CFCA

中 国 金 融 认 证 中 心 标 准

30007.01—2013

SM2 双证书申请及下载规范

SM2 double-certificate enrollment specification

2013-06-01 发布　　2013-06-01 实施

中国金融认证中心　　发布

目　　录

1. 范围 1

2. 规范性引用文件 1

3. 术语和定义 1

4. SM2 双证书下载流程 2

5. SM2 双证书请求格式 2

5.1 签名公钥信息 3

5.2 属性信息 3

6. 加密后的加密证书私钥 4

7. 通信报文 4

7.1 客户端请求报文 4

7.2 服务器响应报文 5

8. 证书导入 5

附录 7

SM2 双证书请求示例 7

SM2 双证书申请及下载规范

1. 范围

本规范中，描述了 CFCA SM2 双证书申请及下载流程，并对 CFCA SM2 双证书申请及下载流程中所涉及的数据结构进行了说明。

本文档仅针对 CFCA SM2 双证书请求中的关键节点进行介绍，未涉及部分请参考 PKCS#10 规范。

2. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件，凡是不注日期的引用文件，其最新版本适用于本文件。

RFC 2986	PKCS #10: Certification Request Syntax Specification
GM/T 0002-2012	SM4 分组密码算法
GM/T 0003-2012	SM2 椭圆曲线公钥密码算法
GM/T 0004-2012	SM3 密码杂凑算法
GM/T 0009-2012	SM2 密码算法使用规范
GM/T 0010-2012	SM2 密码算法加密签名消息语法规范

3. 术语和定义

数字证书

也称公钥证书，由证书认证机构(CA)签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按用途可分为签名证书、加密证书。

公钥

非对称密码算法中可以公开的密钥。

私钥

非对称密码算法中，只能由拥有者使用的不公开密钥。

SM2 密码算法

一种椭圆曲线密码算法，密钥长度为 256 比特。

交互密钥

在本规范中，交互密钥特指由申请者产生的非对称密钥对，用于保护加密证书私钥。

4. SM2 双证书下载流程

CFCA SM2 双证书下载步骤如下：

1) 产生签名密钥对和交互密钥对。

2) 生成 Base64 编码的 SM2 双证书请求。

3) 向服务器端提交 SM2 双证书请求。

4) 解析服务器端返回的报文数据，并解密加密证书私钥。

5) 导入签名公钥证书、加密公钥证书、加密证书私钥。

5. SM2 双证书请求格式

SM2 双证书请求的 ASN.1 数据格式：

```
CertificationRequest ::= SEQUENCE {
    certificationRequestInfo    CertificationRequestInfo,
    signatureAlgorithm          AlgorithmIdentifier{{ SignatureAlgorithms }},
    signature                   BIT STRING
}
```

其中：

certificationRequestInfo： SM2 双证书请求信息。

signatureAlgorithm：签名算法 ID，本文档中，取值为：1.2.156.10197.1.501。

signature：使用签名私钥，对 certificationRequestInfo 节点的签名结果，封装格式参见《GM/T 0009-2012 SM2 密码算法使用规范》。

SM2 双证书请求信息的 ASN.1 数据格式：

```
CertificationRequestInfo ::= SEQUENCE {
    version             INTEGER,
    subject             Name,
    subjectPKInfo       SubjectPublicKeyInfo,
    attributes          [0] Attributes
}
```

其中：

version：版本号，本文档中取值为 0x00。

subject：公钥证书 DN。详细介绍，请参考 PKCS#10。

subjectPKInfo：签名公钥信息。详细介绍，请见 5.1 小节。

attributes：属性信息。详细介绍，请见 5.2 小节。

5.1 签名公钥信息

签名公钥信息的 ASN.1 数据结构如下：

```
SubjectPublicKeyInfo    ::= SEQUENCE {
      algorithm                AlgorithmIdentifer,
      subjectPublicKey         BIT STRING
 }
AlgorithmIdentifer::= SEQUENCE {
      algorithm       OBJECT IDENTIFIER,
      parameters      ANY DEFINED BY algorithm OPTIONAL
 }
```

其中：

algorithm：ECC 公钥算法 OID，在本文档中，取值为：1.2.840.10045.2.1。

parameters：SM2 公钥算法 OID，在本文档中，取值为：1.2.156.10197.1.301。

subjectPublicKey：SM2 公钥数据：0x04||签名公钥 X 分量||签名公钥 Y 分量。

5.2 属性信息

属性信息的 ASN.1 数据结构如下：

```
Attributes ::= Context[0] {
      chanllegPassword       ChanllegPassword,
      tempPublicKeyInfo      TempPulicKeyInfo
}
ChanllegPassword ::= SEQUENCE {
      chanllegPasswordOID    OBJECTIDENTIFIER,
      password               PrintableString
}
TempPulicKeyInfo ::= SEQUENCE {
      tempPublicKeyOID       OBJECTIDENTIFIER,
      tempPublicKey          OCTECT STRING
}
```

其中：

password：默认取值：111111。

tempPublicKeyOID：交互公钥标识 OID，本文档中取值为：1.2.840.113549.1.9.63。

tempPublicKey：交互公钥 TempPulicKey 的 OCTECT STRING 编码。

5.2.1 交互公钥

交互公钥的 ASN.1 数据结构如下：

```
TempPulicKey ::= SEQUENCE {
    version                 INTEGER,
    tempPublicKeyData       OCTET STRING
}
```

