

文件编号：EGS N308-6

日期：2005 年 12 月 15 日

标题：“电子政务标准化指南 第 6 部分：信息安全”

来源：“电子政务标准化指南 第 6 部分：信息安全”工作组

内容摘要：“电子政务标准化指南 第 6 部分：信息安全”征求意见稿

页数：46

电子政务标准化总体组秘书处

联系人：陈星

通信地址：北京市东城区安定门东大街 1 号

电话：(010) 84029233 传真：(010) 64007681 手机：13581787525

电子邮件：chenxing@cesi.ac.cn

电子政务标准化指南

(第二版)

第六部分：信息安全

(征求意见稿)

国家标准化管理委员会
国务院信息化工作办公室

二 五年十月

前言

电子政务是国家信息化建设的重要领域。标准化是支撑电子政务的重要手段。为了加强电子政务标准化工作，国务院信息化工作办公室和国家标准化管理委员会成立了“国家电子政务标准总体组”。总体组适时编写了《电子政务标准化指南》，以指导我国电子政务的建设，促进其健康发展。

《电子政务标准化指南》共分以下六个部分：

第一部分：总则

第二部分：工程管理

第三部分：网络建设

第四部分：信息共享

第五部分：支撑技术

第六部分：信息安全

《电子政务标准化指南 第 6 部分 信息安全》的定位为：在电子政务建设过程和运行维护过程中，指导如何根据实际需要，按照国家政策、法规的要求，选择相应的信息安全标准，支持建设符合国家政策要求的、规范的、有效的电子政务信息安全体系。

本指南的起草单位为全国信息安全标准化技术委员会 WG1 工作组、信息产业部电子工业标准化研究所、中国电子科技集团第三十研究所、上海二零卫士信息安全有限公司、北京大学。

本指南主要起草人：张建军、王立福、贾颖禾、马朝斌、吴志刚、胡啸、陈星、刘学洋、曾波

电子政务标准化指南 第6部分 信息安全

目次

第一章 概述.....	4
1、编写目的.....	4
2、编写原则.....	4
3、范围.....	4
第二章 电子政务信息安全标准体系.....	5
1、标准体系概念.....	5
2、电子政务信息安全标准体系.....	5
3、国家保密标准与密码技术标准.....	6
4、标准明细表.....	7
4.1 基础标准 (52).....	7
4.2 技术与机制标准 (44).....	10
4.3 信息安全管理 (11).....	12
4.4 评估标准 (34).....	13
第三章 关键标准说明与使用.....	15
1、基础标准.....	15
1.1 术语.....	15
1.2 体系与模型.....	15
1.3 保密标准.....	19
1.4 密码技术.....	21
2、技术与机制标准.....	22
2.1 标识与鉴别.....	22
2.2 授权与访问.....	24
2.3 管理技术.....	28
2.4 物理安全.....	29
3、信息安全管理.....	30
4、评估标准.....	32
4.1 评估基础标准.....	32
4.2 产品测评标准.....	35
4.3 系统测评标准.....	39
附录.....	41
1. 术语表.....	41
2. 电子政务信息系统安全实施的一般步骤与采标指南.....	41
2.1 电子政务信息系统安全实施的一般步骤描述.....	41
2.2 采标指南.....	44

第一章 概述

1、编写目的

《电子政务标准化指南 第6部分 信息安全》的编写拟达到以下目的：

1) 完善电子政务信息安全标准体系

本指南规划了电子政务信息安全标准体系,介绍了电子政务建设中所需要的一些重要标准,其中既有已经发布的标准,也有尚需制定的标准。本指南将指导电子政务信息安全标准体系的建设。

2) 指导电子政务信息安全体系建设的标准化

本指南对电子政务系统安全体系建设的相关标准进行了描述,以帮助电子政务的建设者、用户在系统的规划、设计、建设、验收、测评、运行中,选取、采用合适的标准,按照标准开展工作,有效地支持电子政务信息安全体系的建立,更好地保证电子政务系统的安全。

2、编写原则

1) 立足中国国情,结合我国电子政务特点,建立实用的标准体系

本指南是配合我国电子政务的建设而编制的,其内容符合现阶段我国电子政务建设、运行、管理的特点,用于指导电子政务实际建设中解决信息安全问题时的采标,建立相应的信息安全标准体系。

2) 遵循国家法律、法规、标准,保持技术最大相容

国家已经颁布了若干信息安全相关法令、法规、标准。本指南基于这些文件,针对电子政务建设的实际需要,介绍这些标准的主要内容,供电子政务信息安全系统建设时参考。本指南提供的标准除了国家已经颁布的标准外,还根据最近国家立项的信息安全标准情况,对即将颁布的相关标准进行了介绍。

3) 满足选标、采标需求

本指南从电子政务系统的建设者和用户在系统建设过程中选取、采用信息安全标准的需求出发,以易于选标、采标的方式编写、制定。

3、范围

本指南可作为电子政务系统规划、设计、建设、验收、测评、运行过程中,信息安全方面采标工作的指导,适用于电子政务系统建设的决策人和管理者、电子政务系统的建设者、电子政务系统相关安全产品研究开发人员。

第二章 电子政务信息安全标准体系

1、 标准体系概念

标准体系是由一定范围内的具有内在联系的标准组成的科学有机整体，是编制标准制定、修订计划的依据之一，也是标准使用者阅读、理解标准的有效工具。标准体系能促进一定范围内的标准组成趋向科学化，是一幅现有、应有和预计制订标准的蓝图，并随着科学技术的发展不断地得到完善和更新。

信息安全标准体系是指信息安全保障体系建设所需标准按其内在联系构成的科学有机整体，一般包括结构图和明细表两部分。信息安全标准体系是信息安全保障体系建设所需标准的结构化蓝图

2、 电子政务信息安全标准体系

电子政务信息安全标准从总体上划分为四大类：基础标准、技术与机制标准、管理标准和应用标准，在每一大类的基础上，按照标准所涉及的主要内容进行细分。电子政务信息安全标准体系总体框架如图 1 所示。

