

ICS 35.040
CCS L 80



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

GB/T 15843.5-2005

**Information technology -- Security technique -- Entity
authentication -- Part 5: Mechanisms using zero knowledge
techniques**

(English Translation)

Issued on: April 19, 2005

Implemented on: October 1, 2005

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine**

Table of Contents

Foreword	4
1 Scope	5
2 Normative Reference	5
3 Terms and Definitions	6
4 Symbols and Notation	8
5 Mechanism Based on Identities	11
5.1 Specific requirements	11
5.2 Parameter selection	11
5.3 Identity selection	12
5.4 Accreditation generation	13
5.5 Authentication exchange	13
6 Certificate-Based Mechanism Using Discrete Logarithms	16
6.1 Specific requirements	16
6.2 Key selection	17
6.3 Authentication exchange	17
7.1 Specific requirements	20
7.2 Authentication exchange	20
Annex A (Normative) Principles of Zero Knowledge Mechanisms	23
A.1 Introduction	23
A.2 The need for zero-knowledge mechanisms	23
A.3 The definition	24
A.4 An example	25
A.5 Basic design principles	27
Annex B (Informative) Guidance on Parameter Choice	28
B.1 Parameter choice for the identity-based mechanism	28
Annex C (Informative) Examples	30
C.1 Mechanism based on identities	30
C.1.1 Example with public exponent 2	30
C.1.2 Example with public exponent 3	34
C.1.3 Example with public exponent $2^{16} + 1$	39
C.2 Mechanism based on discrete logarithms	40
C.2.1 Example using 768-bit p , 128-bit q and RIPEMD-128	40

C.2.2 Example using 1024-bit p, 160-bit q and SHA-1	42
C.3 Mechanism based on a trusted public transformation	44
C.3.1 Example using 767-bit RSA and RIPEMD-160	44
C.3.2 Example using 1024-bit RSA and SHA-1	46
Annex D (Informative) Comparison of the Mechanism	48
D.1 Measures for comparing the mechanisms	48
D.2 Mechanism based on identities	49
D.2.1 The case where v is large (e.g. the Guillou-Quisquater scheme)	49
D.2.2 Fiat-Shamir scheme	51
D.3 Certificate-based mechanism using discrete logarithms	52
D.3.1 Computational complexity	52
D.3.2 Communication complexity	53
D.3.3 Size of the claimant's accreditations	53
D.3.4 Degree of security	53
D.4 Certificate-based mechanism using an asymmetric encipherment system	53
D.4.1 Computational complexity	53
D.4.2 Communication complexity	54
D.4.3 Size of the claimant's accreditations	54
D.4.4 Degree of security	54
D.5 Comparison of the mechanisms	54
Annex E (Informative) Information about Patents	56
Annex F (Informative) Bibliography	57

1 Scope

This Part of GB/T 15843 specifies three entity authentication mechanisms using zero knowledge techniques. All the mechanisms specified in this Part of GB/T 15843 provide unilateral authentication. These mechanisms are constructed using the principles of zero knowledge, but they will not be zero knowledge according to the strict definition sketched in Annex A for all choices of parameters.

The first mechanism is said to be based on identities. A trusted accreditation authority provides each claimant with private accreditation information, computed as a function of the claimant's identification data and the accreditation authority's private key.

The second mechanism is said to be certificate-based using discrete logarithms. Every claimant possesses a public key, private key pair for use in this mechanism. Every verifier of a claimant's identity must possess a trusted copy of the claimant's public verification key;

the means by which this is achieved is beyond the scope of this

Standard, but it may be achieved through the distribution of certificates signed by a

Trusted Third Party.

The third mechanism is said to be certificate-based using an asymmetric encipherment system. Every claimant possesses a public key, private key pair for an asymmetric cryptosystem. Every verifier of a claimant's identity must possess a trusted copy of the claimant's public key; the means by which this is achieved is beyond the scope of this

Standard, but it may be achieved through the distribution of certificates signed by a

Trusted Third Party.

2 Normative Reference

The provisions in following documents become the provisions of this Part through reference in this Part of GB/T 15843. For dated references, the subsequent amendments (excluding corrigendum) or revisions do not apply to this Part, however, parties who reach an agreement based on this Standard are encouraged to study if the latest versions of these documents are applicable. For undated references, the latest edition of the referenced document applies.

GB 15851-1995 Information Technology - Security Techniques - Digital Signature

Scheme Giving Message Recovery (idt ISO/IEC 9796:1991)

GB/T 15843.1-1999 Information Technology - Security Techniques - Entity

Authentication - Part 1: General (idt ISO/IEC 9798-1:1997)

GB/T 18238 (all parts) Information Technology - Security Techniques - Hash-

Function (idt ISO/IEC 10118)

3 Terms and Definitions

For the purpose of this Part of GB/T 15843, the terms and definitions given in GB/T 15843.1-1999 and the following apply.