ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25060—2010

信息安全技术　公钥基础设施 X.509数字证书应用接口规范

Information security techniques—Public Key Infrastructure—Interface specification of X.509 digital certificates application

2010-09-02 发布　　2011-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准凡涉及密码算法相关内容，按国家有关法规实施。

本标准的附录A为规范性附录。

本标准由全国信息安全标准化技术委员会(TC 260)提出并归口。

本标准起草单位：长春吉大正元信息技术股份有限公司。

本标准主要起草人：李伟平、何长龙、刘勇、付敏。

引　言

基于PKI技术体系的电子签名和电子认证为电子政务和电子商务的开展提供了技术支持，特别是《中华人民共和国电子签名法》的颁布为基于电子签名的应用提供了法律依据。但是，由于各厂商对数字证书应用需求理解的差异性及实践经验不足，数字证书应用API实现存在很大的随意性，以及相关标准规范的缺乏，导致各厂家同类产品间差别大，给基于数字证书应用、应用系统集成和数字证书管理及推广带来极大困难。

对基于数字证书应用需求进行研究、总结，统一规划、编制基于PKI技术体系的数字证书应用接口规范，有利于数字证书应用产品提供商缩短产品研发周期，减少研发和支持成本；有利于应用开发商和服务商摆脱特定CA提供的接口而在规范的数字证书应用接口上进行数字证书应用的开发，减少针对开发的设计、实现和测试，使其能够专注于应用产品功能；有利于降低数字证书应用的复杂度，并便于用户对数字证书的使用。

本标准基于《公钥密码基础设施应用技术体系　通用密码服务接口规范》，进行了适当剪裁，针对数字证书应用进行了规范，可用于指导数字证书认证系统中数字证书应用产品的研制和开发。

本标准在编写过程中得到了商用密码基础设施专项工作组的指导。

信息安全技术　公钥基础设施
X.509数字证书应用接口规范

1　范围

本标准定义了数字证书应用标识及一组证书应用接口。

本标准适用于基于数字证书的安全中间件的设计和实现，对基于数字证书的安全功能的研制、开发、测试亦可参照使用。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 20518—2006　信息安全技术　公钥基础设施　数字证书格式

PKCS#7 V1.5:加密消息语法标准

3　术语和定义

下列术语和定义适用于本标准。

3.1

数字证书　digital certificate

由认证权威数字签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

3.2

证书撤销列表　certificate revocation list

标记一系列不再被证书发布者所信任的证书的签名列表。

3.3

数字信封　digital envelope

附加到消息中的数据，它允许消息的预期接收方验证该消息内容的完整性。

4　缩略语

下列缩略语适用于本标准。

CA	证书认证机构	(Certificate Authority)
CRL	证书撤销列表	(Certificate Revocation List)
DER	可区分编码规则	(Distinguished Encoding Rules)
PKCS#1	RSA加密标准	(RSA Cryptography Standard)
PKCS#7	加密消息的语法标准	(Cryptographic Message Syntax Standard)
PKI	公钥基础设施	(Public Key Infrastructure)
OID	对象标识符	(Object Identifier)

5 标识定义

5.1 常量定义

宏 描 述	预定义值	说 明
# define SGDX_TRUE	0x00000001	布尔值为真
# define SGDX_FALSE	0x00000000	布尔值为假

5.2 密码算法标识

5.2.1 对称算法标识

宏 描 述	预定义值	说 明
# define SGDX_SM1_ECB	0x00000101	SM1 算法 ECB 加密模式
# define SGDX_SM1_CBC	0x00000102	SM1 算法 CBC 加密模式
# define SGDX_SM1_CFB	0x00000104	SM1 算法 CFB 加密模式
# define SGDX_SM1_OFB	0x00000108	SM1 算法 OFB 加密模式
# define SGDX_SM1_MAC	0x00000110	SM1 算法 MAC 加密模式
# define SGDX_SSF33_ECB	0x00000201	SSF33 算法 ECB 加密模式
# define SGDX_SSF33_CBC	0x00000202	SSF33 算法 CBC 加密模式
# define SGDX_SSF33_CFB	0x00000204	SSF33 算法 CFB 加密模式
# define SGDX_SSF33_OFB	0x00000208	SSF33 算法 OFB 加密模式
# define SGDX_SSF33_MAC	0x00000210	SSF33 算法 MAC 加密模式

5.2.2 非对称算法标识

宏 描 述	预定义值	说 明
# define SGDX_RSA	0x00010000	RSA 算法

5.2.3 杂凑算法标识

宏 描 述	预定义值	说 明
# define SGDX_SHA1	0x00000002	SHA1 杂凑算法
# define SGDX_SHA256	0x00000004	SHA256 杂凑算法

