于指导 IPSec VPN 产品的研制、检测、使用和管理。基于本规范研制的 IPSec VPN 产品所用的密码算法和密码部件须经国家密码管理局审批。本规范中未明确指明为可选要素的部分均为必备要素。

本规范主要由范围、规范性引用文件、术语与缩略语、密码算法和密钥种类、协议、IPSec VPN 产品要求、IPSec VPN 产品检测、合格判定等 8 章内容和附录 A（资料性附录）IPSec VPN 概述组成。其中，协议由密钥交换协议、安全报文协议等两节内容组成。IPSec VPN 产品要求由产品功能要求、产品性能要求、安全管理要求等 3 节内容组成。IPSec VPN 产品检测由产品功能检测、产品性能检测、安全管理检测等 3 节内容组成。

28.1.12 SSL VPN 技术规范（GM/T 0024）

GM/T 0024-2014 SSL VPN 技术规范

本规范的协议内容参照传输层安全协议（RFC4346 TLS1.1）。依据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，在 TLS1.1 的握手协议中增加了 ECC、IBC 的认证模式和密钥交换模式，取消了 DH 密钥协商方式，修改了密码套件的定义。此外，在本规范中还增加了网关-网关协议。

本规范对 SSL VPN 的密码算法、技术协议、产品的功能、性能和管理以及检测进行了规定。本规范适用于 SSL VPN 产品的研制，也可用于指导 SSL VPN 产品的检测和使用。本规范中未明确指明为可选要素的部分均为必备要素。基于本规范研制的 SSL VPN 产品所用的密码算法和密码部件须经国家密码管理局审批。

本规范主要由范围、规范性引用文件、术语和定义、符号和缩略语、密码算法和密钥种类、协议、产品要求、产品检测基本要求、合格判定等 9 章内容组成。其中，协议由概述、数据类型定义、记录层协议、握手协议族、密钥计算、网关到网关协议等 6 节内容组成。产品要求由产品功能要求、产品性能要求、安全管理要求等 3 节内容组成。产品检测基本要求由产品功能检测基本要求、产品性能检测基本指标、安全管理检测基本要求等 3 节内容组成。

28.1.13 安全认证网关产品规范（GM/T 0026）

GM/T 0026-2014《安全认证网关产品规范》

本规范规定了安全认证网关产品使用的密码算法和密钥种类，对安全认证网关产品的功能、性能、安全管理以及产品检测进行了规定，可用于指导安全认证网关产品的研制、检测、使用和管理。本规范有效解决了安全认证网关产品的安全性和规范性的统一，有利于节省产品开发商的开发成本和开发难度，有利于各厂家产品之间的互联互通。本规范有利于提升用户对产品的规范使用和管理水平，有利于相关检测机构对该类产品的规范化检测。

本规范共包括 9 章正文：

第 1 章“范围”，描述了本规范的适用范围、规范的边界等。

第 2 章“规范性引用文件”，描述了本规范应用的相关文件，包括《随机数检测规范》、《IPSec VPN 技术规范》、《SSL VPN 技术规范》、《密码设备管理规范》等规范。

第 3 章“术语和缩略语”，介绍了规范中使用的术语和缩略语。

第4章“符号和缩略语”，介绍了规范中使用的符号和缩略语。

第5章“安全认证网关概述”，给出了安全认证网关产品的概述。

第6章“密码算法和密钥种类”，列出了规范中使用的密码算法和密钥种类。

第7章“安全认证网关产品要求”，从产品功能、产品性能、安全性要求和管理要求等方面对安全认证网关产品提出了具体要求。

第8章“安全认证网关产品检测”，规定了安全认证网关产品须完成的检测。第7章和第8章为本规范的关键章节。

第9章“合格判定”，说明了产品的合格判定标准。

28.1.14 签名验签服务器技术规范（GM/T 0029）

GM/T 0029-2014《签名验签服务器技术规范》

本标准的主要目的是规定签名验签服务器的相关技术规范，包括签名验签服务器的功能要求、安全要求、接口要求、检测要求和消息协议语法规范等有关内容，为签名验签服务器的研制和开发提供指导和依据。

本规范共包括8章正文和2个附录：第1章“范围”；第2章“规范性引用文件”；第3章“术语和定义”；第4章“符号和缩略语”；第5章“签名验签服务器的功能要求”；第6章“签名验签服务器的安全要求”；第7章“签名验签服务器的检测要求”；第8章“合格判定”；附录A“消息协议语法规范”；附录B“响应码定义和说明”。

