www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Translated English of Chinese Standard: GM/T0003.3-2012

www.ChineseStandard.net → Buy True-PDF → Auto-delivery.

Sales@ChineseStandard.net

GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
File No.: 36828-2012

GM/T 0003.3-2012

Public key cryptographic algorithm SM2 based on elliptic curves – Part 3: Key exchange protocol

Issued on: March 21, 2012 **Implemented on: March 21, 2012**

Issued by: State Cryptography Administration

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Table of Contents

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Public key cryptographic algorithm SM2 based on elliptic curves - Part 3: Key exchange protocol

1 Scope

This Part of GM/T 0003 specifies the key exchange protocol of public key cryptographic algorithm SM2 based on elliptic curves and gives the examples and their processes of key exchange.

This Part applies to the key exchange in commercial cryptography applications, which can satisfy both sides of communication to use two or optional three message passing processes to compute and obtain one shared secret key (session key) decided by both sides. Meanwhile, this Part can also provide standard positionings and standardization references of products and technologies for security product manufacturers to improve the credibility and interoperability of security products.

2 Normative references

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

GM/T 0003.1-2012, *Public key cryptographic algorithm SM2 based on elliptic curves – Part 1: General*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

key confirmation from A to B

guarantee which convinces user B that user A has a certain secret key

3.2

key derivation function

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

K, K_A, K_B: a shared secret key agreed upon in the key exchange protocol.

KDF(): the key derivation function.

mod*n*: the modulo n operation. E.g.: 23 mod 7 = 2.

n: the order of base point *G* (*n* is the prime factor of $\#E(F_q)$).

O: one special point on the elliptic curve, called the point at infinity or null point, which is the identity element of the additive group of the elliptic curve.

P_A: the public key of user A.

P_B: the public key of user B.

q: the number of elements in the finite field F_q.

r_A: the value of a temporary key generated by user A in a key exchange.

r_B: the value of a temporary key generated by user B in a key exchange.

$x \| y$: the concatenation of *x* and *y*, where *x* and *y* can be a bit string or byte string.

Z_A: the hash value in regard to distinguishing identifiers of user A, some system parameters of elliptic curve and public keys of user A.

Z_B: the hash value in regard to distinguishing identifiers of user B, some system parameters of elliptic curve and public keys of user B.

$\#E(F_q)$: the number of points on $E(F_q)$, called the order of elliptic curve $E(F_q)$.

[*k*]*P*: the *k* point-multiplication of point *P* on elliptic curve, i.e. $[k]P=\underbrace{P+P+\cdots+P}_{\text{Number k}}$,

where *k* is a positive integer.

[x, y]: the set of integers which is greater than or equal to *x*, and less than or equal to *y*.

$\lceil x \rceil$: the ceiling function, which is the minimum integer greater than or equal to *x*. E.g.:

$\lceil 7 \rceil = 7, \lceil 8.3 \rceil = 9$.

$\lfloor x \rfloor$: the bottom function, which is the maximum integer less than or equal to *x*. E.g.:

$\lfloor 7 \rfloor = 7, \lfloor 8.3 \rfloor = 8$.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

5.4.3 Key derivation functions

The role of key derivation functions is to derive key data from a shared secret bit string. During the process of key agreement, the key derivation function acts on the shared secret bit string obtained from the key exchange to generate the session key required or the key data required for further encryption.

The key derivation function needs to call the cryptographic hash function.

Let the cryptographic hash function be H_v (), whose output length is exactly a hash value of v bits.

The key derivation function *KDF* (*Z,* klen):

Input: the bit string *Z*, integer *klen* (indicating the bit length of key data to be obtained, where the values is required to be less than $(2^{32} - 1)v$).

Output: the key data bit string *K* with the length of *klen*.

a) initialize a counter of 32 bits $ct = 0\mathbf{x}00000001$;

b) perform for *i* from 1 to $\lceil klen/v \rceil$:

b.1) compute $Ha_i = H_v(Z \| ct)$;

b.2) $ct++$;

c) if *klen/v* is an integer, let $Ha!_{\lceil klen/v \rceil} = Ha_{\lceil klen/v \rceil}$,

Or else, let $Ha!_{\lceil klen/v \rceil}$ be the left-most $(klen - (v \times \lfloor klen/v \rfloor))$ bit of $Ha_{\lceil klen/v \rceil}$;

d) let $K = Ha_1 \| Ha_2 \| \cdots \| Ha_{\lceil klen/v \rceil - 1} \| Ha!_{\lceil klen/v \rceil}$.

