Emergency Technology Processing Coordination Center, National Information Technology Security

Full Research Center, the First Research Institute of the Ministry of Public Security, the Communication Metrology Center of the Ministry of Industry and Information Technology, the Information Security Level Protection Evaluation Center of the Ministry of Public Security,

University of Defense Technology, Beijing Municipal Affairs Network Management Center, Chongqing University of Posts and Telecommunications, Yulong Computer Communication Technology (Shenzhen) Co., Ltd., People of China

University, Chinese People's Liberation Army Information Security Evaluation and Certification Center, China Telecom Corporation, National Information Center, Peking University Shenzhen Postgraduate

Institute, China Electric Power Research Institute, Beijing Zhongdian Huada Electronic Design Co., Ltd., Southeast University, China Mobile Communications Group Design Institute have

Co., Ltd., Chinese People's Liberation Army Information Engineering University, Jiangnan Institute of Computing Technology, Beijing University of Posts and Telecommunications, Shanghai Longzhao Electronics Co., Ltd.,

Beijing Wulong Telecommunications Technology Company, Beijing Wangbei Hechuang Technology Co., Ltd., Shenzhen Hongdian Technology Co., Ltd., Peking University Founder Group

Company, Haier Group, Beijing Guangxin Finance Technology Co., Ltd., Beijing Liuhe Wantong Microelectronics Technology Co., Ltd., Honghao Ming Chuan Technology (North

Beijing) Co., Ltd., Beijing City Hotspot Information Co., Ltd., Beijing Huaan Guangtong Technology Development Co., Ltd., Maipu Communication Technology Co., Ltd.,

Changchun Jida Zhengyuan Information Technology Co., Ltd., Tsinghua University, Beijing Tianyi Integrated Technology Co., Ltd., Guilin University of Electronic Technology, Xi'an

Realan Technology Co., Ltd., Broadband Wireless IP Standard Working Group, WAPI Industry Alliance.

introduction

This part of GB/T 15843 defines the entity authentication mechanism using digital signature technology, which is divided into two types. one-way authentication and mutual authentication.

Among them, one-way authentication is divided into one-pass authentication and two-pass authentication according to the number of message transfers; mutual authentication is based on the number of message transfers.

The number is divided into two pass authentication, three pass authentication, two pass parallel authentication, and five pass authentication.

Since the distribution method of the certificate used for signature is beyond the scope of this section, the sending of the certificate is optional in all mechanisms.

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

The issuing agency of this document draws attention to the fact that when a declaration

conforms to this document, it may involve the chapter 6 and "a method of two-way authentication of entities".

A kind of two-way authentication method and system for entities based on a trusted third party" and other related patents.

The issuing agency of this document has no position on the authenticity, validity and scope of the patent.

The patent holder has assured the issuing organization of this document that he is willing to work with any applicant under reasonable and non-discriminatory terms and conditions.

Negotiations on patent licensing. The statement of the patent holder has been filed with the issuing agency of this document. For relevant information, please contact

Way to get.

Patentee. Xi'an Xidian Jietong Wireless Network Communication Co., Ltd.

Address. A201, Qinfeng Tower, Xi'an Software Park, No. 68, Keji 2nd Road, High-tech Zone, Xi'an

Contact. Liu Changchun

Please note that in addition to the above-mentioned patents, certain contents of this document may still involve patents. The issuing agency of this document is not responsible for identifying these

Liability for patents.

Information technology security technology entity authentication

Part 3.Mechanisms using digital signature technology

1 Scope

This part of GB/T 15843 specifies an entity authentication mechanism using digital signature technology. There are two authentication mechanisms for a single entity

Authentication (one-way authentication), the rest is the mutual authentication mechanism of two entities.

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 time stamps or serial numbers are used, one-way authentication only needs to be transmitted once, while mutual authentication requires two transmissions. If using random