Chinastandards.org

ICS 35.040

GM

GM/T 0044.2-2016

Identity-based cryptographic algorithms SM9 - Part 2: Digital signature algorithm

SM9标识密码算法 第2部分：数字签名算法

(English Translation)

Issued by: State Administration of Cryptography

Preview: page 1 of 3 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0044-2-2016

Chinastandards.org

Table of Contents

1 Scope
2 Normative references
3 Terms and definitions
4 Symbols
5 Algorithm parameters and auxiliary functions
5.1 General
5.2 System parameter group
5.3 Generation of system signature master key and user signature key
5.4 Auxiliary functions
6 Digital signature generation algorithm and flow
6.1 Digital signature generation algorithm
6.2 Digital signature generation algorithm flow
7 Digital signature verification algorithm and flow
7.1 Digital signature verification algorithm
7.2 Digital signature verification algorithm flow

1 Foreword

GM/T 0044.2-2016 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 of GM/T 0044?2016 specifies an identity-based digital signature algorithm built upon pairings from elliptic curves, including the digital signature generation and verification algorithms together with their corresponding processes. This part of GM/T 0044?2016 is applicable for a receiver to use the signer's identity to verify data integrity and the sender's identity; and for a third party to verify authenticity of a signature and the signed message.

GM/T 0044.2-2016 falls under ICS 35.040, in the field of information technology.

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

Preview: page 2 of 3 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0044-2-2016

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

3 Normative references

GM/T 0004 - , SM3 Cryptographic Hash Algorithm GM/T 0005, Randomness Test Specification

GM/T 0044.1 - ?2016, SM9 Identity-based Cryptographic Algorithms - Part 1: General GM/Z 4001, Cryptographic Terminology

4 About this standard

Issued by: State Administration of Cryptography

English translation: about 13 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 0044.3-2016 - Part 3: Key exchange protocol

GM/T 0044.4-2016 - Part 4: Key encapsulation mechanism and public key encryption alogorithm

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, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0044-2-2016