5.3 证书项标识

5.3.1 基本证书域标识

宏 描 述	预定义值	说 明
# DEFINE SGDX_CERT_VERSION	0x00000001	版本
# DEFINE SGDX_CERT_SERIALNUMBER	0x00000002	序列号
# DEFINE SGDX_CERT_SIGNATURE	0x00000003	签名算法
# DEFINE SGDX_CERT_ISSUER	0x00000004	颁发者
# DEFINE SGDX_CERT_VALIDITY	0x00000005	有效期
# DEFINE SGDX_CERT_SUBJECT	0x00000006	主体
# DEFINE SGDX_CERT_SUBJECTPUBLICKEYINFO	0x00000007	证书公钥信息
# DEFINE SGDX_CERT_ISSUERUNIQUEID	0x00000009	颁发者唯一标识符
# DEFINE SGDX_CERT_SUBJECTUNIQUEID	0x00000010	主体唯一标识符
# define SGDX_CERT_EXTENSIONS	0x00000011	扩展项

5.3.2 标准的扩展域标识

宏 描 述	预定义值	说 明
# define SGDX_EXT_SUBJECTPUBLICKEYINFO	0x00000012	机构密钥标识符
# define SGDX_EXT_SUBJECTPUBLICKEYINFO	0x00000013	主体密钥标识符
# define SGDX_EXT_KEYUSAGE	0x00000014	密钥用法
# define SGDX_EXT_PRIVATEKEYUSAGEPERIOD	0x00000015	私有密钥使用期
# define SGDX_EXT_CERTIFICATEPOLICIES	0x00000016	证书策略
# define SGDX_EXT_POLICYMAPPINGS	0x00000017	策略映射
# define SGDX_EXT_BASICCONSTRAINTS	0x00000018	基本限制
# define SGDX_EXT_POLICYCONSTRAINTS	0x00000019	策略限制
# define SGDX_EXT_EXTKEYUSAGE	0x00000020	扩展密钥用途
# define SGDX_EXT_CRLDISTRIBUTIONPOINTS	0x00000021	CRL 分发点
# define SGDX_EXT_AUTHORITYKEYIDENTIFIER	0x00000022	机构密钥标识符
# define SGDX_EXT_SUBJECTKEYIDENTIFIER	0x00000023	主体密钥标识符
# define SGDX_EXT_SUBJECTALTNAME	0x00000024	主体替换名称
# define SGDX_EXT_ISSUERALTNAME	0x00000025	颁发者替换名称
# define SGDX_EXT_SUBJECTDIRECTORYATTRIBUTES	0x00000026	主体目录属性
# define SGDX_EXT_NAMECONSTRAINTS	0x00000027	名称限制
# define SGDX_EXT_POLICYCONSTRAINTS	0x00000028	策略限制
# define SGDX_EXT_INHIBITANYPOLICY	0x00000029	限制所有策略
# define SGDX_EXT_FRESHESTCRL	0x00000030	最新的 CRL
# define SGDX_EXT_AUTHORITYINFOACCESS	0x00000031	机构信息访问
# define SGDX_EXT_SUBJECTINFORMATIONACCESS	0x00000032	主体信息访问
# define SGDX_EXT_IDENTIFYCARDNUMBER	0x00000033	个人身份标识号码
# define SGDX_EXT_INURANCENUMBER	0x00000034	个人社会保险号
# define SGDX_EXT_ICREGISTRATIONNUMBER	0x00000035	企业工商注册号
# define SGDX_EXT_ORGANIZATIONCODE	0x00000036	企业组织机构代码
# define SGDX_EXT_TAXATIONNUMBER	0x00000037	企业税号
# define SGDX_EXT_ID_PKIX	0x00000038	私有的 Internet 扩展
# define SGDX_EXT_NETSCAPECERTTYPE	0x00000039	netscape 属性

6 接口描述

6.1 概述

本标准定义了符合 GB/T 20518—2006 的数字证书应用的环境函数、证书函数、密码运算函数和消息函数等，这些函数能够完成取证书信息，验证证书有效性，制作、验证数字签名，制作、解析数字信封等常用数字证书应用，以及一些辅助性功能函数，如 Base64 的编码、解码、数据摘要计算等。

本条以表格的形式列出了这些函数接口的功能及名称，如表 1、表 2、表 3、表 4、表 5 分别给出环境

函数、证书函数、密码运算函数、消息函数和辅助函数的概述，关于这些函数接口的详细定义请参见本章后面的函数接口定义部分。

表 1 环境函数

序号	接口名称	接口说明
1	SAFX_Initialize	初始化环境
2	SAFX_Finalize	清理环境
3	SAFX_Login	打开密码设备
4	SAFX_Logout	关闭密码设备

表 2 证书函数

序号	接口名称	接口说明
1	SAFX_GetCertificateInfo	取证书基本项信息
2	SAFX_GetExtTypeInfo	取证书扩展项信息
3	SAFX_VerifyCertificateSign	验证证书签名
4	SAFX_VerifyCertificateValidity	验证证书有效期
5	SAFX_VerifyCertificateByCrl	根据 CRL 验证证书是否被撤销

