本规范介绍了8位字节串和位串之间的转换，包括位串到8位字节串的转换、8位字节串到位串的转换、整数到8位字节串的转换、8位字节串到整数的转换。

本规范介绍了SM2算法的数据格式，包括密钥数据格式、加密数据格式、签名数据格式、密钥对保护数据格式。

本规范还介绍了预处理和计算过程，包括生成密钥、加密、解密、签名、验签和密钥协商。

28.1.6 SM2密码算法加密签名消息语法规范（GM/T 0010）

GM/T 0010-2012《SM2密码算法加密签名消息语法规范》

本规范定义了使用SM2密码算法的加密签名消息语法，适用于使用SM2算法进行加密和签名操作时对操作结果的标准化封装。

本规范对6类对象data，signedData，envelopedData，signedAndEnvelopedData，encryptedData和keyAgreementInfo的标识符进行了定义。

对象标识符OID	对象标识符定义
1.2.156.10197.6.1.4.2	SM2密码算法加密签名消息语法规范
1.2.156.10197.6.1.4.2.1	数据类型data
1.2.156.10197.6.1.4.2.2	签名数据类型signedData
1.2.156.10197.6.1.4.2.3	数字信封数据类型envelopedData
1.2.156.10197.6.1.4.2.4	签名及数字信封数据类型signedAndEnvelopedData
1.2.156.10197.6.1.4.2.5	加密数据类型encryptedData
1.2.156.10197.6.1.4.2.6	密钥协商类型keyAgreementInfo

本规范对上述6类对象的数据类型结构进行了详细定义。

28.1.7 数字证书认证系统密码协议规范（GM/T 0014）

GM/T 0014-2012《数字证书认证系统密码协议规范》

本规范适用于电子政务/电子商务基于密码技术的数字证书认证系统的设计、建设、检测、运营及管理，规范数字证书认证系统中密码协议的标准化应用，推动数字证书认证系统密码协议的互联互通和相互认证。对于组织或机构内部使用的数字证书认证系统密码协议的建设、运营及管理，可参考使用。同时本规范还可为安全产品生产商提供产品和技术的准确定位和标准化的参考，提高安全产品的可信性和互操作性。

本规范涉及的相关协议指数字证书认证系统中涉及到密码技术的安全协议，特别是证书认证系统使用的有关安全协议。这些协议包括用户终端同RA之间的安全协议，RA同CA之间的安全协议，CA同KM之间的安全协议，CA同LDAP服务之间的安全协议，CA同OCSP服务之间的安全协议，用户同LDAP服务之间的安全协议，用户同OCSP服务之间的安全协议等。

本规范给出了与协议直接相关的格式、语法等内容，其中凡涉及RSA密码算法的，其密钥结构遵循PKCS#1规范，其封装结构遵循PKCS#7规范；凡涉及SM2算法的，其密钥结构遵照GM/T 0009，其封装结构遵循GM/T 0010；凡涉及对象标识符的应遵循GM/T 0006。

另外，本规范附录 1 中给出了证书模板格式、证书作废列表格式、加密值、PKI 消息的状态码和故障信息等，附录 2 给出了 RA 与 CA 之间的相关协议说明，附录 3 给出了协议报文的实例，附录 4 给出了非实时发布证书协议流程。

28.1.8 基于 SM2 密码算法的数字证书格式规范（GM/T 0015）

GM/T 0015-2012《基于 SM2 密码算法的数字证书格式规范》

本规范规定了基于 SM2 密码算法的数字证书和证书撤销（作废）列表的基本结构，并对数字证书和证书撤销列表中的各数据项内容进行了描述。适用于数字证书认证系统的研发、数字证书认证机构的运营以及基于数字证书的安全应用。

本规范详细介绍了数字证书格式，包括基本证书域和 TBSCertificate 的数据结构两部分内容。TBSCertificate 包含了证书结构中的前十项信息。这些信息主要有主体和颁发者的名称、主体的公钥、有效期、版本号和序列号，有些 TBSCertificate 还可以包含可选的唯一标识符项和扩展项。还介绍了证书扩展域及其数据结构，包括标准扩展和专用因特网扩展。

本规范还介绍了 CRL 格式，包括 CRL 的数据结构、TBSCertList 及其数据结构和 CRL 扩展项及其数据结构，并在附录中给出了证书的结构以及实例、证书和 CRL 内容表和数字证书编码举例。

28.1.9 通用密码服务接口规范（GM/T 0019）

GM/T 0019-2012《通用密码服务接口规范》

本规范规定了统一的通用密码服务接口，适用于公开密钥应用技术体系下密码应用服务的开发，密码应用支撑平台的研制及检测，也可用于指导直接使用密码设备的应用系统的开发。

本规范对算法标识和数据结构、密码服务接口和密码服务接口函数进行了定义。算法标识和数据结构主要内容包括算法标识与常量定义、用户证书列表、密钥容器信息列表和证书中 DN 的结构；密码服务接口的主要内容包括环境类函数、证书类函数、密码运算类函数和消息类函数。