其中，第5章描述了签名验签服务器的主要功能，包括初始化功能要求、与CA基础设施的连接功能要求、应用管理功能要求、证书管理和验证功能要求、数字签名功能要求、访问控制功能要求、设备管理功能要求、日志管理功能要求、设备自检功能要求。

第6章定义了签名验签服务器在密码设备、系统要求、使用要求、管理要求、物理安全、网络部署、API接口、环境适应性、可靠性等方面的要求。

第7章定义了签名验签服务器的检测要求，包括外观和结构、提交文档、功能检测、性能检测、环境适应性检测等检测内容。

附录A中签名验签服务的消息协议接口采用请求响应模式，协议模型由请求者、响应者和它们之间的交互协议组成。通过本协议，请求者将数字签名、验证数字签名等请求发送给响应者，由响应者完成签名验签服务并返回结果。本规范中的接口消息协议包括导出证书、解析证书、验证证书有效性、数字签名、验证数字签名、消息签名、验证消息签名等服务功能。

附录B定义了消息协议的响应码。

28.1.15 安全电子签章密码技术规范（GM/T 0031）

GM/T 0031-2014《安全电子签章密码技术规范》

本规范的制定可以有效提升电子签章产品使用密码技术的安全性和规范性，保障行业的健康发展。同时，有利于节省产品开发商的开发成本和开发难度，有利于各厂家产品之间的互联互通，降低用户选用产品的技术门槛，提升用户对产品的规范使用和管理水平，有利于相关检测机构对该类产品的规范化检测。

本规范共包括6章正文：第1章“范围”；第2章“规范性引用文件”；第3章“术语和定义”；第4章“符号和缩略语”；第5章“电子签章的密码应用安全机制”；第6章“电

子签章密码应用协议”。

其中，第 1 章至第 4 章为总述性内容，介绍规范的范围、规范引用、关键术语等。

第 5 章和第 6 章为电子签章密码应用的关键章节，详细规定了数据格式、密码处理流程等。

第 5 章介绍了电子签章密码应用的基本安全机制。

第 6 章分别对电子印章和电子签章的数据格式、处理流程等，从密码安全应用的角度进行了规范。

28.1.16 时间戳接口规范（GM/T 0033）

GM/T 0033-2014《时间戳接口规范》

本标准的目标是在上层应用与时间戳系统之间制定一套统一的时间戳服务接口，为应用系统提供精确可信的时间认证服务，确保时间戳服务在信息系统的应用中能够通用，实现信息系统互联互通，为应用实现业务处理的抗抵赖性提供基础，同时有利于相关检测机构对该类产品的规范化检测。遵循本规范的时间戳服务产品可以实现和时间戳系统无关以及和证书认证系统无关的时间认证服务，保证时间戳服务对用户、对应用的透明性和无关性。

本规范共包括 9 章正文：第 1 章“范围”；第 2 章“规范性引用文件”；第 3 章“术语和定义”；第 4 章“符号和缩略语”；第 5 章“标识和数据结构”；第 6 章“时间戳服务描述”；第 7 章“时间戳的请求和响应格式”；第 8 章“时间戳服务与时间戳服务机构的通讯方式”；第 9 章“时间戳服务接口组成和功能说明”。

其中，第 1 章至第 4 章为总述性内容，介绍规范的整体情况、关键术语、符号和缩略语等。

第 5 章介绍了规范中定义的算法标识和数据结构，包括标识定义、密码服务接口以及时间戳服务接口常量定义。

第 6 章描述了时间戳服务接口的逻辑结构。

第 7 章定义了时间戳服务请求格式、响应格式的 ASN.1 编码方式。

第 8 章定义了 5 种通讯方式：电子邮件方式、文件方式、Socket 方式、HTTP 方式、SOAP 方式，并规定了消息传输格式。

第 9 章描述了 7 个与时间戳服务有关的函数，涵盖了获取时间戳服务的全部功能，包括环境函数和时间戳服务函数两大类。环境函数类中包含初始化环境和清除环境函数，时间戳服务函数类中包含生成时间戳请求、生成时间戳应答、验证时间戳有效性、获取时间戳主要信息、解析时间戳详细信息。在上述部分中详细描述了各个接口函数，包括各函数的原型、描述、参数说明、返回值说明及备注等详细信息。

28.1.17 基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范（GM/T 0034）

GM/T 0034-2014《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》

本标准主要是规定了为公众服务的数字证书认证系统的设计、建设、检测、运行及管理规范。本规范的目标是为实现数字证书认证系统的互联互通和交叉认证提供统一的依据，

指导第三方认证机构的数字证书认证系统的建设和检测评估，规范数字证书认证系统中密码及相关安全技术的应用，并有利于相关检测机构对该类产品的规范化检测。同时非第三方认证机构的数字证书认证系统的建设、运行及管理也可参照本标准执行。

