GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

File No.: 38307-2013

GM/T 0009-2012

SM2 cryptography algorithm application specification

SM2 密码算法使用规范

Issued on: November 22, 2012 **Implemented on: November 22, 2012**

Issued by: State Cryptography Administration

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. The issuing authority shall not be held responsible for identifying any or all such patent rights.

This Standard was proposed by and shall be under the jurisdiction of State Cryptography Administration.

Main drafting organizations of this Standard: Beijing Haitai Fangyuan Technologies Co., Ltd., Westone Information Industry Inc., Wuxi Jiangnan Information Security Engineering Technology Center, Xingtang Communication Technology Co., Ltd., Shandong De'an Information Technology Co., Ltd., Shanghai Koal Software Co., Ltd.

Main drafters of this Standard: Liu Ping, Jiang Hongyu, Liu Zengshou, Zeng Yubo, Li Yuanzheng, Xu Qiang, Tan Wuzheng, Kong Fanyu, Wang Nina.

SM2 cryptography algorithm application specification

1 Scope

This standard defines the application method of SM2 cryptography algorithm, as well as the data formats of secret key, encryption and signature.

This standard applies to the use of SM2 cryptography algorithm, as well as the research-development and testing of equipment and systems that support SM2 cryptography algorithm.

2 Normative references

The following documents are essential for the application of this document. For dated references, only the dated version applies to this document. For undated references, the latest edition (including all amendments) applies to this document.

GM/T 0003 (all parts) SM2 elliptic curve public key cryptography algorithm

GM/T 0004 SM3 cryptographic hash algorithm

3 Terms and definitions

The following terms and definitions apply to this document.

3.1

Algorithm identifier

It is used to indicate the digitized information of algorithmic mechanism.

3.2

SM2 algorithm

It is an elliptic curve cryptography algorithm with a key length of 256 bits.

3.3

SM3 algorithm

It is a hash algorithm with an output length of 256 bits.

For M_0, the leftmost 8-blen% 8-bit is set to 0, and the right is set to $B_0B_1 \ldots B_{8-8mlen+blen-1}$.

Output M.

6.2 The conversion from Octet String to Bit String

The conversion process from Octet String to Bit String is as follows:

INPUT: An Octet String with a length of mlen -- M.

OUTPUT: A Bit String with a length of blen -- B.

ACTION: Convert Octet String -- $M = M_0M_1 \ldots M_{mlen-1}$ into Bit String -- $B = B_0B_1 \ldots B_{blen-1}$; use the following method:

From $0 \le i \le mlen-1$, set: $B_{8i}B_{8i+1} \ldots B_{8i+7} = Mi$

Output B.

6.3 The conversion from integer to Octet String

If an integer is converted into Octet String, the basic method is to use binary system to express first, then convert Result Bit String into Octet String. The following is the conversion process:

INPUT: a non-negative integer x, the expected length of Octet String is mlen. The basic restriction is:

$$2^{8(rnlen)} > x$$

OUTPUT: An Octet String with a length of mlen -- M.

ACTION: Convert x-value $x = X_{mlen-1}2^{8(mlen)} + X_{mlen-2}2^{8\ (rnlen-2)} + \ldots + x_1 2^8 + x_0$ based on $2^8=256$ into an Octet String $M = M_0M_1 \ldots M_{mlen-1}$; use the following method:

From $0 \le i \le mlen-1$, set: $M_i = X_{mlen-1-i}$

Output M.

6.4 The conversion from Octet String to integer

Octet String may be simply regarded as integer that is based on 256, and the conversion process is as follows:

INPUT: An Octet String with a length of mlen -- M.

OUTPUT: An integer x.

9 Calculation process

9.1 Generating keys

SM2 key-generation refers to the process of generating the key-pair of SM2 algorithm; the key-pair includes the private key and the corresponding public key. The length of the private key is 256 bits and the length of the public key is 512 bits.

INPUT: None

OUTPUT: k SM2PrivateKey SM2 private key

Q SM2PublicKey SM2 public key

For detailed calculation process, see GM/T 0003.

9.2 Encryption

SM2 encryption refers to the process of generating the corresponding ciphertext by using the specified public key to perform the specific encryption-calculation on the plaintext. The ciphertext can only specify the private key that is corresponding to the public key to decrypt.

INPUT: Q SM2PublicKey SM2 public key

m Byte String Plaintext data to be encrypted

OUTPUT: c SM2Cipher Ciphertext

Where:

The format of the output parameter c is defined in 7.2;

XCoordinate and YCoordinate of the output parameter c are x-component and y-component of the public key that is randomly generated;

The calculation formula of HASH in the output parameter c is:

$$HASH = SM3 (x \| m \| y)$$

In which, x and y are x-component and y-component of Q;

CipherText in the output parameter c is an encrypted ciphertext whose length is equal to the length of plaintext.

For detailed calculation process, see GM/T 0003 and GM/T 0004.

9.6 Key agreement

Key agreement is the agreement process of establishing a shared secret key between two users. In this way, the value of a shared secret key can be determined.

Suppose the two sides of key agreement are A and B, the key-pairs are (d_A, Q_A) and (d_B, Q_B) respectively; and the bit length of the key data that both sides need to obtain is klen. Key agreement protocol is divided into two stages.

Stage I: Produce temporary key-pair

User A:

Call and generate key algorithm to produce temporary key-pair (r_A, R_A), identify ID for the identity of R_A and user A. Send it to user B

User B:

Call and generate key algorithm to produce temporary key-pair (r_B, R_B), identify ID for the identity of RB and user B. Send it to user A

Stage II: Calculate a shared secret key

User A:

Input parameters:

Q_A	SM2PublicKey	User A's public key
Q_B	SM2PublicKey	User B's public key
R_A	SM2PublicKey	User A's temporary public key
ID_A	OCTET STRING	User A's ID
R_B	SM2PublicKey	User B's temporary public key
ID_B	OCTET STRING	User B's ID
d_A	SM2PrivateKey	User A's private key
r_A	SM2PrivateKey	User A's temporary private key
klen	INTEGER	The bit length of the key data that needs to be outputted

Output parameters:

K	OCTET STRING	The key data whose bit length is Men

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------