本规范中密码服务接口函数定义主要分为以下四类函数。

1．环境类函数

（1）初始化环境：SAF_Initialize
（2）清除环境：SAF_Finalize
（3）获取接口版本信息：SAF_GetVersion
（4）用户登录：SAF_Login
（5）修改 PIN：SAF_ChangePin
（6）注销登录：SAF_Logout

2．证书类函数

（1）添加根 CA 证书：SAF_AddPrustedRootCaCertificate
（2）获取根 CA 证书个数：SAF_GetRootCaCertificateCount

（3）获取根 CA 证书：SAF_GetRootCaCertificate
（4）删除根 CA 证书：SAF_RemoveRootCaCertificate
（5）添加 CA 证书：SAF_AddCaCertificate
（6）获取 CA 证书个数：SAF_GetCaCertificateCount
（7）获取 CA 证书：SAF_GetCaCertificate
（8）删除 CA 证书：SAF_RemoveCaCertificate
（9）添加 CRL：SAF_AddCrl
（10）验证用户证书：SAF_VerifyCertificate
（11）根据 CRL 文件获取用户证书注销状态：SAF_VerifyCertificateByCrl
（12）根据 OCSP 获取证书状态：SAF_GetCertificateStateByOCSP
（13）通过 LDAP 方式获取证书：SAF_GetCertificateFromLdap
（14）通过 LDAP 方式获取证书对应的 CRL：SAF_GetCrlFromLdap
（15）取证书信息：SAF_GetCertificateInfo
（16）取证书扩展信息：SAF_GetExtTypeInfo
（17）列举用户证书：SAF_EnumCertificate
（18）列举用户的密钥容器信息：SAF_EnumKeyContainerInfo
（19）释放列举用户证书的内存：SAF_EnumCertificateFree
（20）释放列举密钥容器信息的内存：SAF_EnumkeyContainerInfoFree

3．密码运算类函数

（1）单块 Base64 编码：SAF_Base64_Encode
（2）单块 Base64 解码：SAF_Base64_Decode
（3）创建 Base64 对象：SAF_Base64_CreateBase64Obj
（4）销毁 Base64 对象：SAF_Base64_DestroyBase64Obj
（5）通过 Base64 对象继续编码：SAF_Base64_EncodeUpdate
（6）通过 Base64 对象编码结束：SAF_Base64_EncodeFinal
（7）通过 Base64 对象继续解码：SAF_Base64_DecodeUpdate
（8）通过 Base64 对象解码结束：SAF_Base64_DecodeFinal
（9）生成随机数：SAF_GenRandom
（10）HASH 运算：SAF_Hash
（11）创建 HASH 对象：SAF_CreateHashObj
（12）删除 HASH 对象：SAF_DestroyHashObj
（13）通过对象多块 HASH 运算：SAF_HashUpdate
（14）结束 HASH 运算：SAF_HashFinal
（15）生成 RSA 密钥对：SAF_GenRsaKeyPair
（16）获取 RSA 公钥：SAF_GetPublicKey
（17）RSA 签名运算：SAF_RsaSign
（18）对文件进行 RSA 签名运算：SAF_RsaSignFile
（19）RSA 验证签名运算：SAF_RsaVerifySign

（20）对文件及其签名进行 RSA 验证：SAF_RsaVerifySignFile
（21）基于证书的 RSA 公钥验证：SAF_VerifySignByCert
（22）生成 ECC 密钥对：SAF_GenEccKeyPair
（23）获取 ECC 公钥：SAF_GetEccPublicKey
（24）ECC 签名：SAF_EccSign
（25）ECC 验证：SAF_EccVerifySign
（26）ECC 公钥加密：SAF_EccPublicKeyEnc
（27）基于证书的 ECC 公钥加密：SAF_EccPublicKeyEncByCert
（28）基于证书的 ECC 公钥验证：SAF_EccVerifySignByCert
（29）创建对称算法对象：SAF_CreateSymmAlgoObj
（30）生成会话密钥并用外部公钥加密输出：SAF_GenerateKeyWithEPKu
（31）导入加密的会话密钥：SAF_ImportEncedKey
（32）生成密钥协商参数并输出：SAF_GenerateAgreementDataWithECC
（33）计算会话密钥：SAF_GenerateKeyWithECC
（34）产生协商数据并计算会话密钥：SAF_GenerateAgreementDataAndKeyWithECC
（35）销毁对称算法对象：SAF_DestroySymmAlgoObj
（36）销毁会话密钥句柄：SAF_DestroyKeyHandle
（37）单块加密运算：SAF_SymmEncrypt
（38）多块加密运算：SAF_SymmEncryptUpdate
（39）结束加密运算：SAF_SymmEncryptFinal
（40）单块解密运算：SAF_SymmDecrypt
（41）多块解密运算：SAF_SymmDecryptUpdate
（42）结束解密运算：SAF_SymmDecryptFinal
（43）单组数据消息鉴别码运算：SAF_Mac
（44）多组数据消息鉴别码运算：SAF_MacUpdate
（45）结束消息鉴别码运算：SAF_MacFinal

