GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 38.040

CCS L 80

GM/T 0080-2020

SM9 Cryptographic Algorithm Application Specification

SM9 密码算法使用规范

Issued on: December 28, 2020 **Implemented on: July 01, 2021**

Issued by: State Cryptography Administration

Table of Contents

SM9 Cryptographic Algorithm Application Specification

1 Scope

This Document defines the application method of SM9 cryptographic algorithm, as well as data formats such as keys, encryption, and signatures, etc.

This Document is applicable to the application of SM9 cryptographic algorithm, and the development and testing of equipment and systems that support SM9 cryptographic algorithm.

2 Normative References

The following documents are essential to the application of this Document. For the dated documents, only the versions with the dates indicated are applicable to this Document; for the undated documents, only the latest version (including all the amendments) is applicable to this Document.

GB/T 32905 Information Security Technology - SM3 Cryptographic Hash Algorithm

GB/T 32907 Information Security Techno1ogy - SM4 Block Cipher Algorithm

GB/T 32918 (all parts) Information Security Technology - Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves

GB/T 38635.1-2020 Information Security Technology - Identity-Based Cryptographic Algorithms SM9 - Part 1: General

GB/T 38635.2-2020 Information Security Technology - Identity-Based Cryptographic Algorithms SM9 - Part 2: Algorithm

3 Terms and Definitions

For the purpose of this Document, the following terms and definitions apply.

3.1 Algorithm identifier

Digitized information that is used to indicate algorithmic mechanisms.

3.2 SM9 algorithm

PPS: Public Parameter Service.

5 SM9 Key Pair

5.1 Generator

The Generator P_1 point on G_1 is marked as (x_{p1}, y_{P1}); and the ASN.1 of the data format is defined as SM9P1::=BIT STRING; the type is BIT STRING; and its content is:

04 ‖ X_1 ‖ Y_1, where X_1 and Y_1 respectively identify the x component and y component of the point; and each component has a length of 256 bits.

The Generator P_2 point on G_2 is marked as (x_{p2}, y_{P2}); and the ASN.1 of the data format is defined as SM9P2::=BIT STRING; the type is BIT STRING; and its content is:

04 ‖ X_1 ‖ X_2 ‖ Y_1 ‖ Y_2, where X_1, X_2 and Y_1, Y_2 respectively identify the x component and y component of the public key; and each component has a length of 256 bits, or

03 ‖ X_1 ‖ X_2, where X_1 and X_2 respectively identify each x component of the public key; and each component has a length of 256 bits. Select the value whose rightmost bit is 1 in the decompressed Y root value (Y_1 ‖ Y_2). After the restoration, the rightmost bit of the Y root value shall be 1; otherwise, Y_1=base field q - root Y_1, Y_2=base field q - root Y_2. or

02 ‖ X_1 ‖ X_2, where X_1 and X_2 respectively identify the 2 x components of the public key; and each component has a length of 256 bits. Select the option value whose rightmost bit is 0 in the decompressed Y root value (Y_1 ‖ Y_2). After the restoration, the Y root value takes the option value whose rightmost bit is 0, otherwise Y_1=base field q - root Y_1, Y_2=base field q - root Y_2.

5.2 SM9 master private key

It includes the SM9 signature master private key and the encryption master private key; both are an integer greater than or equal to 1 and less than N-1 (N is the order of the cyclic group G_1, G_2, and G_T, and its value is shown in Appendix A.1 of GB/T 38635.2-2020), abbreviated as s, with the length of 256 bits.

5.3 SM9 master public key

It includes SM9 signature master public key $Ppub_2$ and encryption master public key $Ppub_1$. They are points on G_2 and G_1; and the coordinates are expressed as (x_{SPub}, y_{SPub}) and (x_{EPub}, y_{EPub}). Thereof, the x and y coordinates of the signature master public key also contain two components, namely x_1 component and x_2 component, y_1 component and y_2 component, and the length of each component is 256 bits. The length of the x and y coordinates of the encryption master public key are both 256 bits.

5.4 SM9 user private key

It includes SM9 user signature private key and user encryption private key, which are points on G_1 and G_2 respectively; and the coordinates are expressed as (x_{SPri}, y_{SPri}) and (x_{EPri}, y_{EPri}). The length of the x and y coordinates of the user signature key are both 256 bits. The x and y coordinates of the user's encryption private key also contain two components, namely x_1 component and x_2 component, y_1 component and y_2 component, and the length of each component is 256 bits.

5.5 SM9 user public key

In IBC technology, the user identification ID can uniquely determine the user's public key, which represents the public key in applications. The representation of ID coordinates based on bilinear pairing can be divided into user signature public key coordinates and user encryption public key coordinates. The user signature public key and the signature master public key are of the same coordinate structure; and there are two respective components on the x and y coordinates, which are marked as Q_S; and user encryption public key and the encryption master public key are of the same coordinate structure, which is marked as Q_E.

NOTE: Here is how to generate the user's public key coordinates.

Input: Algorithm function *H*, *userID*, *hid*, master public key $Ppub_i$, generator P_i i=1,2.

Output: User public key Q_A.

Calculation method:

$Q_{AS}=[H_1(ID_A \| hid, N)]P_2+Ppub_2=(X_{QA2}, Y_{QA2})$, signature public key coordinates are used for signature/verification of signature.

$Q_{AE}=[H_1(ID_A \| hid, N)]P_1+Ppub_1=(X_{QA1}, Y_{QA1})$, encryption public key coordinates are used for key encapsulation, encryption/decryption.

6 Data Format

6.1 Key data structure

The key is divided into signature/encryption master key, and signature/encryption user key:

a) The ASN.1 of data format of SM9 algorithm signature master private key is defined as:

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

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