Chinastandards.org

ICS 35.040
CCS L 80

GM

GM/T 0085-2020

Identity-based cryptographic algorithm SM9 based on technology system framework

基于SM9标识密码算法的技术体系框架

(English Translation)

Issued on: December 28, 2020 **Implemented on: July 1, 2021**

Issued by: State Administration of Cryptography

Preview: page 1 of 5 shown, 17 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0085-2020

Chinastandards.org

Table of Contents

Scope 1
Normative references 2
Terms and definitions 3
Abbreviations 4
Basic features 5
Upper-level identification key management system 6
Lower-level application key management system 7
Classification overview 8
Overall framework class 9
Encryption service class 10
Cryptographic application interface class 11
Application protocol class 12

1 Scope

This document describes the identity-based cryptographic algorithm SM9 based on IBC technology application framework, the framework of the identification cryptographic key management system, and the standard specifications involved in the application of the SM9 identification cryptographic algorithm.

This document applies to the application system construction, product and system development of SM9 identity-based cryptographic algorithm, the identification cryptographic key management system construction and management, and related standard development and inquiries.

2 Normative references

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

GM/T 0044.1, Identity-based cryptographic algorithms SM9 - Part 1: General GM/T 0044.2, Identity-based cryptographic algorithms SM9 - Part 2: Digital signature algorithm GM/T 0044.3, Identity-based cryptographic algorithms SM9 - Part 3: Key exchange protocol GM/T 0044.4, Identity-based cryptographic algorithms SM9 - Part 4: Key encapsulation

Preview: page 2 of 5 shown, 17 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0085-2020

mechanism and public key encryption algorithm GM/T 0086, Specification of key management system based on SM9 identity cryptography algorithm GM/Z 4001, Cryptology terminology

3 Terms and definitions

Terms determined by GM/T 0044.1 ~ GM/T 0044.4, and GM/Z 4001, and the following ones are applicable to this document.

Identity-based cryptography; IBC A cryptographic mechanism for generating a user key based on the unique identity of the user/entity and the system master key within the specified application range.

Public parameter service; PPS the service of providing users of the IBC system with related public information, including cryptographic algorithm parameters, system policies and user identification changes.

4 Abbreviations

The following abbreviations apply to this document.

KMS: Key Management Server PPS: Public Parameter Server

5 Basic features

IBC is a public key cryptography technology. It can calculate the user's public key from the identity of the user/entity (hereinafter collectively referred to as the user) and a set of public mathematical parameters. The corresponding user's private key is calculated from the user ID, a set of public mathematical parameters, and a secret value (system private key and other parameters) within a domain.

This document uses the identity-based cryptographic algorithm of GM/T 0044.1 ~ GM/T 0044.4. It can support cryptographic operations such as digital signature and verification, data encryption and decryption, key agreement, key encapsulation and transmission, and can realize the basic functions of public key cryptography.

identification status release services, trusted time services, etc. for IBC technology applications. This part relies on the theory of the basic technical part, the calculation support of the cryptographic equipment part and the interface part to complete the functional services of the source of trust; it is used to support various applications of IBC technology.

The cryptographic device service consists of cryptographic machines, cryptographic cards, smart cryptographic terminals and other devices, and provides basic cryptographic services to the general cryptographic service layer through standard cryptographic device application interfaces.

Preview: page 3 of 5 shown, 17 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0085-2020

The main functions include key generation, cryptographic operations and other services.

The cryptographic device accepts the cryptographic device management of the general cryptographic service layer through a unified device management interface.

The cryptographic device shall have functions such as key loading, storage, update, backup and recovery, and ensure the security of the key in the cryptographic device.

The general cryptographic service is composed of general cryptographic services and cryptographic device management services, which provide upper-layer applications with cryptographic services and device management services that are transparent to the underlying specific cryptographic devices.

The general cryptographic service provides general cryptographic services such as identification authentication, confidentiality, integrity and non-repudiation of information to the typical cryptographic service layer and application layer through a unified cryptographic service interface, and transforms the upper-layer cryptographic service requests into specific basic cryptographic operation request, and calls the corresponding cryptographic device through a unified cryptographic device application interface to achieve specific cryptographic operations and key operations.

The cryptographic device management provides a unified device management application interface to the upper management application, provides device management functions for the upper management applications such as remote key management, device maintenance, and device monitoring, and converts the management request of the upper management application into a standard message call, and realizes the message transfer between the management application and the cryptographic device through a secure channel.

A typical cryptographic service consists of services such as identity authentication, single sign-on, access control, time stamp and electronic seal, and provides corresponding cryptographic services for upper-level applications.

Figure 2 - Key infrastructure relationship architecture diagram

See GM/T 0086 for the technical specifications of the key management system.

The distribution method means that the lower-level KMS applies to the upper-level KMS to generate and sign a master key pair through the following process.

The reporting method means that the lower-level KMS generates a pair of master keys, and the upper-level KMS signs its master public key through the following process.

The independently deployed identification key management system can generate the master key and set the application layer master key by itself.

Preview: page 4 of 5 shown, 17 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0085-2020

7.2 Upper-level identification key management system

The upper-level identification key management system is divided into two types:

the hierarchical management KMS system and the independent KMS application system.

a) KMS system of hierarchical management the upper-layer identification key management system includes upper-level KMS and upper-level PPS publishing system.

The upper-level KMS is the trust foundation of the IBC system and runs independently in an offline manner. Class and control the application infrastructure, to generate the master private key for the key distribution method KMS.

The higher-level PPS publishing system publishes the benchmark algorithm parameters specified by this root, all the information of the application KMS system registered through this root, the PPS address and status, forming a unified management structure and a complete deployment structure, to provide mutual recognition and mutual trust inquiry list for each application IBC system.

b) Independent KMS application system the independent key management infrastructure includes the application KMS and the application PPS publishing system.

Independent KMS, itself, is the source of trust for this IBC system; it operates independently in an online manner to provide key issuance management services for applications.

The independent PPS publishing system publishes the basic algorithm parameters and user key status information specified by this root, and provides parameter and key information query services for applications.

7.3 Lower-level application key management system

The lower-level application key management infrastructure is divided into three types: key distribution method, key reporting method, and independent deployment method.

a) Key distribution method application KMS the key distribution method application KMS shall apply for registration to the upper-level KMS, and the upper-level KMS shall issue the application master private key from top to bottom, which is controlled by the root.

When the IBC operation system indicates that it can provide users with safe and reliable services, the registered KMS system shall be used to issue private keys for them.

b) Key reporting method application KMS the key reporting method application KMS is to self-generate the application root key according to the public parameters issued by an upper-level KMS, and report its public key to the upper-level KMS, and accept the supervision and management of the upper-level KMS.

c) Independent deployment method application KMS the independent deployment method application KMS as a self-generated root key and is managed by itself, without reporting to

Preview: page 5 of 5 shown, 17 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0085-2020