4．消息类函数

（1）编码 PKCS#7 格式的带签名的数字信封数据：SAF_Pkcs7_EncodeData
（2）解码 PKCS#7 格式的带签名的数字信封数据：SAF_Pkcs7_DecodeData
（3）编码 PKCS#7 格式的签名数据：SAF_Pkcs7_EncodeSignedData
（4）解码 PKCS#7 格式的签名数据：SAF_Pkcs7_DecodeSignedData
（5）编码 PKCS#7 格式的数字信封数据：SAF_Pkcs7_EncodeEnvelopedData
（6）解码 PKCS#7 格式的数字信封数据：SAF_Pkcs7_DecodeEnvelopedData
（7）编码 PKCS#7 格式的摘要数据：SAF_Pkcs7_EncodeDigestedData
（8）解码 PKCS#7 格式的摘要数据：SAF_Pkcs7_DecodeDigestedData
（9）编码基于 SM2 算法的带签名的数字信封数据：SAF_SM2_EncodeSignedAndEnvelopedData
（10）解码基于 SM2 算法的带签名的数字信封数据：SAF_SM2_DecodeSignedAnd

EnvelopedData

（11）编码基于 SM2 算法的签名数据：SAF_SM2_EncodeSignedData

（12）解码基于 SM2 算法的签名数据：SAF_SM2_DecodeSignedData

（13）编码基于 SM2 算法的数字信封：SAF_SM2_EncodeEnvelopedData

（14）解码基于 SM2 算法的数字信封：SAF_SM2_DecodeEnvelopedData

在附录中给出了上述接口函数返回值错误代码的定义。

28.1.10　证书应用综合服务接口规范（GM/T 0020）

GM/T 0020-2012《证书应用综合服务接口规范》

本规范规定了面向证书应用的统一服务接口，适用于公钥密码应用技术体系下密码应用服务产品的开发，密码应用支撑平台的研制及检测，也可用于指导直接使用密码设备和密码服务应用系统的集成和开发。

证书应用综合服务接口位于应用系统和典型密码服务接口之间，向应用层直接提供证书信息解析、基于数字证书身份认证和信息的机密性、完整性、不可否认性等高级密码服务。该接口可直接供应用系统调用，将应用系统的密码服务请求转向通用密码服务接口，通过通用密码服务接口调用相应的密码设备实现具体的密码运算和密钥操作。通用密码服务接口应遵循 GM/T 0019。

本规范所定义的证书应用综合服务接口包括客户端服务接口和服务器端服务接口两类，其中服务器端服务接口采用 COM 组件形式和 Java 形式描述。

客户端服务接口采用客户端控件方式，客户端控件适用于客户端程序调用，接口的形态包括 DLL 动态库、ActiveX 控件、Applet 插件等，接口应支持 Windows XP、Windows 2000、Windows 2003、Vista、Windows 7 等终端用户使用的主流操作系统。客户端控件接口的主要函数功能应包括：配置管理、证书解析、签名与验证、加密与解密、数字信封、XML 数据的签名与验证等。在定义客户端服务接口时，本规范以 ActiveX 控件为例进行描述，其中 BSTR 代表函数返回值或参数类型为 OLECHAR 字符串类型，不同的开发语言应采取对应的类型定义，如 char *、CString、java.lang.String 等。

服务器端服务接口适用于服务器端程序调用，接口的形态包括 COM 组件、JAR 包、WebService 等形态，接口应支持 Windows、Linux、UNIX、AIX、Solaris 等服务器使用的主流操作系统。服务器端服务接口的函数功能与客户端控件接口相对应，主要包括：配置管理、数字证书解析、签名与验证、加密与解密、数据信封、XML 数据的签名与验证、时间戳等。

本规范在附录中给出了证书应用综合服务接口的错误代码返回值、典型部署模型和集成示例。

28.1.11　IPSec VPN 技术规范（GM/T 0022）

GM/T 0022-2014 IPSec VPN 技术规范

本规范的协议部分主要依据 RFC4301、RFC4302、RFC4303、RFC4308、RFC4309 等标准制定。按照我国相关密码政策和法规，结合我国实际应用需求及产品生产厂商的实践经验，对密钥协商、密码算法及使用、某些功能项的实施方法提出了一些特定的要求。

本规范对 IPSec VPN 的技术协议、产品功能、性能和管理以及检测进行了规定，可用