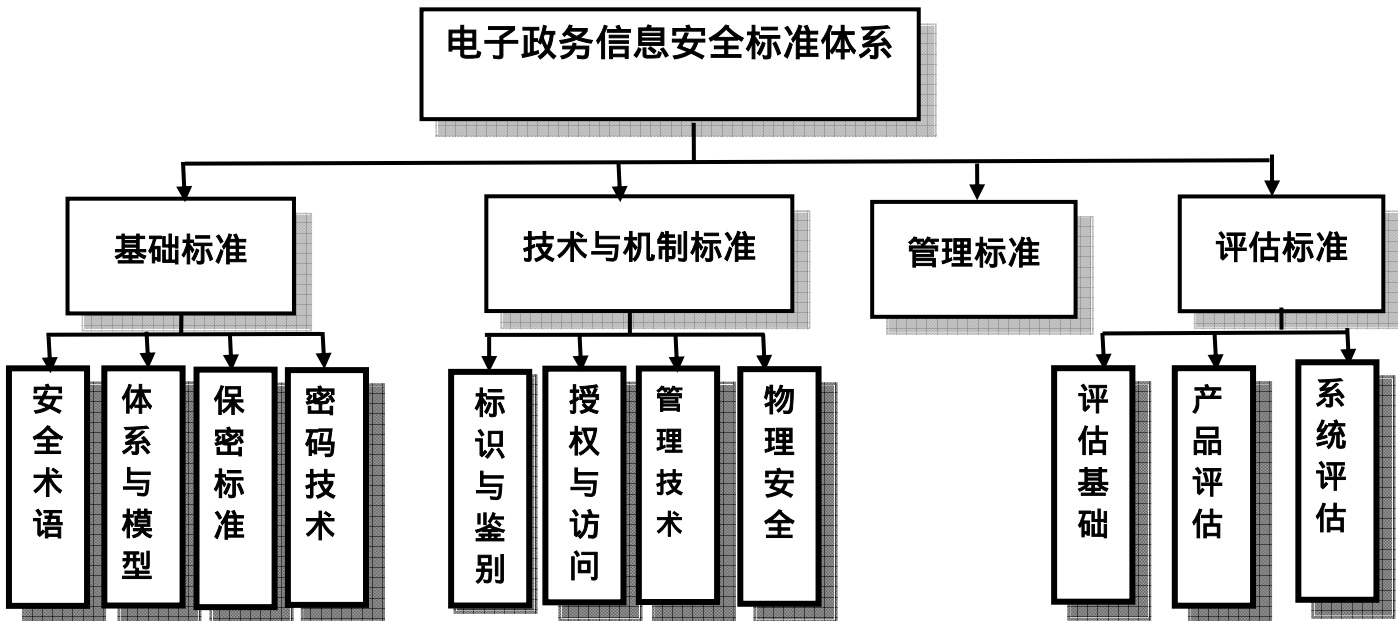


图 1 电子政务信息安全标准体系框架

基础标准分为安全术语、安全体系与模型标准、保密标准和密码技术标准4类。基础标准主要对信息安全领域最基本的内容进行约定，是其他信息安全标准制定、使用的基础。

技术与机制类标准分为标识与鉴别、授权与访问、管理技术、物理安全4类标准。技术与机制类标准通过规定信息安全相关技术领域的基本技术机制，为不同安全产品和系统的互操作性、兼容性、一致性奠定基础。技术与机制类标准一般不涉及具体的实现细节，而集中于对通用的、基础性的安全机制进行规定。

管理标准主要是对信息安全涉及的管理方面的安全措施进行规定。

评估标准则是根据安全产业的需求，针对安全产品与系统的技术要求与测评准则制定的标准。评估标准分为基础评估标准标准、安全产品评估标准和系统安全评估标准。

3、 国家保密标准与密码技术标准

在电子政务信息安全标准体系中，国家保密标准和密码技术标准是基础类标准中非常重要和核心的两类标准。

国家保密标准用于指导涉及国家秘密的信息系统中处理信息的安全保密所制定的保密防范和保密检查标准。所有涉及国家秘密的电子政务信息系统建设都必须按照国家保密标准的要求进行建设。

国家秘密信息对于国家安全和利益具有极端重要的意义，是国家信息安全保护的核心。涉密信息系统是处理国家秘密的信息系统，是关系到国家安全和利益的信息系统，是国家信息安全工作的重中之重。

国家保密标准分为技术标准和管理标准，技术标准主要包括电磁泄漏发射防护和检测、涉密信息系统技术要求和测评、安全保密产品技术要求和测试方法、涉密信息消除和介质销毁、其它技术标准（包括保密会议移动通信干扰器技术要求和测试方法、保密会议电子系统安全技术要求和测试方法等），管理标准主要包括电子文件管理、涉密信息系统管理、实验室要求等标准。现有的国家保密标准从技术和管理两方面涵盖了保密防范和保密检查工作所需，既包括了传统保密工作所需要的标准（如保密会议的安全要求、涉密信息消除和介质销毁、电子文件保密管理等），也包括了信息化和高技术发展条件下保密工作所需要的标准（如涉密信息系统技术要求和测评、信息安全保密产品技术要求和测试方法、涉密信息系统管理、TEMPEST防护和检测等）。

电子政务建设需要用到的国家保密标准主要包括电磁泄漏发射防护和检测、涉密信息系统技术要求和测评等技术标准，以及电子文件管理、涉密信息系统管理、电子政务保密管理指南等管理标准。

须引用密码办对密码技术标准在国家信息安全标准体系中的作用的描述，说明我国对密码技术的管理方法和控制措施，说明在电子政务建设过程中，要严格遵守国家有关密码技术的相关规定……

4、 标准明细表

4.1 基础标准 (52)

4.1.1 安全术语 (1)

标准编号	标准名称	对应国际标准	状态
GB/T 5271.8	信息技术 词汇 第8 部分：安全	ISO/IEC 2382-8	已发布

4.1.2 体系与模型 (17)

标准编号	标准名称	对应国际标准	状态
GB/T 9387.2-1995	信息处理系统 开放系统互连 基本参考模型 第2 部分：安全 体系结构	ISO 7498-2:1989	已发布
GB/T 17965-2000	信息技术 开放系统互连 高层 安全模型	ISO/IEC 10745 : 1995	已发布
GB/T 18237.1-2000	信息技术 开放系统互连 通用 高层安全 概述、模型和记法	ISO/IEC11586-1:19 96	已发布
GB/T 18237.2-2000	信息技术 开放系统互连 通用 高层安全 安全交换服务元素 (SESE) 服务定义	ISO/IEC11586-2:19 96	已发布
GB/T 18237.3-2000	信息技术 开放系统互连 通用 高层安全 安全交换服务元素 (SESE) 协议规范	ISO/IEC11586-3:19 96	已发布
GB/T 18237.4-2003	信息技术 开放系统互连 通用 高层安全 保护传送语法规范	ISO/IEC 11586-4:1996	已发布
GB/T 18231-2000	信息技术 低层安全	ISO/IECTR13594:1 995	已发布
GB/T 17963-2000	信息技术 开放系统互连 网络 层安全协议	ISO/IEC 11577:1995	已发布
GB/T 16264.8-2005	信息技术 开放系统互连 目录 第8部分：公钥和属性证书框架	ISO/IEC 9594-8	已发布
GB/T 18794.1-2002	信息技术 开放系统互连 开放系 统安全框架 第1部分:概述	ISO 10181-1:1996	已发布
GB/T 18794.2-2002	信息技术 开放系统互连 开放 系统安全框架 第2部分:鉴别框架	ISO 10181-2:1996	已发布
GB/T 18794.3-2003	信息技术 开放系统互连 开放 系统安全框架 第3部分:访问控 制框架	ISO 10181-3:1996	已发布
GB/T 18794.4-2003	信息技术 开放系统互连 开放系 统安全框架 第4部分:抗抵赖框	ISO 10181-4:1997	已发布

	架		
GB/T 18794.5-2003	信息技术 开放系统互连开放系统安全框架 第5部分：机密性框架	ISO 10181-5:1996	已发布
GB/T 18794.6-2003	信息技术 开放系统互连开放系统安全框架 第6部分：完整性框架	ISO 10181-6:1996	已发布
GB/T 18794.7-2003	信息技术 开放系统互连开放系统安全框架 第7部分：安全审计和报警框架	ISO10181-7:1996	已发布
GB/T 16264.8-1996	信息技术 开放系统互连 目录 第8部分：鉴别框架	ISO/IEC 9594-8:1997 ITU-T X.509	已发布