本规范共包括11章正文：第1章“范围”；第2章“规范性引用文件”；第3章“术语”；第4章“缩略语”；第5章“证书认证系统”；第6章“密钥管理中心”；第7章“密码算法、密码设备及接口”；第8章“证书认证中心建设”；第9章“密钥管理中心建设”；第10章“证书认证中心运行管理要求”；第11章“密钥管理中心运行管理要求”。

其中，第1章至第4章为总述性内容，介绍规范的整体情况、关键术语、符号和缩略语等。

第5章介绍了证书认证系统的设计细节，包括系统的总体设计和各子系统设计，并提供了设计原则以及各个子系统的实现方式。

第6章描述了密钥管理中心的组成模块，包括密钥生成、密钥管理、密钥库管理、认证管理、安全审计、密钥恢复和密码服务等模块。

第7章定义了证书认证系统的密码算法、密码设备和接口。

第8章从系统、安全、数据备份、可靠性、物理安全、人事管理制度等方面规范了证书认证中心的建设。

第9章从系统、安全、数据备份、可靠性、物理安全、人事管理制度等方面规范了密钥管理中心的建设。

第10章从人员管理、业务运行管理、密钥分管、安全管理、安全审计、文档配备等方面对证书认证中心的运行管理要求进行了规范。

第11章从人员管理、业务运行管理、密钥分管、安全管理、安全审计、文档配备等方面对密钥管理中心的运行管理要求进行了规范。

28.1.18　证书认证系统检测规范（GM/T 0037）

GM/T 0037-2014《证书认证系统检测规范》

本规范的编制主要用于检测按照《证书认证系统密码及其相关安全技术规范》研制或建设的数字证书认证系统，也可以为其他数字证书认证系统的研制、建设提供参考作用。其主要作用是为国内第三方认证服务系统提供一个标准的、规范的测试范围、测试内容、测试方法以及判定策略。

本规范主要由以下几部分对数字证书认证系统的检测进行规范。

1．检测对象

《规范》确定适用的检测对象为证书认证系统产品及按《证书认证系统密码及其相关安全技术规范》要求建设的证书认证服务运营系统项目。

2．测试大纲

规定了测试大纲编制的原则，并在附录中提供了可供参考的测试大纲的示例。

3．检测环境

确定了产品和项目的检测环境。

4．检测内容

对场地、网络、岗位及权限管理、安全管理、系统初始化、系统功能、性能、数据备份和恢复、第三方安全产品、入根、证书格式、证书链、算法等 13 个方面详细规定了检测内容。

5．检测方法

规定了 13 项检测内容的具体检测方法。

6．合格判定

规定了判定产品和项目合格的最低条件。

通过检测内容和检测方法可以很清楚地了解到研制、建设一个第三方认证服务系统时应具备的系统功能和检测内容。规范最后还附有检测大纲、认证系统的网络结构、认证系统机房布局和物理连线等资料性附录，供国内 PKI 厂商和运营商参考。

28.1.19　证书认证密钥管理系统检测规范（GM/T 0038）

GM/T 0038-2014《证书认证密钥管理系统检测规范》

《规范》的编制主要用于检测按照《证书认证系统密码及其相关安全技术规范》研制或建设的密钥管理系统，也可以为其他密钥管理系统的研制、建设提供参考。其主要作用是为国内第三方认证服务系统的密钥管理系统提供一个标准的、规范的测试范围、测试内容、测试方法以及判定策略。

本规范主要由以下几部分对密钥管理系统的检测进行了规范。

1．检测对象

《规范》确定适用的检测对象为密钥管理系统产品及按《证书认证系统密码及其相关安全技术规范》要求建设的密钥管理系统项目。

2．测试大纲

规定了测试大纲编制的原则，并在附录中提供了可供参考的测试大纲的示例。

3．检测环境

确定了产品和项目的检测环境。

4．检测内容

对场地、网络、岗位及权限管理、安全管理、系统初始化、系统功能、性能、数据备份和恢复、第三方安全产品等 9 个方面详细规定了检测内容。

5．检测方法

规定了 9 项检测内容的具体检测方法。

6．合格判定

规定了判定产品和项目合格的最低条件。

通过检测内容和检测方法可以很清楚地了解到研制、建设一个密钥管理系统时应具备的系统功能和检测内容。规范最后还附有检测大纲、密钥管理系统的网络结构、密钥管理