表 3 密码运算函数

序号	接口名称	接口说明
1	SAFX_RsaSign	RSA 签名运算
2	SAFX_RsaVerifySign	RSA 验证签名运算
3	SAFX_RsaPublicKeyEncByCert	RSA 公钥加密运算
4	SAFX_Pkcs1RsaPrivateKeyDec	RSA 私钥解密运算
5	SAFX_Hash	计算数据摘要

表 4 消息函数

序号	接口名称	接口说明
1	SAFX_Pkcs7_EncodeSignedData	编码 PKCS7 格式的签名数
2	SAFX_Pkcs7_DecodeSignedData	解码 PKCS7 格式的签名数据
3	SAFX_Pkcs7_EncodeEnvelopedData	编码 PKCS7 格式的数字信封
4	SAFX_Pkcs7_DecodeEnvelopedData	解码 PKCS7 格式的数字信封
5	SAFX_Pkcs7_EncodeSignedAndEnvelopedData	编码 PKCS7 格式的签名数字信封
6	SAFX_Pkcs7_DecodeSignedAndEnvelopedData	解码 PKCS7 格式的签名数字信封
7	SAFX_Pkcs7_EncodeDigestedData	编码 PKCS7 格式的摘要数据
8	SAFX_Pkcs7_DecodeDigestedData	解码 PKCS7 格式的摘要数据
9	SAFX_Pkcs7_EncodeEncryptedData	编码 PKCS7 格式的加密数据
10	SAFX_Pkcs7_DecodeEncryptedData	解码 PKCS7 格式的加密数据

表 5 辅助函数

序号	接口名称	接口说明
1	SAFX_GetVersion	取接口实现的版本号
2	SAFX_GetSpecificationsVersion	取对应标准的版本号
3	SAFX_Base64_Encode	BASE64 编码
4	SAFX_Base64_Decode	BASE64 解码

6.2 环境函数

6.2.1 初始化环境

描述：

初始化数字证书应用程序空间。

原型：

```
int SAFX_Initialize(
                void**    hAppHandle
            )
```

参数：

hAppHandle　　输入参数，应用接口句柄

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.2.2 清理环境

描述：

清理数字证书应用程序空间。

原型：

```
int SAFX_Finalize(
                void*    hAppHandle
            )
```

参数：

hAppHandle　　输入参数，应用接口句柄

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.2.3 打开密码设备

描述：

用户打开密码设备，建立安全令牌。

原型：

```
int SAFX_Login(
                void*           hAppHandle,
                unsigned int    uiUsrType,
                unsigned char*  pucPin,
                unsigned int    uiPinLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
uiUsrType	输入参数，用户类型，0 表示管理员，1 表示普通用户
pucPin	输入参数，设备口令
uiPinLen	输入参数，设备口令长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.2.4 关闭密码设备

描述：

用户关闭密码设备。

原型：

```
int SAFX_Logout(
                void*   hAppHandle
            )
```

参数：

hAppHandle	输入参数，应用接口句柄

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.3 证书函数

6.3.1 取证书基本项信息

描述：

获取证书基本项信息。

原型：

```
int SAFX_GetCertificateInfo(
                void*           hAppHandle,
                unsigned char*  pucCertificate,
                unsigned int    uiCertificateLen,
                unsigned int    uiInfoType,
                unsigned char*  pucInfo,
                unsigned int*   puiInfoLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucCertificate	输入参数，DER 编码的数字证书
uiCertificateLen	输入参数，DER 编码的数字证书长度
uiInfoType	输入参数，证书基本项标识
pucInfo	输出参数，获取的证书基本项信息
puiInfoLen	输出参数，获取的证书基本项信息长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.3.2 取证书扩展项信息

描述：

获取证书扩展项信息。

原型：

```
int SAFX_GetExtTypeInfo(
                void*           hAppHandle,
                unsigned char*  pucDerCertExt,
                unsigned int    uiDerCertExtLen,
                unsigned int    uiInfoType,
                unsigned char*  pucPriOid,
                unsigned int    uiPriOidLen,
                unsigned char*  pucInfo,
                unsigned int*   puiInfoLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucDerCertExt	输入参数，全体扩展项地址
uiDerCertExtLen	输入参数，全体扩展项长度
uiInfoType	输入参数，证书扩展项标识
pucPriOid	输入参数，扩展项的 OID，如果不是私有扩展项类型，该参数为 NULL
uiPriOidLen	输入参数，扩展项的 OID 长度，pucPriOid 无效时，该参数为 NULL
pucInfo	输出参数，获取的证书扩展项信息
puiInfoLen	输出参数，获取的证书扩展项信息长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.3.3 验证证书签名

描述：

使用证书链验证证书是否有效。

原型：