4.1.3 保密标准 (23)

标准编号	标准名称	对应国际标准	状态
	使用现场的信息设备电磁泄漏发射检查测试方法和安全判据		已发布
	涉密信息设备使用现场的电磁泄漏发射防护要求		已发布
	信息设备电磁泄漏发射限值		已发布
	信息设备电磁泄漏发射限值测试方法		已发布
	电磁干扰器技术要求和测试方法		已发布
	处理涉密信息的电磁屏蔽室的技术要求和测试方法		已发布
	密码设备电磁泄漏发射限值		已发布
	密码设备电磁泄漏发射测试方法(总则)		已发布
	电话密码机电磁泄漏发射测试方法		已发布
	电磁屏蔽机柜技术要求与测试方法		未发布
	红黑电源隔离防护产品技术要求和测试方法		未发布
	用于涉密信息系统的光端机的电磁泄漏发射限值和测试方法		未发布
	涉及国家秘密的计算机信息系统保密技术要求		已发布
	涉及国家秘密的计算机信息系统安全保密方案设计指南		已发布
	涉及国家秘密的计算机信息系统安全保密测评指南		已发布
	涉及国家秘密的信息系统分级保护技术要		未发布

	求		
	涉及国家秘密的信息系统分级测评准则		未发布
	涉及国家秘密的计算机信息系统数据备份要求		未发布
	涉及国家秘密的计算机信息系统应急响应要求		未发布
	电子文件密级标识格式规范		已发布
	涉及国家秘密的信息系统分级管理规范		未发布
	涉及国家秘密的信息系统工程监理规范		已发布
	电子政务保密管理指南		未发布

4.1.4 密码技术 (11)

标准编号	标准名称	对应国际标准	状态
GB/T 15277-1994	信息处理 信息技术 安全技术 N 位块密码算法的操作方式	ISO/IEC 10116 : 1997	已发布
GB/T 15278-1994	信息处理 数据加密 物理层互操作性要求		已发布
GB/T 18238.1-2000	信息技术 安全技术 散列函数 第1部分：概述	ISO/IEC 10118-1 : 1994	已发布
GB/T 18238.2-2002	散列函数 第2部分：使用R比特分组：加密算法的散列函数	ISO/IEC 10118-2 : 2000	已发布
GB/T 18238.3-2002	散列函数 第3部分：专用散列函数	ISO/IEC 10118-3 : 2004	已发布
GB 15852-1995	信息技术 安全技术 用块密码算法作密码校验函数的数据完整性机制	ISO/IEC 9797:1994	已发布
	分组算法应用接口规范		计划研制
	PCI密码卡技术规范		计划研制
	商用密码杂凑算法应用接口规范		计划研制
	椭圆曲线密码算法应用接口规范		计划研制
	证书认证系统密码及相关安全技术规范		计划研制

4.2 技术与机制标准 (44)

4.2.1 标识与鉴别 (11)

标准编号	标准名称	对应国际标准	状态
GB/T 15851-1995	信息技术 安全技术 带消息恢复的数字签名方案	ISO/IEC 9796:199	已发布
GB/T 17902.1-1999	信息技术 安全技术 带附录的数字签名 第1部分:概述	ISO/IEC 14888-1:1998	已发布
GB/T 17902.2-2005	信息技术 安全技术 带附录的数字签名 第2部分:基于身份的机制	ISO/IEC 14888-2:1999	已发布
GB/T 17902.3-2005	信息技术 安全技术 带附录的数字签名 第3部分:基于证书的机制	ISO/IEC 14888-3:1998	已发布
	XML数字签名语法与处理规范		计划研制
GB/Z 19717-2005	基于多用途互联网邮件扩展(MIME)的安全报文交换		已发布
GB/T 15843.1-1999	信息技术 安全技术 实体鉴别 第1部分:概述	ISO/IEC 9798-1:1991	已发布
GB/T 15843.2-1997	信息技术 安全技术 实体鉴别 第2部分:采用对称加密算法的机制	ISO/IEC 9798-2:1994	已发布
GB/T 15843.3-1998	信息技术 安全技术 实体鉴别 第3部分:用非对称签名技术的机制	ISO/IEC 9798-3:1997	已发布
GB/T 15843.4-1999	信息技术 安全技术 实体鉴别 第4部分:采用密码校验函数的机制	ISO/IEC 9798-4:1995	已发布
GB/T 15843.5-2005	信息技术 安全技术 实体鉴别 第5部分:使用零知识技术的机制	ISO/IEC 9798-5:2004	已发布

4.2.2 授权与访问 (17)

标准编号	标准名称	对应国际标准	状态
GB/T 17903.1-1999	信息技术 安全技术-抗抵赖 第1部分:概述	ISO/IEC 13888-1:1998	已发布
GB/T 17903.2-1999	信息技术 安全技术 抗抵赖 第2部分:使用对称技术的机制	ISO/IEC 13888-2:1998	已发布
GB/T 17903.3-1999	信息技术 安全技术 抗抵赖 第3部分:使用非对称技术的机制	ISO/IEC 13888-3:1998	已发布
GB/T	信息技术 安全技术 公钥基础设		已发布

19713-2005	施 在线证书状态协议		
GB/T 19714-2005	信息技术 安全技术 公钥基础设施 证书管理协议		已发布
GB/T 19771-2005	信息技术 安全技术 公钥基础设施 PKI组件最小互操作规范		已发布
	信息技术 安全技术 公钥基础设施 数字证书格式		即将颁布
	信息技术 安全技术 公钥基础设施 时间戳规范		即将报批
	信息技术 安全技术 CA认证机构建设和运营管理规则		即将报批
	信息技术 安全技术 安全支撑平台技术框架		即将报批
	信息技术 安全技术 权限管理中心技术规范		即将报批
	信息技术 安全技术 公钥基础设施 证书策略与认证业务声明框架		即将报批
	信息技术 安全技术 证书载体应用程序接口		即将报批
	信息技术 安全技术 CA密码设备应用程序接口		即将报批
	信息技术 安全技术 PKI应用支撑平台		即将报批
	信息技术 安全技术 公钥基础设施 简易在线证书状态协议		计划研制
	信息技术 安全技术 公开密钥基础设施 电子签名卡应用接口		计划研制

4.2.3 管理技术 (8)

标准编号	标准名称	对应国际标准	状态
GB/T 17143.1-1997	信息技术 开放系统互连 系统管理 第1部分:客体管理功能	ISO/IEC 10164-1 : 1993	已发布
GB/T 17143.2-1997	信息技术 开放系统互连 系统管理 第2部分:状态管理功能	ISO/IEC 10164-2 : 1993	已发布
GB/T 17143.3-1997	信息技术 开放系统互连 系统管理 第3部分:表示关系的属性	ISO/IEC 10164-3 : 1993	已发布
GB/T 17143.4-1997	信息技术 开放系统互连 系统管理 第4部分:告警报告功能	ISO/IEC 10164-4 : 1992	已发布
GB/T 17143.5-1997	信息技术 开放系统互连 系统管理 第5部分:事件报告管理功能	ISO/IEC 10164-5 : 1993	已发布
GB/T	信息技术 开放系统互连 系统	ISO/IEC 10164-6 :	已发布

