

ICS 35.040
CCS L 80

GM

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

GM/T 0093-2020

Certificate and key exchange format specification

证书与密钥交换格式规范

(English Translation)

Issued on: December 23, 2020

Implemented on: July 1, 2021

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative references	2
Terms and definitions	3
Abbreviations	4
OID definition	5
CKX type	6
AuthenticatedSafe type	7
Overview	8
KeyBag Type	9
CrlBag type	10
SafeContents type	11
Create CKX data unit	12
Import keys and certificates from a CKX data unit	13
Extended attributes	14

1 Scope

This document specifies the transmission syntax of information, such as certificates and keys, including private keys, certificates, certificate revocation lists, various forms of secret values, as well as their extended standardized packaging.

This document is suitable for application scenarios, where personal SM2 algorithm certificates and keys and other information are migrated between different platforms.

2 Normative references

The contents of the following documents constitute the indispensable clauses of this document through normative references in the text. Among them, for dated reference documents, only the version corresponding to that date is applicable to this document; for undated reference documents, the latest version (including all amendments) is applicable to this document.

GB/T 15852.2-2012 Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function GB/T 35275-2017 Information security technology - SM2 cryptographic algorithm encrypted signature message syntax specification GB/T 35276-2017 Information security technology - SM2

cryptography algorithm usage specification GB/T 33560-2017 Information security technology - Cryptographic application identifier criterion specification GM/T 0091-2020 Password-based key derivation specification GM/Z 4001 Cryptographic terms

3 Terms and definitions

The terms and definitions, which are defined in GM/Z 4001 and GM/T 0091-2020, are applicable to this document.

Attribute

An ASN.1 type, which identifies an attribute type (through an object identifier) AND its associated attribute value.

Platform

A collection of machine hardware, operating system, application software.

Source platform

The platform of origin of the personal information, that will ultimately be delivered to the target platform.

Target platform

The final destination platform, to which the personal information generated on the source platform is to be transmitted.

Destination encryption key pair the key pair of a specific platform, which is used in the public key confidentiality protection method.

4 Abbreviations

The following abbreviations apply to this document.

ASN.1. Abstract Syntax Notation One, X.208 CKX. Certificate and Key Exchange Format. This document specifies a portable format, for storing and transmitting user or server private keys, public keys, certificates. It is a binary format; these files are also called CKX files.

5 OID definition

This document defines the identifiers of the six objects keyBag, shroudedKeyBag, certBag, crlBag, secretBag, safeContentBag, as well as related attribute identifiers, as shown in Table 1.

6.1 CKX type

CKX is the highest-level exchange data unit, which is defined in this document.

The integrity protection of AuthenticatedSafe content is used, to realize the secure transfer of CKX data units from one platform to another.

6.2 AuthenticatedSafe type

The contentType field of authSafe is Data type or SignedData type. The content field of authSafe directly (when the type is Data) or indirectly (when the type is SignedData) contains an AuthenticateSafe type BER code.

6.4.1 Overview

This document defines 6 types of SafeBag, which are corresponding to KeyBag, ShroudedKeyBag, CertBag, CRLBag, SecretBag, SafeContents types.

6.4.2 KeyBag Type

The KeyBag of this document is an SM2 private key type ECPrivateKey.

6.4.5 CrlBag type

CRLBag contains a certificate revocation list (CRL). Use object identifiers to distinguish different types of CRLs.

6.4.7 SafeContents type

The sixth type of SafeBag is SafeContents, which allows multiple KeyBag, EncryptedPrivateKeyBag, CertBag, CRLBag, SecretBags to be nested, under the upper layer SafeContents, in a recursive manner.

7.1 Create CKX data unit

The steps to create a CKX data unit are described below.

7.2 Import keys and certificates from a CKX data unit

Importing from CKX is the opposite of the process of creating a CKX. Generally speaking, when an application imports keys from CKX, etc., all irrelevant object identifiers shall be ignored. Sometimes, users need to be reminded to provide certain object identifiers.

8 Extended attributes

This document provides the exchange format of certificates and keys.

GM/T 0093-2020

CRYPTOGRAPHIC INDUSTRY STANDARD ICS 35.040 CCS L 80 Certificate and key exchange format specification Issued on. DECEMBER 28, 2020 Implemented on. JULY 01, 2021 Issued by. National Cryptography Administration

Table of Contents

Foreword... 3

Introduction... 4

1 Scope... 6

2 Normative references... 6

3 Terms and definitions... 6

4 Abbreviations... 8

5 OID definition... 8

6 Definition of basic type... 9

6.1 CKX type... 9

6.2 AuthenticatedSafe type... 11

6.3 SafeContents type... 12

6.4 SafeBag type... 13

7 Basic process of certificate and key exchange... 16

7.1 Create CKX data unit... 16

7.2 Import keys and certificates from a CKX data unit... 17

8 Extended attributes... 17 Appendix A (Normative) ASN.1 syntax notation... 18 Appendix B (Informative) Import and export example of double certificate and private key... 22

References... 30

1 Scope

This document specifies the transmission syntax of information, such as certificates and keys, including private keys, certificates, certificate revocation lists, various forms of secret values, as well as their extended standardized packaging.

This document is suitable for application scenarios, where personal SM2 algorithm