```
int SAFX_VerifyCertificateSign(
                void*           hAppHandle,
                unsigned char*  pucCertificate,
                unsigned int    uiCertificateLen,
                unsigned char*  pucP7bCertificateChain,
                unsigned int    uiP7bCertificateChainLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucCertificate	输入参数，DER 编码的数字证书
uiCertificateLen	输入参数，DER 编码的数字证书长度
pucP7bCertificateChain	输入参数，PKCS#7 签名数据格式含根证书的证书链
uiP7bCertificateChainLen	输入参数，PKCS#7 签名数据格式含根证书的证书链长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.3.4 验证证书有效期

描述：

验证证书在特点的时间点是否有效。

原型：

```
int SAFX_VerifyCertificateValidity(
                    void*           hAppHandle,
                    unsigned char*  pucCertificate,
                    unsigned int    uiCertificateLen,
                    unsigned long   ulTime
                )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucCertificate	输入参数，DER 编码的数字证书
uiCertificateLen	输入参数，DER 编码的数字证书长度
ulTime	输入参数，验证在该时间点证书是有效，如果取 NULL 值，则使用系统当前时间进行验证

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.3.5 根据 CRL 验证证书是否被撤销

描述：

根据 CRL 验证证书是否被撤销。

原型：

```
int SAFX_VerifyCertificateByCrl(
                    void*           hAppHandle,
                    unsigned char*  pucCertificate,
                    unsigned int    uiCertificateLen,
                    unsigned char*  pucDerCrl,
                    unsigned int    uiDerCrlLen
                )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucUsrCertificate	输入参数，DER 编码的证书
uiUsrCertificateLen	输入参数，DER 编码的证书长度
pucDerCrl	输入参数，DER 编码的 CRL
uiDerCrlLen	输入参数，DER 编码的 CRL 长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.4 密码运算函数

6.4.1 RSA 签名运算

描述：

按照 PKCS#1 的要求进行签名运算。

原型：

```
int SAFX_RsaSign(
                void*           hAppHandle,
                unsigned char*  pucKeyPairPin,
                unsigned int    uiKeyPairPinLen,
                unsigned int    uiDigestAlgorithm,
                unsigned char*  pucInData,
                unsigned int    uiInDataLen,
                unsigned char*  pucSignData,
                unsigned int*   puiSignDataLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucKeyPairPin	输入参数，密钥保护密码
uiKeyPairPinLen	输入参数，密钥保护密码长度
uiDigestAlgorithm	输入参数，杂凑算法标识
pucInData	输入参数，输入数据
uiInDataLen	输入参数，输入数据长度
pucSignData	输出参数，DER 编码的签名数据
puiSignDataLen	输出参数，DER 编码的签名数据长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.4.2 RSA 验证签名运算

描述：

验证符合 PKCS1 格式签名数据的运算。

原型：

```
int SAFX_RsaVerifySign(
                void*           hAppHandle,
                unsigned char*  pucCertificate,
                unsigned int    uiCertificateLen,
                unsigned char*  pucSignData,
                unsigned int    puiSignDataLen,
                unsigned char*  pucInData,
                unsigned int    uiInDataLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucCertificate	输入参数，DER 编码的数字证书

uiCertificateLen	输入参数,DER 编码的数字证书长度
pucSignData	输入参数,DER 编码的签名数据
puiSignDataLen	输入参数,DER 编码的签名数据长度
pucInData	输入参数,原始数据
uiInDataLen	输入参数,原始数据长度

返回值:

SARX_OK:成功

其他:失败,详见附录 A。

6.4.3 RSA 公钥加密运算

描述:

按照 PKCS#1 的要求进行基于证书的 RSA 公钥加密运算。

原型:

```
int SAFX_RsaPublicKeyEncByCert(
                    void*           hAppHandle,
                    unsigned char*  pucCertificate,
                    unsigned int    uiCertificateLen,
                    unsigned char*  pucInData,
                    unsigned int    uiInDataLen,
                    unsigned char*  pucOutData,
                    unsigned int*   puiOutDataLen
                )
```

参数:

hAppHandle	输入参数,应用接口句柄
pucCertificate	输入参数,DER 编码的数字证书
uiCertificateLen	输入参数,DER 编码的数字证书长度
pucInData	输入参数,明文数据
uiInDataLen	输入参数,明文数据长度
pucOutData	输出参数,密文数据
puiOutDataLen	输出参数,密文数据长度

返回值:

SARX_OK:成功

其他:失败,详见附录 A。

6.4.4 RSA 私钥解密运算

描述:

按照 PKCS#1 的要求进行 RSA 私钥解密运算。

原型:

```
int SAFX_Pkcs1RsaPrivateKeyDec(
                    void*           hAppHandle,
                    unsigned char*  pucKeyPairPin,
                    unsigned int    uiKeyPairPinLen,
                    unsigned char*  pucInData,
                    unsigned int    uiInDataLen,
```

```
                unsigned char*   pucOutData,
                unsigned int*    puiOutDataLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucKeyPairPin	输入参数，密钥保护密码
uiKeyPairPinLen	输入参数，密钥保护密码长度
pucInData	输入参数，密文数据
uiInDataLen	输入参数，密文数据长度
pucOutData	输出参数，明文数据
puiOutDataLen	输出参数，明文数据长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.4.5 计算数据摘要

描述：

对给定数据计算其摘要。

原型：

```
int SAFX_Hash(
                void*            hAppHandle,
                unsigned int     uiDigestAlgorithm,
                unsigned char*   pucInData,
                unsigned int     uiInDataLen,
                unsigned char*   pucOutData,
                unsigned int*    puiOutDataLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
uiDigestAlgorithm	输入参数，杂凑算法标识
pucInData	输入参数，输入数据
uiInDataLen	输入参数，输入数据长度
pucOutData	输出参数，摘要值
puiOutDataLen	输出参数，摘要值长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.5 消息函数

6.5.1 概述

PKCS#7 V1.5：加密消息标准共定义了 6 种数据类型，分别为：数据(data)，签名数据(signedData)，数字信封(envelopedData)，签名数字信封(signedAndEnvelopedData)，摘要数据(digestedData)和加密数据(encryptedData)。除数据(data)为原始类型不需要密码运算外，其他五个数据类型需要密码运算，本标准定义了与其相对应的编码和解码函数接口，如表 6 所示。

表 6　PKCS#7 数据类型操作函数

PKCS#7 数据类型	功能	函数名称
signedData	编码	SAFX_Pkcs7_EncodeSignedData
	解码	SAFX_Pkcs7_DecodeSignedData
envelopedData	编码	SAFX_Pkcs7_EncodeEnvelopedData
	解码	SAFX_Pkcs7_DecodeEnvelopedData
signedAndEnvelopedData	编码	SAFX_Pkcs7_EncodeSignedAndEnvelopedData
	解码	SAFX_Pkcs7_DecodeSignedAndEnvelopedData
digestedData	编码	SAFX_Pkcs7_EncodeDigestedData
	解码	SAFX_Pkcs7_DecodeDigestedData
encryptedData	编码	SAFX_Pkcs7_EncodeEncryptedData
	解码	SAFX_Pkcs7_DecodeEncryptedData

6.5.2　编码 PKCS7 格式的签名数据

描述：

使用签名密钥对原文数据进行数字签名，并打成 PKCS#7 签名数据格式的数据包。详细参见 PKCS#7 规范的 SignedData 类型定义。

原型：

```
int SAFX_Pkcs7_EncodeSignedData(
                void*           hAppHandle,
                unsigned char*  pucSignerCertificate,
                unsigned int    uiSignerCertificateLen,
                unsigned char*  pucKeyPairPin,
                unsigned int    pucKeyPairPinLen,
                unsigned int    uiDigestAlgorithm,
                unsigned char*  pucData,
                unsigned int    uiDataLen,
                unsigned char*  pucDerP7SignedData,
                unsigned int*   puiDerP7SignedDataLen

                )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucSignerCertificate	输入参数，签名者证书
uiSignerCertificateLen	输入参数，签名者证书长度
pucKeyPairPin	输入参数，密钥保护密码
uiKeyPairPinLen	输入参数，密钥保护密码长度
uiDigestAlgorithm	输入参数，杂凑算法标识
pucData	输入参数，需要签名的数据
uiDataLen	输入参数，需要签名的数据长度
pucDerP7SignedData	输出参数，符合 PKCS#7 标准的签名数据包
puiDerP7SignedDataLen	输出参数，符合 PKCS#7 标准的签名数据包长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.5.3 解码 PKCS7 格式的签名数据

描述：

从 PKCS#7 签名数据格式的数据包中解析出原文、签名者数字证书等。

原型：

```
int SAFX_Pkcs7_DecodeSignedData(
                void*           hAppHandle,
                unsigned char*  pucDerP7SignedData,
                unsigned int    uiDerP7SignedDataLen,
                unsigned char*  pucSignerCertificate,
                unsigned int    uiSignerCertificateLen,
                unsigned int*   puiDigestAlgorithm,
                unsigned char*  pucData,
                unsigned int*   puiDataLen,
                unsigned char*  pucSign,
                unsigned int*   puiSignLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucDerP7SignedData	输入参数，符合 PKCS#7 签名数据格式的数据包
uiDerP7SignedDataLen	输入参数，符合 PKCS#7 签名数据格式的数据包长度
pucSignerCertificate	输出参数，签名者证书
puiSignerCertificateLen	输出参数，签名者证书长度
puiDigestAlgorithm	输出参数，杂凑算法标识
pucData	输出参数，原文数据
puiDataLen	输出参数，原文数据长度
pucSign	输出参数，签名值
puiSignLen	输出参数，签名值长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.5.4 编码 PKCS7 格式的数字信封