17143.6-1997	管理 第6部分:日志控制功能	1993	
GB/T 17143.7-1997	信息技术 开放系统互连 系统 管理 第7 部分 :安全报警报告 功能	ISO/IEC 10164-7:1992	已发布
GB/T 17143.8-1997	信息技术 开放系统互连 系统 管理 第8 部分 :安全审计跟踪 功能	ISO/IEC 10164-8:1993	已发布

4.2.4 物理安全 (8)

标准编号	标准名称	对应国际标准	状态
GB/T 9361-1988	计算机场地安全要求		已发布
GB/T 2887-1989	计算机场地通用规范		已发布
GB 50174-1993	电子计算机机房设计规范		已发布
SJ/T 30003-1993	电子计算机机房施工及验收规范		已发布
GB 9254-1998	信息技术设备的无线电干扰极 限值和测量方法	CISPR 22: 1997	已发布
GB/T 17618-1998	信息技术设备抗扰度限值 和测量方法	CISPR 24:1997	已发布
GB 4943-2001	信息技术设备的安全	IEC 60950:1999	已发布
	信息安全等级保护 物理安全 技术要求		计划研制

4.3 信息安全管理 (11)

标准编号	标准名称	对应国际标准	状态
GB 17859-1999	计算机信息系统 安全保护等级 划分准则		已发布
GB/T 19715.1-2005	信息技术 信息技术安全管理指 南 第1部分 :信息技术安全概念 和模型	ISO/IEC TR 13335-1:1996	已发布
GB/T 19715.2-2005	信息技术 信息技术安全管理指 南 第2部分 :管理和规划信息技 术安全	ISO/IEC TR 13335-1:1996	已发布
GB/T 19716-2005	信息技术 信息安全管理实用规 则	ISO/IEC 17799:2000	已发布
	信息安全等级保护 信息系统安 全管理要求		即将报批
	信息安全等级保护 信息系统工 程管理要求		即将报批
	信息系统安全等级保护实施指南		计划研制

	信息安全风险评估指南		计划研制
	信息系统灾难恢复指南		计划研制
	网络与信息安全事件分类指南		计划研制
	信息技术 安全技术 信息安全事故管理		计划研制

4.4 评估标准 (34)

4.4.1 评估基础标准 (7)

标准编号	标准名称	对应国际标准	状态
GB/T 18336.1-2001	信息技术 安全技术 信息技术 安全性评估准则 第1 部分：简 介和一般模型	ISO/IEC 15408-1:1999	已发布
GB/T 18336.2-2001	信息技术 安全技术 信息技术 安全性评估准则 第2 部分：安 全功能要求	ISO/IEC 15408-2:1999	已发布
GB/T 18336.3-2001	信息技术 安全技术 信息技术 安全性评估准则 第3 部分：安 全保证要求	ISO/IEC 15408-3:1999	已发布
	保护轮廓和安全目标产生指南		即将报批
	信息系统安全保障评估框架		即将报批
	信息安全等级保护测评准则		计划研制
	信息技术安全通用评估方法		计划研制

4.4.2 产品评估标准 (23)

标准编号	标准名称	对应国际标准	状态
GB/T 17900-1999	网络代理服务器的安全技术要求		已发布
GB/T 18018-1999	路由器安全技术要求		已发布
GB/T 18019-1999	信息技术 包过滤防火墙安全技 术要求		已发布
GB/T 18020-1999	信息技术 应用级防火墙安全技 术要求		已发布
	操作系统安全保护等级评估准则		即将颁布
	数据库管理系统安全保护等级 评估准则		即将颁布
	路由器安全保护等级评估准则		即将颁布
	包过滤防火墙安全保护等级评 估准则		即将颁布
	信息安全等级保护 操作系统安		即将报批

	全技术要求		
	信息安全等级保护 数据库管理系统安全技术要求		即将报批
	智能卡嵌入式软件安全技术要求 (EAL4 增强级)		即将报批
	信息安全等级保护 隔离产品安全技术要求		即将报批
	信息安全等级保护 隔离产品评估准则		即将报批
	网络脆弱性扫描产品技术要求		即将报批
	网络脆弱性扫描产品测评方法		即将报批
	入侵检测系统技术要求和测评方法		即将报批
	防火墙技术要求和测评方法		即将报批
	虹膜特征鉴别技术要求		计划研制
	智能卡芯片安全技术要求 (EAL4 增强级)		计划研制
	信息技术 安全技术 交换机 安全技术要求 (EAL3增强级)		计划研制
	路由器安全等级保护技术要求		计划研制
	信息技术 审计跟踪产品技术要求		计划研制
	服务器安全技术要求		计划研制

4.4.3 系统评估标准 (4)

标准编号	标准名称	对应国际标准	状态
	信息安全等级保护 信息系统安全通用技术要求		即将报批
	信息安全等级保护网络安全基础技术要求		即将报批
	PKI系统安全等级保护技术要求		计划研制
	PKI系统安全等级保护评估准则		计划研制

第三章 关键标准说明与使用

1、 基础标准

1.1 术语

1) .GB/T 5271.8 信息技术 词汇 第8 部分：安全（等同采用ISO/IEC 2382-8）

本标准给出了与信息技术安全相关概念的基本术语及其定义，并明确了这些条目之间的关系。本标准适用于信息和数据安全保护方面的有关标准及国内外交流。

本标准详细定义了有关密码术、信息分类与信息访问控制、数据与信息的恢复和安全违规等数据与信息安全保护方面的术语及其定义，包括一般概念（共计31条）、信息分类（共计6条）、密码技术（共计16条）、访问控制（共计24条）、安全违规（共计52条）、敏感信息的保护（共计32条）、数据恢复（共计13条）、拷贝保护（共计14条）。

1.2 体系与模型

1) .GB/T 9387.2-1995 信息处理系统 — 开放系统互连 — 基本参考模型 — 第2 部分：安全体系结构（等同采用ISO 7498-2:1989）

本标准首先给出了安全方面的基本术语，描述了安全服务、特定的普遍性的安全机制，以及安全服务与安全机制之间的关系。详细规定了安全服务和安全机制与OSI各层之间的关系；安全服务和安全机制的配置，并分别规定了物理层、数据链路层、网络层、运输层、会话层、表示层和应用层的服务和机制；安全管理，包括OSI安全管理的分类（含系统安全、安全服务和安全机制管理）、特定的系统安全管理活动、安全机制的管理功能。标准以附录的形式给出了有关OSI中安全问题的背景信息、安全服务与安全机制配置的理由、应用选取加密的位置。

本标准确定了与安全体系结构有关的一般要素，它们能适用于开放系统之间需要通信保护的各种场合。为了安全通信而完善与开放系统互连相关的现有标准或开发新标准，本标准在参考模型的框架内建立起一些指导原则与制约条件，提供一个解决OSI安全问题的一致性方法。本标准的任务是：a. 提供安全服务与有关机制的一般描述，这些服务与机制可以为GB 9387-88参考模型所配备；b. 确定在参考模型内部可以提供这些服务与机制的位置。