其中：

version：版本号，本文档中取值为：0x01。

tempPublicKeyData：交互公钥数据，结构如下：

0x00 0xB4 0x00 0x00||0x00 0x01 0x00 0x00 ||交互公钥 X 分量||32 字节 0x00 扩展空间||交互公钥 Y 分量||32 字节 0x00 扩展空间。

6. 加密后的加密证书私钥

加密后的加密证书私钥 ASN.1 数据结构如下：

```
EncryptedPrivateKey ::= SEQUENCE {
    version                     INTEGER,
    encryptedPrivateKeyData     OCTET STRING
}
```

其中：

version：版本号，本文档中取值为：0x01。

encryptedPrivateKeyData：加密后的加密证书密钥对数据。其密文格式为：C1||C3||C2。

解密后的明文格式为：加密公钥 X 分量（32 字节）||

加密公钥 Y 分量（32 字节）||加密私钥（32 字节）。

7. 通信报文

7.1 客户端请求报文

客户端向服务器端提交的证书请求报文中，应包含证书下载两码、双证书请求。

URL 访问格式如下：

http://ip:port/cgi-bin/service.do?**businessType**=**certDown**&**sn**=xxxx&**authCode**=xxxx&**p10**=xxxx

实际应用中需注意：

1) 服务器地址在证书申请前，需与 CFCA 确认。

2) sn、authCode、p10 处应填充实际的参考号、授权码、证书请求。

3) p10 申请中出现的“+”必须用“%2B”替换，“=”必须用“%3D”替换。

7.2 服务器响应报文

服务器返回的请求响应报文结构如下(String 类型，共六项用“||”分隔)：

errorCode||errorMessage||businessType||signCert||encCert||encPriKey

其中：

errorCode：错误码。0 表示成功，其他值表示失败。

errorMessage：错误信息，用于描述 erroCode 对应的错误信息。当 erroCode 为 0 时，此项为 0。

businessType：业务类型。

signCert：签名公钥证书。erroCode 非 0 时，此项为 0。

encCert：加密公钥证书。erroCode 非 0 时，此项为 0。

encPriKey：加密后的加密证书私钥。erroCode 非 0 时，此项为 0。

8. 证书导入

从服务器端成功接收到响应报文，解析后得到：签名公钥证书、加密公钥证书、加密后的加密证书私钥。其中签名公钥证书、加密公钥证书，都是 Base64 编码的公钥证书数据，且每隔 64 个字符用“,”分隔。

为保证加密证书私钥的安全性，在传输过程采用交互公钥对其加密。以下将通过一个示例，来说明解密加密证书私钥的步骤。

从服务器端获取到的加密后的加密证书私钥数据为：

0000000000000001000000000000000100000000000000000000000000000000000000000000000273MIHGA
gECBIHA03F96Luqbu8LnxnEwtqPiEe/QfUhTemY4PDVwm8oB9K60aZdngeP,FLd2y50fjoxAqsV6FpKEVOTmz
WjLeU9oPVfaq8sNwCILjmLMdJWgEgusaX/vNanK,gXxd7TcqPFNfmIweGmwV4X/QoBhIO5Z08ZYIWkVhKTgoE
y2bMjMSRt93L7tgMdG/,h3VwGm8DSV/rzNUsUXab0ZIVGWSen1Z9PxMo2elCfVR1QfMi4mL6NQ3/qkuWBSFz,
3kShWZ7clFWY,

该数据可拆分成如下格式：

0000000000000001

0000000000000001

0000000000000000

0000000000000000

0000000000000273

MIHGAgECBIHA03F96Luqbu8LnxnEwtqPiEe/QfUhTemY4PDVwm8oB9K60aZdngeP,FLd2y5Ofjox……

跳过前 64 字节，0000000000000273 表示密文长度（含“,”）。本例中的密文长度为：273。

加密证书私钥数据解析流程如下：

1） 去掉密文中的“,”后进行 Base64 解码。

2） 再进行 ASN.1 解码（ASN.1 结构请参见章节 6），即可取得“加密后的加密证书密钥对数据”。

3） 对“加密后的加密证书密钥对数据”解密即可得到加密证书密钥对明文。

附录

SM2 双证书请求示例

MIIBOTCCAXUCAQAwWzENMAsGA1UEBh4EAEMATjEhMB8GA1UECh4YAEMARgBDAEEAIABUAEUAUwBU
ACAAQwBBMScwJQYDVQQDHh4AYwBlAHIAdABSAGUAcQB1AGkAcwBpAHQAaQBvAG4wWTATBgcqhkjO
PQIBBggqgRzPVQGCLQNCAAQv93JF1oROzBImU6Plgleu+HI659cECfKn+gajy7JWGAEoSyw+9rsB
WoRA+kqA7FmgO8NcNcm3fRBWS+yLBMLUoIG3MBMGCSqGSIb3DQEJBxMGMTExMTExMIGfBgkqhkiG
9w0BCT8EgZEwgY4CAQEEgYgAtAAAAAEAAGmQSyS20/zQ4tHJQKA5EYPgdLuPE568SYcKlqmwWGjW
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAACokwM02BfEmqVM+qPPlx2I4v38pc1N4WgC
xVb2QmgSygAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMAwGCCqBHM9VAYN1BQADSAAw
RQIgfm4txwd5pHMPPtsHEfN+4Y8iMKmKCxy1T3eIMwkYS0kCIQCu6nbbBxVF99qaX1h1/qksk9u9
fs6qkzlkrFbkPkvMjw==