描述：

制作符合 PKCS#7 数字信封格式的数据包。被打包的信息包括接收者信息和数据密文等。详细参见 PKCS#7 规范的 EnvelopedData 类型定义。

原型：

```
int SAFX_Pkcs7_EncodeEnvelopedData(
                void*           hAppHandle,
                unsigned char*  pucData,
                unsigned int    uiDataLen,
                unsigned char*  pucEncCertificate,
```

```
                unsigned int      uiEncCertificateLen,
                unsigned int      uiEncAlgorithm,
                unsigned char*    pucDerP7EnvelopedData,
                unsigned int*     puiDerP7EnvelopedDataLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucData	输入参数，需要制作数字信封的数据
puiDataLen	输入参数，需要制作数字信封的数据长度
pucEncCertificate	输入参数，接收者证书
uiEncCertificateLen	输入参数，接收者证书长度
uiEncAlgorithm	输入参数，加密算法标识
pucDerP7EnvelopedData	输出参数，符合 PKCS#7 数字信封格式的数据包
puiDerP7EnvelopedDataLen	输出参数，符合 PKCS#7 数字信封格式的数据包长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.5.5 解码 PKCS7 格式的数字信封

描述：

从符合 PKCS#7 数字信封格式的数据包中解析出原文数据。

原型：

```
int SAFX_Pkcs7_DecodeEnvelopedData(
                void*             hAppHandle,
                unsigned char*    pucDerP7EnvelopedData,
                unsigned int      uiDerP7EnvelopedDataLen,
                unsigned char*    pucData,
                unsigned int*     puiDataLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucDerP7EnvelopedData	输入参数，符合 PKCS#7 数字信封格式的数据包
uiDerP7EnvelopedDataLen	输入参数，符合 PKCS#7 数字信封格式的数据包长度
pucData	输出参数，解密的原文数据
puiDataLen	输出参数，解密的原文数据长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.5.6 编码 PKCS7 格式的签名数字信封

描述：

制作符合 PKCS#7 签名数字信封格式的数据包。被打包的信息可能包括接收者信息、加密数据、签名信息、签名者的证书等。详细参见 PKCS#7 规范的 SignedAndEnvelopedData 类型定义。

原型：

```
int SAFX_Pkcs7_EncodeSignedAndEnvelopedData(
                void*           hAppHandle,
                unsigned char*  pucSignerCertificate,
                unsigned int    uiSignerCertificateLen,
                unsigned char*  pucKeyPairPin,
                unsigned int    pucKeyPairPinLen,
                unsigned int    uiDigestAlgorithm,
                unsigned char*  pucEncCertificate,
                unsigned int    uiEncCertificateLen,
                unsigned int    uiEncAlgorithm,
                unsigned char*  pucData,
                unsigned int    uiDataLen,
                unsigned char*  pucDerP7Data,
                unsigned int*   puiDerP7DataLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucSignerCertificate	输入参数，签名者证书
uiSignerCertificateLen	输入参数，签名者证书长度
pucKeyPairPin	输入参数，密钥保护密码
uiKeyPairPinLen	输入参数，密钥保护密码长度
uiDigestAlgorithm	输入参数，杂凑算法标识
pucEncCertificate	输入参数，接收者证书
uiEncCertificateLen	输入参数，接收者证书长度
uiEncAlgorithm	输入参数，加密算法标识
pucData	输入参数，原始数据
uiDataLen	输入参数，原始数据长度
pucDerP7Data	输出参数，PKCS#7 签名数字信封格式的数据包
puiDerP7DataLen	输出参数，PKCS#7 签名数字信封格式的数据包长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.5.7 解码 PKCS7 格式的签名数字信封

描述：

从符合 PKCS#7 签名数字信封格式的数据包中解析出原文、签名者数字证书等。

原型：

```
int SAFX_Pkcs7_DecodeSignedAndEnvelopedData(
                void*           hAppHandle,
                unsigned char*  pucDerP7Data,
                unsigned int    uiDerP7DataLen,
                unsigned char*  pucData,
                unsigned int*   puiDataLen,
```

```
                unsigned char*   pucSignerCertificate,
                unsigned int*    puiSignerCertificateLen,
                unsigned int*    puiDigestAlgorithm
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucDerP7Data	输入参数，PKCS#7 签名数字信封格式的数据包
uiDerP7DataLen	输入参数，PKCS#7 签名数字信封格式的数据包长度
pucData	输出参数，原文数据
puiDataLen	输出参数，原文数据长度
pucSignerCertificate	输出参数，签名者证书
puiSignerCertificateLen	输出参数，签名者证书长度
puiDigestAlgorithm	输出参数，杂凑算法标识

