www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Translated English of Chinese Standard: GM/T0006-2012

www.ChineseStandard.net → Buy True-PDF → Auto-delivery.

Sales@ChineseStandard.net

GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
RECORD NO.: 36833-2012

GM/T 0006-2012

Cryptographic application identifier criterion specification

密码应用标识规范

GM/T 0006-2012 -- How to BUY & immediately GET a full-copy of this standard?
1. www.ChineseStandard.net;
2. Search --> Add to Cart --> Checkout (3-steps);
3. No action is required - Full-copy of this standard will be automatically & immediately delivered to your EMAIL address in 0~60 minutes.
4. Support: Sales@ChineseStandard.net. Wayne, Sales manager

Issued on: March 21, 2012 **Implemented on: March 21, 2012**

Issued by: State Cryptography Administration

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Table of Contents

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuer of this document shall not be held responsible for identifying any or all such patent rights.

This Standard was proposed by and shall be under the jurisdiction of the State Cryptography Administration.

The drafting organizations of this Standard: Shandong De'an Information Technology Co., Ltd., Chengdu Westone Information Industry Co., Ltd., Wuxi Jiangnan Information Security Engineering Technology Center, Xingtang Telecommunications Technology Co., Ltd., Shanghai Koal Software Co., Ltd., Beijing Electronic Certificate Authority Center, Wonders Information System Co., Ltd., JIT Co., Ltd., Beijing Haitai Fangyuan Technologies Co., Ltd., Shanghai Electronic Certificate Authority Center.

The main drafters of this Standard: Liu Ping, Liu Xiaodong, Kong Fanyu, Li Yuanzheng, Xu Qiang, Liu Zengshou, Li Shusheng, Tan Wuzheng, Li Yufeng, Li Weiping, Cui Jiuqiang, Zhou Dong.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Introduction

In cryptographic application, some field or phrase is usually used to represent the information data used such as cryptographic algorithm and data entity. If the definitions of these identifiers are not unified, it is difficult to achieve interconnection and interworking between cryptographic protocols and cryptographic interfaces.

The object of this Standard is to standardize the identifiers which are used in all aspects such as cryptographic protocol interfaces and management; to achieve compatibility and unification of all elements of cryptographic infrastructure; to guide and facilitate the development of cryptographic equipment and the implementation of protocols; and to facilitate the work of administrative departments.

The drafting process of this Standard was under the guidance of the National Commercial Cryptography Application Technology System General Work Group.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Cryptographic application identifier criterion specification

1 Scope

This Standard specifies the identifiers in cryptographic applications, which are used for the representation and use of standard algorithm identifiers, key identifiers, equipment identifiers, data identifiers, protocol identifiers and so on.

This Standard applies to the guidance for the standardized use of identifiers in the development and use of cryptographic equipment and cryptographic systems, as well as the guidance for the use of identifiers in the compilation of other relevant standards or protocols.

2 Terms and conventions

For the purposes of this document, the following terms and definitions apply.

2.1

identifier

A 32-bit integer which is used to identify cryptographic algorithm, cryptographic protocols, etc., in cryptographic services and cryptographic management.

2.2

public key certificate

A digital certificate (digital ID) which establish the identity of the entity owning public key. The certificate is signed and issued by the third-party trusted authority, certifying the effectiveness of the binding relationship between the subject public key and the subject identifier information. The certificate usually includes unforgeable public key information which is related to the subject.

3 Symbols and abbreviations

For the purposes of this Part, the following abbreviations apply.

BASE64	Rules of encoding for conversion of hexadecimal data into visible characters
CBC	Cipher block chaining

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

ECB	Electronic code book
CFB	Ciphertext feedback
OFB	Output feedback
OID	Object identifier

4 Format and encoding of identifiers

Identifiers are of the 32-bit unsigned integer type, which are defined and processed directly as the integer type during implementation or call of cryptographic service interfaces or security management interfaces.

During cross-platform transmission, in order to avoid the influences or errors which are caused by the byte order differences of different platforms, identifiers shall be processed in accordance with the network byte order that the big-endian bytes are in front.

5 Cryptographic service type identifiers

5.1 General

Cryptographic service type identifiers define the representation phrases and data of cryptographic algorithm, operational data, cryptographic protocol, etc., which are involved in cryptographic equipment or cryptographic service interfaces. Such data identifiers are used in the calling process of cryptographic equipment or cryptographic service interfaces, such as data encryption, digital signature, identity authentication and other application scenarios.

5.2 Algorithm identifiers

5.2.1 Block cipher algorithm identifiers

Block cipher algorithm identifiers include the types of cryptographic algorithm and the encryption modes of cryptographic algorithm, which are used when calling cryptographic service for cryptographic operation or obtaining the cryptographic operational capability of cryptographic equipment.

The rules for encoding block cipher algorithm identifiers: they are encoded from low bits to high bits; the 0^{th} to the 7^{th} bits indicate the working mode of block cipher algorithm; and the 8^{th} to the 31^{st} bits indicate the block cipher algorithm by bits, e.g.:

——SGD_SM1_ECB:0000 0000 0000 0000 0000 0001 0000 0001 (0x 00 00 01 01)

——SGD_SSF33_MAC:0000 0000 0000 0000 0000 0010 0001 0000 (0x 00 00 02 10)

When multiple block cipher algorithms exist concurrently, they can be represented using “or”.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

The definitions of device status identifiers are as shown in Table 23.

Table 23 -- Device status identifiers

Label	Identifier	Description
SGD_STATUS_INIT	0x00000201	Initial status; KEY has not been installed in cryptographic device, so it can't provide service
SGD_STATUS_READY	0x00000202	Ready status; KEY has been installed in cryptographic device, so it can provide cryptographic service
SGD_STATUS_EXCEPTION	0x00000203	Exceptional status; KEY has been installed but device can't provide cryptographic service

6.5.5 Device number format

Device number which is used in combination with device type, can be the unique identifier for some cryptographic device. When the device types are the same, the device number is unique which is unrepeatable.

Label format: ××××××××-×××-××××× (date of manufacture - batch number - serial number).

Batch number contains 8 digits, indicating the date of manufacture of the cryptographic device, in the order from left to right: 4 digits for year, 2 digits for month and 2 digits for day, e.g. 20080229.

Batch number contains 3 digits, indicating the production batch of the same type of cryptographic devices; and when it is less than 3 digits, then use 0 to complement to 3 digits from the left, e.g. 001.

Serial number contains 5 digits, indicating the serial number of some product batch of some type; and when it is less than 5 digits, then use 0 to complement to 5 digits, e.g. 00123.

The rules for encoding device number: every 4 bits represent 1 number of a device number from high bits to low bits; the 63rd to the 32nd bits indicate the date of manufacture; the 33rd to the 44th bits indicate the production batch; and the 45th to the 64th bits indicate the serial number, e.g.:

20080229 - 001 - 00123 is represented as 0x 20 08 02 29 00 10 01 23.

This is an excerpt of the PDF (Some pages are marked off intentionally)

Full-copy PDF can be purchased from 1 of 2 websites:

1. https://www.ChineseStandard.us

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. https://www.ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - https://www.ChineseStandard.us).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

------ The End ------