本标准扩充了GB 9387-88的应用领域，包括了开放系统之间的安全通信。对基本的安全服务与机制以及它们的恰当配置按基本参考模型作了逐层说明。此外还说明了这些安全服务与机制对于参考模型而言在体系结构上的关系。在某些端系统、设备和组织结构中，可能还需要附加某些别的安全措施，这些措施也适用于各种不同的应用上下文中。确定为支持这种附加的安全措施所需要的安全服务不在本标准的工作范围之内。开放系统互连的安全功能仅仅涉及能让端系统之间进行信息的安全传送的通信通路的可见方面，不考虑在端系统、设备或组织内所需要的安全措施，除非牵连到在OSI中可见性安全服务的选择与定位。安全结构问题的这些方面也可以进行标准化，但不在OSI标准的工作范围之内。本标准对在GB9387-88中定义的概念与原则作了补充，但未改动它们。本标准既不是一个实施规范，也不是评价实际执行方案一致性的基准。

2).GB/T 17965-2000信息技术 开放系统互连 高层安全模型 (等同采用ISO/IEC 10745 : 1995)

本标准定义一个体系结构模型, 以此为基础: 开发OSI高层独立于应用的安全服务和协议; 利用这些服务和协议满足各种应用的安全要求, 以便使包含内部安全服务的应用特定的ASE的需求量最少。本标准特别规定: OSI高层中通信的安全, 高层中对开放系统OSI安全体系结构和安全框架中定义的安全服务的支持, 根据GB/T 9387.2和GB/T17176高层中安全服务和机制的放置及其之间的关系, 提供和使用安全服务时, 高层之间的交互及高层和低层之间的交互, 高层中管理安全信息的要求。在访问控制方面, 本标准的范围包括控制访问OSI资源和通过OSI可接近的资源的服务和机制。本标准不包括 OSI服务的定义或OSI协议的规范 安全技术和机制, 它们的操作及其协议要求的规范或与OSI通信无关的保证安全的内容。本标准既不是系统的实现规范也不是评价实现一致性的依据。

3) . GB/T 18237.1-2000 信息技术 开放系统互连 通用高层安全 概述、模型和记法 (等同采用ISO/IEC 11586-1:1996)

本标准定义了一组用于辅助在OSI应用中提供安全服务的通用设施。它们包括: 1、一组记法工具, 这组工具支持抽象语法规则中的选择字段保护需求的规范, 并支持安全交换和安全变换规范; 2、应用服务元素 (ASE) 的服务定义、协议规范和PICS形式表, 他们支持在OSI的应用层内提供安全服务; 3、安全传送语法的规范和PICS形式表, 这些语法与支持应用层中的安全服务表示层相关。本标准定义了如下内容: 1、基于OSI高层安全模型 (GB/T17965) 中描述的概念的安全交换协议功能和安全变换的通用模型; 2、一组记法工具, 这组工具支持抽象语法规则中的选择字段保护需求的规范, 并支持安全交换和安全变换规范; 3、由本系列标准包含的通用高层安全设施的应用方面的一组信息性指南。本标准没有定义如下内容: 1、可能由其他标准要求的一组完备的高层安全设施; 2、适于特定应用的一组完备的安全设施; 3、用作支持安全服务的机制。安全交换模型和支持记法既打算用作定义本系列标准所属各部分中的安全交换服务元素的基础, 又用于欲将安全交换引入到其自身规范的任何其他ASE。

4).GB/T 18237.2-2000 信息技术 开放系统互连 通用高层安全 安全交换服务元素 (SESE) 服务定义 (等同采用ISO/IEC 11586-2:1996)。

本标准定义了一组用于辅助在OSI应用中提供安全服务的通用设施。它们包括: 1、一组记法工具, 这组工具支持抽象语法规则中的选择字段保护需求的规范, 并支持安全交换和安全变换规范; 2、应用服务元素 (ASE) 的服务定义、协议规范和PICS形式表, 他们支持在OSI的应用层内提供安全服务; 3、安全传送语法的规范和PICS形式表, 这些语法与支持应用层中的安全服务表示层相关。本标准定义了由安全交换服务元素 (SESE) 提供的服务。该SESE是一个允许安全信息通信以支持在应用层内提供安全服务的ASE。

5).GB/T 18237.3-2000 信息技术 开放系统互连 通用高层安全 安全交换服务元素 (SESE) 协议规范 (等同采用ISO/IEC 11586-3:1996)。

本标准定义了一组用于辅助在OSI应用中提供安全服务的通用设施。它们包括: 1、一组记法工具, 这组工具支持抽象语法规则中的选择字段保护需求的规范, 并支持安全交换和安全变换规范; 2、应用服务元素 (ASE) 的服务定义、协议规范和PICS形式表, 他们支持在OSI的应用层内提供安全服务; 3、安全传送语法的规范和PICS形式表, 这些语法与支持应用层中的安全服务表示层相关。本标准定义了由安全交换服务元素 (SESE) 提供的协议。该SESE是一个允许安全信息通信以支持在应用层内提供安全服务的ASE。

6). GB/T 18237.4-2003 信息技术 开放系统互连 通用高层安全 保护传送语法规范 (等同采用ISO/IEC 11586-4:1996)

7). GB/T 18231-2000 信息技术 低层安全 (等同采用ISO/IEC TR 13594:1995)

本标准描述了在OSI参考模型低层(运输、网络、数据链路和物理层)中提供安全服务的跨层的内容。本标准描述:1、基于GB/T9387.2中定义的低层公共的体系结构概念;2、低层协议之间与安全有关的交互作用的基础;3、OSI的低层与高层之间与安全有关的任何交互作用的基础;4、与其他低层安全协议有关的安全协议的放置以及这种放置的有关作用。在低层安全协议和本标准中描述的模型之间不应该存在冲突。

8).GB/T 17963-2000 信息技术 开放系统互连 网络层安全协议 (等同国际标准ISO/IEC 11577:1995)

本标准规定的协议将由端系统和中间系统使用,以在网络层提供安全服务,而网络层由GB/T15126和GB/T15274定义。本标准中定义的协议称为网络层安全协议(NLSP)本标准规定:

a).支持GB/T9387.2中定义的下列安全服务:

- 对等实体鉴别;
- 数据原发鉴别;
- 访问控制;
- 连接保密性;
- 无连接保密性;
- 通信流量保密性;
- 无恢复的连接完整性(包括数据单元完整性,其中连接上的各个SDU具有完整性保护);
- 无连接完整性。

b).声称与本标准一致的实现的功能要求。

本协议规程依据下列定义:

1. 可用于本协议实例的加密技术的要求;
2. 用于通信实例安全联系中携带信息的要求;
3. 尽管一些安全机制提供的保护程度取决于一些特定的加密技术,而本协议的正确操作并不取决于某种特定的加密或解密算法的选择,这是通信系统的本地事情。

此外,特定的安全策略的选择和实现都不在本标准的范围之内。特定的安全策略的选择以及因此将达到的保护程度,留作使用安全通信的单个实例的系统之间的本地事情。本标准不要涉及同一开放系统的多个安全通信的实例必须采用相同的协议。

9).GB/T 16264.8-2005 信息技术 开放系统互连 目录 第8部分:公钥和属性证书框架 (等同采用ISO/IEC 9594-8)

