

ICS 35.240.15

CCS L 64



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

GB/T 16649.15-2010

**Identification cards -- Integrated circuit cards -- Part 15:
Cryptographic information application**

识别卡 集成电路卡 第15部分：密码信息应用

(English Translation)

Issued on: December 1, 2010

Implemented on: April 1, 2011

Issued by: Standardization Administration of China

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Symbols and abbreviations
5 General
6 Password information object
7 CIO file
The 8 ASN.1 syntax information
Appendix A (normative appendix) ASN.1 module
CIA Examples Appendix B (informative) has a digital signature authentication function of the card
Annex C (informative) Example topology
Examples Appendix D (Informative Appendix) CIO values and their encoded
References

Foreword

GB/T 16649 in the general title "Identification cards - Integrated circuit card" in the current by the following components.

- Part 1. Cards with contacts - Physical characteristics;
- Part 2. Dimensions and location of the contacts Cards with contacts;
- Part 3. Cards with contacts - Electronic signals and transmission protocol;
- Part 4. for structural, security and command exchange;
- Part 5. National numbering system and registration procedure for application identifiers;
- Part 6. inter-industry data elements;
- Part 7. card for Inter Structured Query Language (SCQL) trade order;
- Part 8. Security related inter-industry commands;
- Part 9. Commands for card management;

- Part 10. Cards with contacts synchronization signals and answer to reset the card;
- Part 11. Personal verification through biometric methods (under development);
- Part 12. Cards with contacts - USB electrical interface and operating procedures;
- Part 13. In a multi-application environment, application management commands (under development) is used;
- Part 15. Application of password information.

This section GB/T Part of 1,516,649.

This section identical with the international standard ISO/IEC 7816-15:2004 "Part 15 Identification cards - Integrated circuit card. password information should Use "(in English).

For ease of use, this section made the following editorial changes.

- a) Remove international standards preface;
- b) to the "File" to "in this section." Appendix A of this section is normative annex, appendix B, Appendices C and D are informative appendices.

This part of the National Information Technology Standardization Technical Committee (SAC/TC28) and focal points.

Introduction

GB/T 16649 is the national standard IC card parameters and switching IC card use.

IC card with a password function can be used to secure user identification information systems, and other core security services, for example by Digitally signed to achieve non-repudiation, confidentiality issue for the encoded key. GB/T 16649 purpose of this section is based on available these services provide a standard framework. The main purpose is to provide a solution that can be used for distribution has several compatible card Large system's exchange offer. The system is flexible enough to be used in many different environments, while maintaining the interactivity of the right.

Already it provides a variety of data structures to manage private keys and key data to support public-key infrastructure certificates, with the flexibility to manage Household and entity authentication.

This section GB/T 16649 is based on the PKCS

- Password information;
- Retrieve password information, this feature is a key factor in the concept of "directory file", which provides the card objects and these objects A layer of indirection between the actual format;

- Where appropriate, with other parts of a data object GB/T 16649 defined in the password information to cross-reference;
- Different authentication mechanisms;
- Multiple cryptographic algorithms (their applicability outside the scope of this part of GB/T 16649 in).

This section does not include the card and/or external internal implementation. Not mandatory to perform all of the options in this section.

In the main part of this section and Appendix A of the module there are differences in the definition of ASN.1 case to Appendix A shall prevail.

2 Normative references

The following documents contain provisions which, through reference GB/T 16649 in this section constitute provisions of this section. For dated reference documents Member, all subsequent amendments (not including errata content) or revisions do not apply to this section, however, encouraged to reach under this section Parties to research agreement to use the latest versions of these documents. For undated reference documents, the latest versions apply to this section.

GB/T 13000 Information technology - Universal Multiple-Octet Coded Character Set (UCS) (ISO/IEC 10646:2003, IDT) GB/T 16262 (all parts), Information technology - Abstract Syntax Notation 1 (ASN.1) (idtISO /IEC 8824) GB/T 16263.1 Information technology - ASN.1 encoding rules Part 1. Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) Specification (GB/T 16263.1-2006, ISO/IEC 8825-1:2002, IDT) GB/T 16264.8 Information technology - OSI Directory - Part 8. a public key and attribute certificate frameworks (GB/T 16264.8-2005, ISO/IEC 9594-8:2001, IDT) GB/T 16649 (all parts) Identification cards - Integrated circuit card (ISO/IEC 7816, IDT) GB/T 21078.1 Banking Personal Identification Number management and security - Part 1. ATM and POS systems online PIN the basic principles and requirements for processing (GB/T 21078.1-2007, ISO/IEC 9564-1:2002, MOD) ISO/IEC 7816-11 Identification cards - Integrated circuit cards - Part 11. Adoption of biometric identity verification methods

3 Terms and Definitions

The following terms and definitions apply to this section.