

ICS 35.030
CCS L 80

GM

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

GM/T 0110-2021

Key management interoperability protocol specification

密钥管理互操作协议规范

(English Translation)

Issued on: October 18, 2021

Implemented on: May 1, 2022

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative references	2
Terms and definitions	3
Archive	4
Authorization	5
Compromise	6
Message digest	7
Key wrapping (wrapping)	8
Profile	9
Recover	10
Split key	11
Salt	12
Key derivation	13
XEX-based tweaked-codebook mode with ciphertext stealing	14
Managed object	15
Abbreviations	16
Overview	17
Protocol model	18
Object types	19
Overview	20
Storage security	21
Transmission security	22
Identity authentication	23
Access control	24

1 Scope

This document specifies the key management protocol for communication between the key client and the key management server. This protocol is used to complete operations such as object generation, storage, and state transition in the key management server. It also specifies the security requirements for the application of the protocol.

It does not involve the internal logic structure and security design of the key management

server, nor does it involve the business logic of the key client.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 15852.1, Information technology. Security techniques -- Message authentication codes - Part 1: Mechanisms using a block cipher GB/T 32905, Information security techniques -- SM3 cryptographic hash algorithm GB/T 32907, Information security technology -- SM4 block cipher algorithm GB/T 32918 (all parts), Information security technology -- Public key cryptographic algorithm SM2 based on elliptic curves GB/T 35276, Information security technology -- SM2 cryptography algorithm usage specification GM/T 0024, SSL VPN technical specifications GM/Z 4001, Cryptography terminology

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GM/Z 4001 as well as the followings apply.

3.1 Archive

Put infrequently accessed information into long-term storage.

3.2 Authorization

An access right granted to an entity. It expresses a "formal" permission to perform a security function or activity.

3.3 Compromise

Unauthorized disclosure, alteration, replacement, or use of sensitive data (such as key material and other security-related information).

3.4 Message digest

The result of a cryptographic hash operation on a message.

3.5 Key wrapping (wrapping)

A method of encrypting, MAC/signing, or both encryption and MAC/signing a key.

3.6 Profile

A specification of objects, attributes, operations, message elements, and authentication methods. These objects, attributes, operations, message elements, and authentication methods are used in the interaction between a key management service and a client in a specific context.

3.7 Recover

Recover information that has been archived for long-term preservation.

3.8 Split key

The process of splitting a key into n key components using secret sharing technology.

Each key component cannot be used to deduce the original key alone, but when combined together, the original key can be reconstructed. If k key components ($k \leq n$) are required to reconstruct the original key, then if only $k - 1$ key components are known, the key information of the original key cannot be gotten.

3.9 Salt

A random variable added as a secondary input to a one-way or encryption function that can be used to derive password verification data.

3.10 Key derivation

Derive one or more secret keys from a secret value of a master key, password, or passphrase using a pseudorandom function. It can be used to extend a key into a longer key or to get a key in a desired format.

3.11 XEX-based tweaked-codebook mode with ciphertext stealing

An adjustable codebook mode based on the XEX (XOR-ENCRYPT-XOR) ciphertext stealing algorithm. This encryption mode is mainly used to encrypt static data in storage devices based on data units (including sectors, logical disk blocks, etc.).

3.12 Managed object

The objects managed by the key management server, including symmetric keys, asymmetric keys, certificates, secret data, opaque objects, etc.

4 Abbreviations

The following abbreviations apply to this document.

ASN.1. Abstract Syntax Notation One CA. Certification Authority CRL. Certificate Revocation List CRT. Chinese Remainder Theorem CTR. Counter DER. Distinguished Encoding Rules DNS. Domain Name System GCM. Galois Counter Mode HMAC. Keyed-Hash Message Authentication Code IP. Internet Protocol ISO. International Organization for Standardization IV. Initialization Vector KMIP. Key Management Interoperability Protocol MAC. Message Authentication Code PKCS. Public Key Cryptography Standards PKI. Public Key Infrastructure PSS. Probabilistic Signature Scheme RNG. Random Number Generator RSA. An asymmetric cryptographic algorithm TTLV. Tag, type, length, value URI. Uniform Resource Identifier URL. Uniform Resource Locator XTS. XEX-based tweaked-codebook mode with cipher text stealing

5 Overview

This document aims to define a set of communication protocol specifications between key clients and key management servers. Through this protocol, operations such as creation, storage, use and destruction of objects in the key management server can be completed. These objects are collectively referred to as managed objects in this document. Managed objects in this document include symmetric keys, asymmetric keys, digital certificates, etc. Managed objects have a series of attributes. Attribute information is stored in the key management service. These attributes can be added, modified or deleted through the key management service. The object management operations that the key management server can support include generating encryption keys, importing password objects, querying objects, getting objects, and destroying objects. For standard application examples and main application scenarios, please refer to Annex A.

6.1 Protocol model

The interaction model of the key management interoperability protocol is shown in Figure 1.

Figure 1 -- Interaction model of key management interoperability protocol

As shown in Figure 1, the client sends a request message to the key management server.

The request message shall contain information such as client identity authentication, operation identifier, and operation parameters. The key management server performs corresponding operations according to the request message and returns the operation results to the client as a response message. The response message contains the result state and result data. The protocol described in this document has the following characteristics.

a) Messages are independent of each other. Implementors do not need to maintain message-related states. For specific message data formats and encodings, see 6.5.