本标准描述了一套作为所有安全服务基础的框架,并规定了在鉴别及其它服务方面的安全要求。

10). GB/T 18794.1-2002信息技术 开放系统互连开放系统安全框架 第1部分:概述(等同采用ISO 10181-1:1996)

11). GB/T 18794.2-2002信息技术 开放系统互连 开放系统安全框架 第2部分:鉴别框架(等同采用ISO 10181-2:1996)

12). GB/T 18794.3-2003信息技术 开放系统互连 开放系统安全框架 第3部分:访问控制框架(等同采用ISO 10181-3:1996)

13). GB/T 18794.4-2003 信息技术 开放系统互连 开放系统安全框架 第4部分：抗抵赖框架（等同采用 ISO/IEC 10181-4：1997）

本开放系统互连安全框架的标准论述在开放系统环境中安全服务的应用，此处“开放系统”包括诸如数据库、分布式应用、开放分布式处理和开放系统互连这样一些领域。安全框架涉及定义对系统和系统内的对象提供保护的方法，以及系统间的交互。本安全框架不涉及构建系统或机制的方法学。本部分定义抗抵赖的基本概念，定义通用的抗抵赖服务，确定提供抗抵赖服务的可能的机制，确定抗抵赖服务和机制的通用管理需求。本部分不包括实现抗抵赖所需要完成的协议交换的细节说明，不详细描述可用于支持抗抵赖服务的特定机制，也不给出所支持的安全管理服务 and 协议的细节。在本框架中描述的某些规程通过应用密码技术实现安全。

14). GB/T 18794.5-2003 信息技术 开放系统互连 开放系统安全框架 第5部分：机密性框架（等同采用 ISO/IEC 10181-5：1996）

本部分阐述在检索、传送和管理过程中信息的机密性。本部分定义机密性的基本概念，识别可能的机密性机制类型，对每种机密性机制的设施进行分类和识别，识别用来支持各种类别的机密性机制所需的管理，阐述机密性机制和支持服务与其他安全服务和机制的交互。许多不同类型的标准能使用这个框架，其中包括，体现机密性概念的标准；规定含有机密性的抽象服务的标准；规定使用机密性服务的标准；规定在开放系统体系结构内机密性服务的提供方法的标准，规定机密性机制的标准。本安全框架中所描述的有些规程，通过应用密码技术来实现机密性。但本框架与特定的密码技术或其他算法的使用并无以来关系，当然某些类别的机密性机制可能要依靠特殊的算法特性。

15). GB/T 18794.6-2003 信息技术 开放系统互连 开放系统安全框架 第6部分：完整性框架（等同采用 ISO/IEC 10181-6：1996）

本部分阐述信息检索，传送及管理数据的完整性，定义数据完整性的基本概念；识别可能的完整性机制分类，识别每一类完整性机制的设施，识别支持完整性机制分类所需的管理；阐述完整性机制和支持服务与其他安全服务和机制的交互。许多不同类型的标准能使用这个框架，其中包括，体现完整性概念的标准；规定含有完整性的抽象服务的标准；规定使用完整性服务的标准；规定在开放系统体系结构内完整性服务的提供方法的标准，规定完整性机制的标准。本部分论述的完整性是通过数据值的不变性来定义的。本框架阐述给那些被认为可被潜在攻击者写访问的数据提供完整性。因此它着重于通过密码和非密码的机制提供完整性，并非专门依赖于控制访问。

16). GB/T 18794.7-2003 信息技术 开放系统互连 开放系统安全框架 第7部分：安全审计和报警框架（等同采用 ISO/IEC 10181-7：1996）

本部分所述安全审计和报警的目的是确保按照安全机构适当的安全策略处理与开放系统安全有关的事件，特别是本框架定义安全审计和报警的基本概念，为安全审计和报警提供一个通用的模型，识别安全审计和报警服务与其他安全服务的关系。和其他安全服务一样，安全审计只能在规定的策略范围内提供。许多不同类型的标准能使用这个框架，其中包括，体现审计和报警概念的标准；规定含有审计和报警的抽象服务的标准；规定使用审计和报警的标准；规定在开放系统体系结构内提供审计和报警方法的标准，规定审计和报警机制的标准。

17). GB/T 16264.8-1996 信息技术 开放系统互连 目录 第8部分：鉴别框架（等同采用 ISO/IEC 9594-8:1997|ITU-T X.509）

1.3 保密标准

1.3.1 电磁泄漏发射防护和检测标准

1).使用现场的信息设备电磁泄漏发射检查测试方法和安全判据

本标准在现场测试标准。规定了对涉密部门和会议场所使用的各种信息设备(如计算机、传真机、打印机、扩音设备等)的电磁泄漏发射现场检查测试结果,研究并提出被测设备的使用安全判据。其主要内容是根据测得红信号的最大信噪比计算被测设备的安全距离,适用于对信息设备的现场检测。

2).信息设备电磁泄漏发射限值

本标准对低泄射类信息设备实验室测试标准。本标准对各种低泄射信息设备(如计算机、传真机、打印机等)所应达到的技术指标提出详细的要求,研究并规定低泄射信息设备电磁泄漏辐射发射、传导发射的限值、测试场地要求以及等级划分、安全使用距离等,适用于党政机关、重要企事业单位的涉密部门使用的低泄射信息设备。

3).信息设备电磁泄漏发射测试方法

本标准对低泄射类信息设备实验室测试标准。本标准针对低泄射信息设备的电磁泄漏辐射发射、传导发射等各项技术指标,研究目前国内无宽带接收机情况下的等效测试方法、红黑信号识别方法以及各类信息设备的测试状态。该标准适用于党政机关、重要企事业单位的涉密部门使用的低泄射信息设备。

4).处理涉密信息的电磁屏蔽室的技术要求和测试方法

本标准是针对电磁屏蔽室的测试标准。本标准对内部含有涉密信息设备的屏蔽室应具备的技术指标提出明确要求,规定了电磁屏蔽室的电磁场屏蔽效能要求、传导泄漏发射抑制要求,以及测试方法。该标准对电磁屏蔽室的等级划分和安全使用距离进行了规定,适用于保护涉密信息设备的屏蔽室的保密性能检测。

5).电磁干扰器技术要求和测试方法

适用于电磁干扰器的设计与评测。本标准是针对电磁干扰器性能测试的实验室测试标准,对电磁干扰器提出技术要求,对电磁干扰器电磁泄漏辐射发射防护、传导发射防护、抗还原性以及等级划分等方面制定了测试方法。

6).涉密信息设备使用现场的电磁泄漏发射防护要求

本标准对涉密信息设备的选择、使用和系统安装提出了体的要求。

7).红黑电源隔离防护产品技术要求和测试方法

对涉密信息系统的红黑电源隔离防护产品提出技术要求和测试方法,规范该产品的研制和应用。

8).用于涉密信息系统的光端机电磁泄漏发射限值和测试方法

提出用于涉密信息系统中屏蔽机房和机柜的光端机的电磁泄漏发射的限值要求和测试方法。主要技术内容:制定该类产品的光电转换界面引起的电磁泄漏发射(如:电场和磁场辐射发射的频率范围、发射强度等、通信线和电源线的传导发射的频率范围、发射强度等)的限值要求,并提出测试方法。

