Chinastandards.org

ICS 35.040
CCS L 80

GM

GM/T 0091-2020

Password-based key derivation specification

基于口令的密钥派生规范

(English Translation)

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

Issued by: State Administration of Cryptography

Preview: page 1 of 5 shown, 21 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0091-2020

Chinastandards.org

Table of Contents

Foreword 1
Scope 2
Normative references 3
Terms and definitions 4
Algorithm identifier 5
Key derivation function 6
Symbols and abbreviations 7
Password-based key derivation function 8
Encryption operation 9
Decryption operation 10
MAC generation 11
MAC verification 12
Foreword 13
MAC generation 14
MAC verification 15

Foreword

This document was drafted in accordance with the rules given in GB/T 1.1-2020, Directives for standardization - Part 1: Rules for the structure and drafting of standardizing documents.

1 Scope

This document specifies password-based key derivation specifications, including password-based key derivation function, password-based key encryption scheme, password-based message authentication code.

This document applies to the migrated key which is protected by password during certificate and key migration.

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.

Preview: page 2 of 5 shown, 21 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0091-2020

GB/T 15852.2, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function

3 Terms and definitions

Terms and definitions determined by GB/T 25069-2010, GM/Z 4001, and the following ones are applicable to this document.

3.1 Algorithm identifier

A symbol that is used to uniquely identify a cryptographic algorithm.

3.2 Key derivation function

A function that generates one or more shared secret keys by acting on the shared secret and other parameters which are known to both parties.

[Source. GB/T 25069-2010, 2.2.2.124]

4 Symbols and abbreviations

The following symbols and abbreviations apply to this document.

C. ciphertext, a byte string.

c. iteration count, a positive integer.

DK. derived key, a byte string.

dkLen. the number of bytes of the derived key, a positive integer.

6 Password-based key derivation function

The key derivation function KDF usually uses a password and other parameters to obtain the derived key.

7.1 Encryption operation

The encryption operation that is based on the password P specifically includes the following steps.

7.2 Decryption operation

The steps for decrypting ciphertext C into message M based on password P are as follows.

Preview: page 3 of 5 shown, 21 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0091-2020

8.1 MAC generation

The specific steps for generating the message authentication code T of the message M based on the password P are as follows.

8.2 MAC verification

Process the message M based on the password P; the steps to verify the message authentication code T are as follows.

GM/T 0091-2020

CRYPTOGRAPHY INDUSTRY STANDARD ICS 35.040 CCS L 80 Password-based key derivation specification Issued on. DECEMBER 28, 2020 Implemented on. JULY 01, 2021 Issued by. State Cryptography Administration

Table of Contents

Foreword... 3

1 Scope... 4

2 Normative references... 4

3 Terms and definitions... 4

4 Symbols and abbreviations... 5

5 OID definition... 6

6 Password-based key derivation function... 6

7 Password-based key encryption scheme... 8

7.1 Encryption operation... 8

7.2 Decryption operation... 9

8 Password-based message authentication code... 9

8.1 MAC generation... 9

8.2
MAC verification... 10 Appendix A (Informative) Assistive technology... 11 Appendix B (Normative) ASN.1 grammar... 16 Appendix C (Normative) ASN.1 structure definition... 19 References... 21

Foreword

This document was drafted in accordance with the rules given in GB/T 1.1-2020, Directives for standardization - Part 1: Rules for the structure and drafting of standardizing documents.

Preview: page 4 of 5 shown, 21 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0091-2020

Chinastandards.org

8.1 MAC generation

The specific steps for generating the message authentication code T of the message M based on the password P are as follows.

8.2 MAC verification

Process the message M based on the password P; the steps to verify the message authentication code T are as follows.

Preview: page 5 of 5 shown, 21 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0091-2020