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.5.8 编码 PKCS7 格式的摘要数据

描述：

使用指定的杂凑算法计算原文的摘要，并打包成符合 PKCS#7 摘要数据格式的数据包。详细参见 PKCS#7 规范的 DigestedData 类型定义。

原型：

```
int SAFX_Pkcs7_EncodeDigestedData(
                void*            hAppHandle,
                unsigned int     uiDigestAlgorithm,
                unsigned char*   pucData,
                unsigned int     uiDataLen,
                unsigned char*   pucDerP7DigestedData,
                unsigned int*    puiDerP7DigestedDataLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
uiDigestAlgorithm	输入参数，杂凑算法标识
pucData	输入参数，原文数据
uiDataLen	输入参数，原文数据长度
pucDerP7DigestedData	输出参数，符合 PKCS#7 摘要数据格式的数据包
puiDerP7DigestedDataLen	输出参数，符合 PKCS#7 摘要数据格式的数据包长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.5.9 解码 PKCS7 格式的摘要数据

描述：

从符合 PKCS#7 摘要数据格式的数据包中解析出原文及摘要值。

原型：

```
int SAFX_Pkcs7_DecodeDigestedData(
                void*           hAppHandle,
                unsigned char*  pucDerP7DigestedData,
                unsigned int    uiDerP7DigestedDataLen,
                unsigned int*   puiDigestAlgorithm,
                unsigned char*  pucData,
                unsigned int*   puiDataLen,
                unsigned char*  pucDigest,
                unsigned int*   puiDigestLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucDerP7DigestedData	输入参数，符合 PKCS＃7 摘要数据格式的数据包
uiDerP7DigestedDataLen	输入参数，符合 PKCS＃7 摘要数据格式的数据包长度
puiDigestAlgorithm	输出参数，杂凑算法标识
pucData	输出参数，原文数据
puiDataLen	输出参数，原文数据长度
pucDigest	输出参数，摘要值
puiDigestLen	输出参数，摘要值长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.5.10 编码 PKCS7 格式的加密数据

描述：

制作符合 PKCS＃7 加密数据格式的数据。详细参见 PKCS＃7 规范的 EncryptedData 类型定义。

原型：

```
int SAFX_Pkcs7_EncodeEncryptedData(
                void*           hAppHandle,
                unsigned char*  pucData,
                unsigned int    uiDataLen,
                unsigned char*  pucEncKey,
                unsigned int    uiEncKeyLen,
                unsigned int    uiEncAlgorithm,
                unsigned char*  pucDerP7EncryptedData,
                unsigned int*   puiDerP7EncryptedDataLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucData	输入参数，需要加密的数据
puiDataLen	输入参数，需要加密的数据长度
pucEncKey	输入参数，用于加密原文的密钥

uiEncKeyLen	输入参数,用于加密原文的密钥长度
uiEncAlgorithm	输入参数,加密算法标识
pucDerP7EncryptedData	输出参数,符合 PKCS#7 加密数据格式的数据包
puiDerP7EncryptedDataLen	输出参数,符合 PKCS#7 加密数据格式的数据包长度

返回值:

SARX_OK:成功

其他:失败,详见附录 A。

6.5.11 解码 PKCS7 格式的加密数据

描述:

从符合 PKCS#7 加密数据格式的数据包中解析出原文数据。

原型:

```
int SAFX_Pkcs7_DecodeEncryptedData(
                void*           hAppHandle,
                unsigned char*  pucDerP7EncryptedData,
                unsigned int    puiDerP7EncryptedDataLen,
                unsigned char*  pucEncKey,
                unsigned int    uiEncKeyLen,
                unsigned int    uiEncAlgorithm,
                unsigned char*  pucData,
                unsigned int*   puiDataLen
            )
```

参数:

hAppHandle	输入参数,应用接口句柄
pucDerP7EnvelopedData	输入参数,符合 PKCS#7 加密数据格式的数据包
uiDerP7EnvelopedDataLen	输入参数,符合 PKCS#7 加密数据格式的数据包长度
pucEncKey	输入参数,用于解密数据的密钥
uiEncKeyLen	输入参数,用于解密数据的密钥长度
uiEncAlgorithm	输入参数,加密算法标识
pucData	输出参数,解密的原文数据
puiDataLen	输出参数,解密的原文数据长度

返回值:

SARX_OK:成功

其他:失败,详见附录 A。

6.6 辅助函数

6.6.1 取版本号

描述:

取接口实现的版本号。

原型:

```
int SAFX_GetVersion(
                void*           hAppHandle,
                unsigned char*  puiVersion
            )
```

参数：

hAppHandle　　输入参数，应用接口句柄

puiVersion　　输出参数，版本号

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.6.2 取对应标准的版本号

描述：

取接口对应标准的版本号。

原型：