1.3.2 涉密信息系统技术要求和测评标准

1).涉及国家秘密的计算机信息系统保密技术要求

适用于涉密信息系统的安全保密设计、建设。本标准从物理安全、运行安全、信息安全保密、安全保密管理等四个方面规定了涉密信息系统的安全保密技术要求。

2). 涉及国家秘密的计算机信息系统安全保密方案设计指南

本标准规定了涉及国家秘密的计算机信息系统安全保密方案包括的系统分析、脆弱性分析和威胁分析、风险分析、安全保密系统设计、安全保密技术和措施、安全保密产品的选型原则、安全保密产品与设施的选型和依据、安全保密系统配置方案、安全保密管理措施、安全保密建设实施计划和安全保密系统的经费概算等主要内容,可用于指导涉密系统安全保密方案的设计。

3). 涉及国家秘密的计算机信息系统安全保密测评指南

本标准规定了涉及国家秘密的计算机信息系统安全保密测评准则,适用于评测机构对涉密信息系统的安全保密性进行测评,以及保密部门对涉密系统的安全保密性进行检查,并指导用户和承建单位建设满足安全保密要求的涉密系统。

4). 涉及国家秘密的信息系统分级保护技术要求

本标准规定涉密信息系统的等级划分和相应等级的安全保密技术要求,适用于涉密信息系统的建设单位、设计单位、承建单位建设符合分级保护要求的涉密信息系统,并可用于保密工作部门对涉密信息系统的管理和审批。本标准将替代《涉及国家秘密的计算机信息系统保密技术要求》。

5). 涉及国家秘密的信息系统分级测评准则

本标准根据涉密信息系统的等级划分和相应等级的安全保密技术要求,制定涉密信息系统的分等级的安全保密测评准则,适用于评测机构对涉密信息系统的安全保密性进行测评,以及保密部门对涉密信息系统的安全保密性进行检查,并指导用户和承建单位建设满足安全保密要求的涉密信息系统。本标准将替代《涉及国家秘密的计算机信息系统安全保密测评指南》。

6). 涉及国家秘密的信息系统数据备份要求

本标准根据涉密信息系统的密级和重要性,研究制定涉密信息系统数据备份要求,主要包括数据备份的技术要求、管理要求、安全保密要求。用于指导涉及国家秘密的信息系统中数据备份系统的组建及相关产品的研制、开发。

7). 涉及国家秘密的信息系统应急响应要求

本标准主要根据涉密信息系统的密级和重要性,研究制定涉密信息系统应急响应要求,主要包括应急响应的组成环节和体系结构、每一环节和总体的技术指标、应急响应的管理要求。用于指导涉及国家秘密的信息系统中应急响应系统的组建及相关产品的研制、开发。

1.3.3 电子文件管理标准

1). 电子文件密级标识格式规范

本标准规定电子文件的密级标识格式,可用于传输或使用中的涉密电子文件及数据的密级管理。该标准对电子文件密级标识的格式构成、电子文件密级标识的基本属性、电子文件密级标识的认证方式、电子文件密级划分、电子文件数据操作特性等方面提出了要求。

1.3.4 涉密信息系统管理标准

1). 涉及国家秘密的信息系统工程监理规范

本标准根据涉密信息系统的密级和重要性,制定不同安全级别涉密信息工程监理规范,适用于涉及国家秘密的信息系统工程新建、扩建、改建施工、设备采购和制造的监理工作。主要内容包括:(1)涉密系统工程项目监理机构的结构、职责、权力及义务;(2)涉密信息系统的监理规划及监理实施细则;(3)涉密系统工程新建、扩建、改建施工过程的监理内容;(4)涉密系统工程中设备采购和制造的监理内容。

2). 涉及国家秘密的信息系统分级管理规范

本标准规定涉密信息系统基本的安全保密管理规则,适用于涉密信息系统的使用单位对涉密信息系统实施安全保密管理,也可用于保密工作部门或机构对涉密信息系统的安全保密管理进行检查和指导。该标准对安全保密策略、安全保密管理机构、信息的分类与控制、人员的安全保密、环境与设备的安全保密、系统建设的安全保密管理、系统运行与维护的安全保密管理等方面研究提出管理要求。

3). 电子政务保密管理指南

用于指导电子政务建设过程中遇到的保密问题,确保国家秘密的安全,促进我国电子政务的健康发展。

1.4 密码技术

1). GB/T 15277-1994 信息处理 信息技术 安全技术 N位块密码算法的操作方式,(等同国际标准ISO/IEC 10116:1997)。

本标准描述N位块密码算法的四种操作方式。

本标准确定了四种规定的操作方式,以便在N位块密码的应用中(如数据传输的保护,数据存储、鉴别)本标准对诸如操作方式规范和适用的参数值提供一个有用的参照。

2). GB/T 15278-1994信息处理 数据加密 物理层互操作性要求

3). GB/T 18238.1-2000 信息技术 安全技术 散列函数 第1部分:概述(等同国际标准ISO/IEC 10118-1:1994)

本标准定义了散列函数,它可用于提供鉴别、完整性和抗抵赖服务。本标准包含GB/T 18238各个部分所共用的定义、符号、缩略语和要求

4). GB/T 18238.2-2002散列函数 第2部分:使用R比特分组:加密算法的散列函数(等同国际标准ISO/IEC 10118-2:2000)

5) GB/T 18238.3-2002散列函数 第3部分:专用散列函数(等同国际标准ISO/IEC 10118-3:2004)

6). GB 15852-1995 信息技术 安全技术 用块密码算法作密码校验函数的数据完整性机制(等同国际标准ISO/IEC 9797:1994)。

本标准规定了一种使用密钥和N比特块密码算法计算M比特密码校验值的方法。这种方法可用作数据完整性机制,以检测数据是否已被非授权地改变。这种数据完整性机制的强度依赖于密钥长度及其保密性,依赖于密码算法的特性以及校验值的长度M。本标准适用于任何安全体系结构、进程或应用的安全服务。

7). 分组算法应用接口规范(计划研制)

商用密码分组算法标准 第2部分 工作模式:

本部分规定商用密码分组算法的填充方式、ECB工作模式、CBC工作模式、CFB工作模式、OFB工作模式和CBC MAC计算的方法,给出对每一种工作模式性质的简要评述和每一种工作模式和MAC值计算的实例。本部分适用于商用密码领域。

商用密码分组算法标准第3部分 芯片接口:

本部分给出商用密码分组算法标准低速、中速、高速三类芯片的接口信号定义、地址定义、接口时序和操作流程。本部分适用于商用密码领域。

商用密码分组算法标准 第4部分 IP核接口：

本部分给出商用密码分组算法标准IP核接口的信号定义、接口时序和应用流程。本部分适用于商用密码领域。

8). PCI密码卡技术规范（计划研制）

本规范定义PCI密码卡的相关术语,规定PCI密码卡的功能要求、硬件要求、软件要求(含应用接口要求)、安全性要求(含密钥结构)、检测要求等有关内容。

本规范适用于计算机设备、通信设备或安全保密设备等使用的PCI密码卡；目的是为了**保证PCI密码卡基本技术规格的一致性，有利于不同厂家产品的互联互通，并力求对基础密码算法透明，便于用户的选择和使用，便于主管部门的统一测评、认证和管理。**