5.4.4 Random number generator

This Part specifies the use of the random number generator approved by the State Cryptography Administration.

5.5 Users' other information

User A has the distinguishing identifier ID_A with the length of $entlen_A$ bits, notating $ENTL_A$ as two bytes converted from the integer $entlen_A$; and user B has the distinguishing identifier ID_B with the length of $entlen_B$, notating $ENTL_B$ as two bytes converted from the integer $entlen_B$. In the elliptic curve key exchange protocol specified in this Part, both sides A and B in the key agreement need to use the cryptographic hash functions to obtain the hash value Z_A of user A and the hash value Z_B of user B.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

B6: compute the elliptic curve point $V=[h\cdot t_B](P_A+[\bar{x}_1]R_A)=(x_V,y_V)$. If V is a point at infinity, then B agreement fails. Or else, convert the data type of x_V and y_V into a bit string according to the methods given in 4.2.6 and 4.2.5 of GM/T 0003.1-2012;

B7: compute $K_B=KDF(x_V\|y_V\|Z_A\|Z_B,klen)$;

B8: (optional) convert the data types of the coordinates of R_A, x_1 and y_1, and the coordinates of R_B, x_2 and y_2, into a bit string according to the methods given in 4.2.6 and 4.2.5 of GM/T 0003.1-2012, and compute $S_B=Hash(0x02\|y_V\|Hash(x_V\|Z_A\|Z_B\|x_1\|y_1\|x_2\|y_2))$;

B_9: send R_B (and S_B, optional) to user A;

User A:

A4: take field element x_1 from R_A, convert the data type of x_1 into an integer according to the method given in 4.2.8 of GM/T 0003.1-2012, and compute $\bar{x}_1=2^w+(x_1\&(2^w-1))$;

A5: compute $t_A=(d_A+\bar{x}_1\cdot r_A)\mod n$;

A6: verify whether R_B satisfies the elliptic curve equation. If it does not satisfy, then the agreement fails. Or else, take field element x_2 from R_B, convert the data type of x_2 into an integer according to the method given in 4.2.8 of GM/T 0003.1-2012, and compute $\bar{x}_2=2^w+(x_2\&(2^w-1))$;

A7: compute the elliptic curve point $U=[h\cdot t_A](P_B+[\bar{x}_2]R_B)=(x_U,y_U)$. If U is a point at infinity, then A agreement fails. Or else, convert the data type of x_U and y_U into a bit string according to the methods given in 4.2.6 and 4.2.5 of GM/T 0003.1-2012;

A_8: compute $K_A=KDF(x_U\|y_U\|Z_A\|Z_B,klen)$;

A9: (optional) convert the data types of the coordinates of R_A, x_1 and y_1, and the coordinates of R_B, x_2 and y_2, into a bit string according to the methods given in 4.2.6 and 4.2.5 of GM/T 0003.1-2012, compute $S_1=Hash(0x02\|y_U\|Hash(x_U\|Z_A\|Z_B\|x_1\|y_1\|x_2\|y_2))$, and check whether $S_1=S_B$ is true. If it is not true, then the key from B to A is confirmed a failure;

A10: (optional) compute $S_A=Hash(0x03\|y_U\|Hash(x_U\|Z_A\|Z_B\|x_1\|y_1\|x_2\|y_2))$, and send S_A to user B.

User B:

B10: (optional) compute $S_2=Hash(0x03\|y_V\|Hash(x_V\|Z_A\|Z_B\|x_1\|y_1\|x_2\|y_2))$, and check whether $S_2=S_A$ is true. If it is not true, then the key from A to B is confirmed a failure.

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

Full-copy PDF can be purchased from 1 of 2 websites:

1. https://www.ChineseStandard.us

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. https://www.ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - https://www.ChineseStandard.us).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

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