```
int SAFX_GetSpecificationsVersion(
                void*           hAppHandle,
                unsigned int*   puiSpecificationsVersion
            )
```

参数：

hAppHandle　　输入参数，应用接口句柄

puiSpecificationsVersion　　输出参数，取接口对应标准的版本号

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

备注：版本号的格式为：0xAAAABBBB，其中 AAAA 为主版本号，BBBB 为次版本号。

6.6.3 BASE64 编码

描述：

对数据进行 Base64 编码。

原型：

```
int SAFX_Base64_Encode(
                void*           hAppHandle,
                unsigned char*  pucInData,
                unsigned int    uiInDataLen,
                unsigned char*  pucOutData,
                unsigned int*   puiOutDataLen
            )
```

参数：

hAppHandle　　输入参数，应用接口句柄

pucInData　　输入参数，编码前的数据

uiInDataLen　　输入参数，编码前的数据长度

pucOutData　　输出参数，编码后的数据

puiOutDataLen　　输出参数，编码后的数据长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

6.6.4 BASE64 解码

描述：

对 Base64 编码数据进行解码。

原型：

```
int SAFX_Base64_Decode(
                void*           hAppHandle,
                unsigned char*  pucInData,
                unsigned int    uiInDataLen,
                unsigned char*  pucOutData,
                unsigned int*   puiOutDataLen
            )
```

参数：

hAppHandle	输入参数，应用接口句柄
pucInData	输入参数，解码前的数据
uiInDataLen	输入参数，解码前的数据长度
pucOutData	输出参数，解码后的数据
puiOutDataLen	输出参数，解码后的数据长度

返回值：

SARX_OK：成功

其他：失败，详见附录 A。

附 录 A
（规范性附录）
返回码定义与描述

A.1 返回码意义

返回码是在函数执行完毕后返回的变量，在函数执行成功时，其返回值为 0，在函数执行出错时，其返回值不为 0。关于各返回码的详细说明见表 A.1。

A.2 返回码编号及其解释

表 A.1 返回码编号及其解释

宏 描 述	预定义值	说 明
# define SARX_OK	0x0	成功
# define SARX_UnknownErr	0x02000001	异常错误
# define SARX_NotSupportYetErr	0x02000002	不支持的服务
# define SARX_FileErr	0x02000003	文件操作错误
# define SARX_ProviderTypeErr	0x02000004	服务提供者参数类型错误
# define SARX_LoadProviderErr	0x02000005	导入服务提供者接口错误
# define SARX_LoadDevMngApiErr	0x02000006	导入设备管理接口错误
# define SARX_AlgoTypeErr	0x02000007	算法类型错误
# define SARX_NameLenErr	0x02000008	名称长度错误
# define SARX_KeyUsageErr	0x02000009	密钥用途错误
# define SARX_ModulusLenErr	0x02000010	模的长度错误
# define SARX_NotInitializeErr	0x02000011	未初始化
# define SARX_ObjErr	0x02000012	对象错误
# define SARX_MemoryErr	0x02000100	内存错误
# define SARX_TimeoutErr	0x02000101	超时
# define SARX_IndataLenErr	0x02000200	输入数据长度错误
# define SARX_IndataErr	0x02000201	输入数据错误
# define SARX_GenRandErr	0x02000300	生成随机数错误
# define SARX_HashObjErr	0x02000301	杂凑对象错
# define SARX_HashErr	0x02000302	杂凑运算错误
# define SARX_GenRsaKeyErr	0x02000303	产生 RSA 密钥错
# define SARX_RsaModulusLenErr	0x02000304	RSA 密钥模长错误
# define SARX_CspImprtPubKeyErr	0x02000305	CSP 服务导入公钥错误

表 A.1（续）

宏 描 述	预定义值	说 明
# define SARX_RsaEncErr	0x02000306	RSA 加密错误
# define SARX_RSGDXecErr	0x02000307	RSA 解密错误
# define SARX_HashNotEqualErr	0x02000308	摘要值不相等
# define SARX_KeyNotFountErr	0x02000309	密钥未发现
# define SARX_CertNotFountErr	0x02000310	证书未发现
# define SARX_NotExportErr	0x02000311	对象未导出
# define SARX_DecryptPadErr	0x02000400	解密时做补丁错误
# define SARX_MacLenErr	0x02000401	MAC 长度错误
# define SARX_KeyInfoTypeErr	0x02000402	密钥类型错误

参 考 文 献

[1] 证书认证系统密码及其相关安全技术规范
[2] 数字证书认证系统密码协议规范
[3] 公钥密码基础设施应用技术体系 通用密码服务接口规范

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 公钥基础设施
X.509 数字证书应用接口规范
GB/T 25060—2010
*
中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.75 字数 45 千字
2010 年 11 月第一版 2010 年 11 月第一次印刷
*
书号:155066·1-40464 定价 27.00 元

GB/T 25060-2010

打印日期:2010年12月3日 F009