GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L80
File No.: 49742-2015

GM/T0043-2015

Test specification for digital certificate interoperability

数字证书互操作检测规范

Issued on: April 1, 2015 **Implemented on: April 1, 2015**

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 Cryptography Industry Standardization Technical Committee.

Main drafting organizations of this Standard: Commercial Cryptography Testing Center of State Cryptography Administration, Zhongjin Financial Certification Center Co., Ltd., Aspire Digital Technology (Shenzhen) Co., Ltd., Beijing Certificate Authority, Changchun Jida Zhengyuan Information Technology Co., Ltd., Shanghai Koal Software Co., Ltd., GFA E-commerce Security Ca Co., Ltd.

Main drafters of this Standard: Li Dawei, Zhao Yu, Li Zhiwei, Luo Gansheng, XueYingjun, Deng Kaiyong, Zhou Bi, Tian Minqiu, Li Dong, Xiao Qiulin, Han Yaning, Tan Wuzheng, Li Lixian, Huo Yun, Shang Jin, Zhao Lili, Chang Yuming.

Test specification for digital certificate interoperability

1 Scope

This standard stipulates test content and test method of digital certificate interoperability based on the requirements of GM/T 0015 and GM/T 0034.

This standard applies to the test of digital certificate issued by certificate authentication system.

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.

GB/T 16264.8-2005 Information technology - Open systems interconnection - The directory - Part 8: Public-key and attribute certificate frameworks

GM/T 0006 Cryptographic application Identifier specification

GM/T 0009 SM2 cryptographic algorithm usage specification

GM/T 0015 Digital certificate format specification based on SM2 cryptographic algorithm

GM/T 0016 Smart key cipher application interface specification

GM/T 0034 Certificate authentication system cipher and related security technical specification based on SM2 cryptographic algorithm

GM/Z 4001 Cryptography terminologies

PKCS #10 (v1.7) Certification Request Syntax Standard

3 Terms and definitions

The terms defined in GM/Z 4001 and the following terms and definitions apply to this document.

3.1

6.2.2 Digital certificate extension-item compliance test

The extension-item of user certificate which is issued by CA system shall comply with the requirements of GM/T 0015 and GB/T 16264.8 2005, including:

a) The key identifier extension-item of issuing authority must exist in user certificate, and the value shall be the same as the value in the user key identifier of issuer certificate;

b) The user key identifier extension-item must exist in user certificate, and this value shall be consistent with the calculation result of user public-key in the certificate;

c) The key usage extension-item must exist in user certificate. In which, in the key usage of user signature certificate, the two items of digital signature “digitalSignature” and non-repudiation “nonRepudiation” shall be identified and shall only be identified; in the key usage of user encryption certificate, the three items of key encryption “keyEncipherment”, data encryption “dataEncipherment” and key agreement “keyAgreement” shall be identified and shall only be identified;

d) If there exists extended key usage extension-item in user certificate, it needs to test and verify that the use of the extended key usage cannot conflict with the definition of the key usage extension;

e) If there exists private-key usage-period extension-item in user certificate, the usage-period shall not be greater than the validity-period of certificate;

f) If there exists certificate policy extension-item in user certificate, Internet content can be accessed through the URL stored in the extension-item;

g) The CRL publishing point extension-item must exist in user certificate. According to URL in the CRL publishing point extension-item, it shall be available to download the corresponding CRL file; the CRL shall conform to X.509 V2 standard and the issuer shall be consistent with the issuer of user certificate; moreover, the signature-value in the CRL shall be able to use the issuer certificate of user certificate for verification;

h) If there exists institution information extension-item in user certificate, the issuer certificate of user certificate may be obtained through this extension-item;

i) If there exist other optional extension-items in user certificate, its use shall comply with the requirements of GM/T 0015.

6.2.3 CRL format compliance test

Both signature certificate and encryption certificate need to have a trust-chain establishing test.

6.3.2 Signature certificate interoperability test

When the smart key issued by CA system uses the public-private key-pairs of signature certificate to perform signature verification operation, the called cipher application interface shall meet the requirements of GM/T 0016; the smart key shall complete signature verification interoperability test through calling this interface. These include:

a) SM2 key data format shall meet the requirements of GM/T 0009;

b) SM2 signature data format shall meet the requirements of GM/T 0009;

c) When use SM2 private key to sign input data, the input data is the pre-processed result of the data to be signed through SM2 signature; the signature process shall comply with the requirements of GM/T 0009;

d) When use SM2 public key to verify input data, the input data is the pre-processed result of the data to be signed through SM2 signature; the verification process shall comply with the requirements of GM/T 0009.

6.3.3 Encryption certificate interoperability test

When the smart key issued by CA system uses the public-private key-pairs of encryption certificate to perform encryption-decryption operation, the called cipher application interface shall meet the requirements of GM/T 0016; the smart key shall complete encryption-decryption interoperability test through calling this interface. These include:

a) SM2 key data format shall meet the requirements of GM/T 0009;

b) SM2 encrypted data format shall meet the requirements of GM/T 0009;

c) The key-pair protection data format shall meet the requirements of GM/T 0009;

d) When use SM2 public key to encrypt input data, the encryption process shall comply with the requirements of GM/T 0009;

e) When use SM2 private key to decrypt input data, the decryption process shall comply with the requirements of GM/T 0009.

According to the CRL address in user certificate, download CRL document, and then perform CRL format compliance test. The test result shall meet the requirements of 6.2.3.

7.3 Digital certificate Interoperability test

7.3.1 Certificate trust-chain establishing test

According to the certificate downloading method provided by CA system, download root certificate and second-level CA certificate; read user certificate in the smart key; and then perform certificate trust-chain establishing test. The test result shall meet the requirements of 6.3.1.

7.3.2 Signature certificate Interoperability test

By establishing two users, bind user signature certificates ScertA and ScertB, respectively.

User A uses the private key corresponding to certificate ScertA to sign a piece of data, and then sends the signed data to user B; user B uses the public key of the certificate ScertA to perform signature verification on the data, and the verification shall be able to succeed. The certificate status and the certificate trust-chain of both communication sides shall be verified and passed during the verification process, and the test results shall meet the requirements of 6.3.2.

User B uses the private key corresponding to certificate ScertB to sign a piece of data, and then sends the signed data to user A; user A uses the public key of the certificate ScertB to perform signature verification on the data, and the verification shall be able to succeed. The certificate status and the certificate trust-chain of both communication sides shall be verified and passed during the verification process, and the test results shall meet the requirements of 6.3.2.

7.3.3 Encryption certificate interoperability test

By establishing two users A and B, bind user encryption certificates EcertA and EcertB, respectively.

User A first generates session key, and uses the key to encrypt a piece of data, and then uses the public key corresponding to the certificate EcertB to encrypt the session key, and finally sends the cipher-text data to user B. After receiving the cipher-text data, user B first uses the private key of certificate EcertB to decrypt the session key, and then uses the session key to decrypt the cipher-text data, and the decryption shall be able to succeed. The certificate status and the certificate trust-chain of both communication sides shall be verified and passed during the encryption-decryption process, and the test results shall meet the requirements of 6.3.3.

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

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