Chinastandards.org

ICS 35.040

GM

GM/T 0044.4-2016

Identity-based cryptographic algorithms SM9 - Part 4: Key encapsulation mechanism and public key encryption alogorithm

SM9标识密码算法 第4部分：密钥封装机制和公钥加密算法

(English Translation)

Issued by: State Administration of Cryptography

Preview: page 1 of 3 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0044-4-2016

Chinastandards.org

Table of Contents

1 Scope
2 Normative references
3 Terms and definitions
3.1 Secret key
3.2 Message
3.3 Key derivation function
3.4 Encryption master key
3.5 Identity
3.6 Key generation center (KGC)
4 Symbols

1 Foreword

GM/T 0044.4-2016 was issued by State Administration of Cryptography on 28 March 2016.

It is one of 6 parts of the GM/T 0044 series.

The GM/T prefix marks a recommended standard. It is not law in itself: it becomes binding when a contract names it, when a regulation or a mandatory standard refers to it, or when a producer declares conformity with it.

2 Scope Preview

This part specifies an identity-based key encapsulation mechanism, and a public key encryption and decryption algorithm built upon pairings from elliptic curves and specifies the corresponding processes. The key encapsulation mechanism can be used to encapsulate a secret key to a specific entity. The public key encryption and decryption algorithms are identity-based asymmetric cryptographic algorithms, which allow the sender to encrypt the message using the identity of a receiver, and only the receiver can decrypt the encrypted message using its corresponding private key. This part applies to the key encapsulation and the encryption and decryption of a message.

GM/T 0044.4-2016 falls under ICS 35.040, in the field of information technology.

This catalogue holds 105 other GM/T standards in that field.

In this catalogue, GM/T standards carry edition years from 2012 to 2024.

Preview: page 2 of 3 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0044-4-2016

3 Normative references

GM/T 0004 - , SM3 Cryptographic Hash Algorithm GM/T 0002, SM4 Block Cipher Algorithm

GM/T 0044.1 - ?2016, SM9 Identity-based Cryptographic Algorithms - Part 1: General

GM/T 0044.3 - ?2016, SM9 Identity-based Cryptographic Algorithms - Part 3: Key Exchange Protocol GM/Z 4001, Cryptographic Terminology

4 About this standard

Issued by: State Administration of Cryptography

English translation: about 19 pages

5 Related standards

Other parts of this standard:

GM/T 0044-2016 - SM9 identity-based cryptographic algorithm

GM/T 0044.1-2016 - Part 1: General

GM/T 0044.2-2016 - Part 2: Digital signature algorithm

GM/T 0044.3-2016 - Part 3: Key exchange protocol

GM/T 0044.5-2016 - Part 5: Parameter definition

6 Classification and status

International classification (ICS): 35.040

Prefix GM/T: recommended standard.

Preview: page 3 of 3 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0044-4-2016