

ICS 35.040
CCS L 80



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

GB/T 30277-2013

**Information security technology -- Public key infrastructures --
Certification authentication institution identity code
specification**

信息安全技术 公钥基础设施 电子认证机构标识编码规范
(English Translation)

Issued on: January 1, 1970

Implemented on: January 1, 1970

Issued by: Standardization Administration of China

Table of Contents

- Preface
- Introduction
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Abbreviations
- 5 CA Code Methodology
 - 5.1 CA property classification and Conventions
 - Identified item 5.2 CA code
 - 5.3 CA Code Description Item
- 6 CA application code data structure
 - 6.1 Code defines a digital certificate CA
 - 6.2 CA code data structure DER codec Example
- 7 CA directory server code expressions
- Appendix A (normative) in the field of commercial password associated OID Definition
- Appendix B (Informative Appendix) CA organization code in the directory server text entry format
- Appendix C (Informative Appendix) DER encoding TLV Rule

Foreword

This standard is based on GB/T 1.1-2009 given rule drafting.

This standard by the National Safety Standardization Technical Committee (SAC/TC260) and focal points.

This standard was drafted. National Information Security Engineering Research Center, Shanghai Information Security Engineering Technology Research Center, Beijing Rui oil Fei information technology limited liability company.

Introduction

With the development of information technology, the country has built a national electronic root certification authority and a variety of electronic authentication services. To Party Then the electronic certification bodies unified management, and more mutual recognition of digital certificates, electronic authentication needs of each institution in accordance with a

unified regulation Corresponding code or object paradigm criteria for the granting of an identifier. However, there are various electronic certification authority set their own names and their own grid Style, there is no national uniform standard code. This standard for electronic identification code of the certification body is given a uniform specification to meet the information Construction on different electronic certificates issued by certification bodies carried out to identify needs.

Electronic certification body is divided into national, sectoral and other types. After the "Electronic Signature Law" was promulgated, the electronic certification service industry clear primary Authorities, the gradual improvement of relevant laws and regulations. Currently, there are many electronic certification bodies operating license and obtain relevant information systems the Certificate Services, certificates issued by different Certification Authorities recognize the urgent need to develop a unified, standardized identification code mechanism.

This standard can be used for e-government, e-commerce, industries, enterprises and other types of electronic certification bodies.

Information security technology - Public key infrastructure Electronic certification body identification coding standards

1 Scope

This standard establishes general principles of electronic certification bodies Identification Codes specification.

This standard applies to PKI-based applications, unified electronic coding certification body for the establishment of a national CA Directory provides query basic condition.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version suitable for use herein Member. For undated references, the latest edition (including any amendments) applies to this document.

GB/T 16262.1-2006 Information technology - Abstract Syntax Notation One (ASN.1) - Part 1. Specification of basic notation
GB/T 18521 Names and classification of coding rules for
GB/T 20518-2006 Information security technology - Public key infrastructure - Digital certificate format
GB/T 25069-2010 Information security technology terms
GM/T 0006-2012 Application for identification code

3 Terms and Definitions

The following terms and definitions apply to this document.

Electronic certification bodies certificateauthority Responsible for creating and distributing a

certificate authority that is trusted by the user. The user can choose the agency to create a key.

Object Identifier System gives the object a unique entity of digital codes to the identity of the object.

4 Abbreviations

The following abbreviations apply to this document.

CA. Certification Authorities (CertificationAuthority) OID. object identifier (ObjectIdentifier)

PKI. Public Key Infrastructure (PublicKeyInfrastructure)

5.1 CA attribute categories and conventions

CA system can be explained from different angles its features.