9).商用密码杂凑算法应用接口规范（计划研制）

本规范给出商用密码杂凑算法杂凑算法的运算实例；接口的信号定义、地址定义和操作流程，调用范例等等。本规范适用于商用密码领域

10).椭圆曲线密码算法应用接口规范（计划研制）

本规范给出椭圆曲线密码算法算法初始化接口、密钥生成接口、加解密接口、签名验证接口、密钥协商接口、椭圆曲线点预计算接口、倍乘接口、抽象层次接口、高级计算机语言编程接口、硬件调用接口等。本规范适用于商用密码领域

11).证书认证系统密码及相关安全技术规范（计划研制）

本标准适用于在中华人民共和国境内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，为实现数字证书认证系统的互连互通和交叉认证提供统一的依据，指导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。其他的数字证书认证系统的建设、运行及管理，可参照本标准

2、技术与机制标准

2.1 标识与鉴别

1).GB/T 15851-1995 信息技术 安全技术 带消息恢复的数字签名方案(等同国际标准ISO/IEC 9796:1991)。

本标准规定了对有限长消息使用公开密钥体制的带消息恢复的数字签名方案。这种数字签名方案包含下列两个进程：

--签名进程，它使用秘密签名密钥和签名函数来对消息签名；

--验证进程，它使用公开验证密钥和验证函数来验证签名，同时恢复出消息。签名进程中，必要时，欲签名的消息需填充和扩展，然后加上与消息本身有关的人为的冗余，对消息中是否存在自然的冗余不作假定。这人为的冗余将由验证进程揭示出来，把这人为的冗余去掉便恢复出消息。本标准不规定密钥产生进程，签名函数和验证函数。

2).GB/T 17902.1-1999 信息技术 安全技术 带附录的数字签名 第1部分：概述（等同国际标准ISO/IEC 14888-1:1998）

系列标准GB/T 17902 规定了几个任长度消息的带附录的数字签名机制。该标准是系列标准17902的第一部分，描述带附录的数字签名的基本原则和要求以及该系列标准通用的定义和符号。它适用于带附录的数字签名方案。本标准适用于提供实体鉴别、数据原发鉴别、数据完整性和抗抵赖的方案。

该标准所规定的机制是基于非对称密码技术，所有非对称数字签名机制都涉及密钥对产生、密钥签名和验证密钥三个基本操作（进程）。标准给出了数字签名机制的一般模型，并对三个进程进行了详细规定，其中，密钥产生进程由产生域参数与产生签名密钥和验证密钥组成；对签名进程规定了数据项和验证过程，这些验证过程包括产生预签名、准备消息、计算证据、计算签名；对验证进程规定了数据项和验证过程，这些验证过程包括准备消息、检索证据、计算验证函数、验证证据；还规定了带两部分签名的随机化机制。标准以附录的形式给出了绑定签名机制和散列函数的安全性注释。

3).GB/T 17902.2-2005 信息技术 安全技术 带附录的数字签名 第2部分：基于身份的机制（等同国际标准ISO/IEC 14888-2:1999）

该标准所规定的机制是基于非对称密码技术，所有非对称数字签名机制都涉及密钥对产生、密钥签名和验证密钥三个基本操作（进程）。数字签名的验证需要签名实体的验证密钥。该标准的验证密钥与签名实体有关联，故被称作“基于身份的”。

标准给出了数字签名机制的一般模型，并对三个进程进行了详细规定，其中，密钥产生进程由产生域参数与产生签名密钥和验证密钥组成；对签名进程规定了数据项和验证过程，这些验证过程包括产生预签名、准备消息、计算证据、计算签名；对验证进程规定了数据项和验证过程，这些验证过程包括准备消息、检索证据、计算验证函数、验证证据；Guillou-Quisquater签名机制，包括公钥导出函数、准备消息、计算证据、计算签名的第一部分、计算赋值；带短赋值的基于身份的签名，包括准备消息、计算证据、计算赋值；带消息散列码检索的基于身份的签名，包括计算证据、计算签名的第一部分。标准以附录的形式给出了多种数值的例子。

4).GB/T 17902.3-2005 信息技术 安全技术 带附录的数字签名 第3部分：基于证书的机制（等同国际标准ISO/IEC 14888-3:1998）

该标准所规定的机制是基于非对称密码技术，所有非对称数字签名机制都涉及密钥对产生、密钥签名和验证密钥三个基本操作（过程）。数字签名的验证需要签名实体的验证密钥。该标准的验证密钥必须通过某种证书的方式提供，故被称作“基于证书的”。

标准给出了数字签名机制的一般模型，并对三个进程进行了详细规定，其中，密钥产生进程由产生域参数与产生签名密钥和验证密钥组成；规定了基于离散对数的数字签名机制和基于因子分解的数字签名机制，并对这两种机制分详细规定了密钥生成过程、签名过程和验证过程。标准以附录的形式给出了基于离散对数和基于因子分解的带附录的基于证书的数字签名的例子、椭圆曲线数学背景、带附录的基于证书的数字签名的数值例子所选签名方案具有的特性。

5).XML数字签名语法与处理规范（计划研制）

本规范详细描述使用XML语法和处理规则来创建和表示数字签名的机制。XML签名技术可以应用到任何数字内容（数据对象），还可以包括XML本身。一个XML Signature可以用于一个或者多个资源的内容。Enveloped或者Enveloping Signature作用于和签名在同一XML文档中的所有数据；Detached Signature作用于签名元素以外的所有数据。更具体的说，本规范定义一个XML签名元素类型并且定义一个XML签名应用程序；我们以Schema定义和缩进的方式给出每种要求的规范性的详细说明。本规范还包括了其他一些有用的类型，这些类型（type）用来标识引用资源集合、算法和密钥及管理信息的方法。

XML Signature是一种将引用的数据（字节序列）和密钥关联在一起的方法。它并没有以标准化的方式规定了密钥如何与人或机构相联系，也没有规定被引用和签名的数据的含义。因此，尽管本规范是安全XML应用程序的一个重要组成部分，它本身并不能详细到涵盖

所有应用程序的安全和信任问题，尤其没有涉及使用签名的XML（或其他数据格式）作为一个人与人之间通信和协商的基础这种应用。它必须指定附加的密钥，算法，处理和生成需求。

6).GB/Z 19717-2005 基于多用途互联网邮件扩展（MIME）的安全报文交换

本标准阐述了安全发送和接收多用途Internet邮件扩展（MIME）数据的基本方法。

7).GB/T 15843.1-1999 信息技术 安全技术 实体鉴别 第1部分：概述（等同国际标准ISO/IEC 9798-1:1991）

本标准规定了采用安全技术的实体鉴别机制的鉴别模型及一般要求和限制。这些机制用于证实某个实体就是他所声称的实体。待鉴别的实体，通过表明他确实知道某个秘密来证明其身份。这些机制定义为实体间的信息交换。若有必要，还可以同可信的第三方进行交换。这些机制的详细情况和鉴别交换的内容未在本标准中规定，而在GB/T15843的其他部分中规定。GB/T15843其他各部分规定的机制能用于帮助提供在ISO/IEC 13888中规定的抗抵赖服务。抗抵赖服务的有关内容不在GB/T15843范围之内。

8).GB/T 15843.2-1997 信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制（等同国际标准ISO/IEC 9798-2:1994）

本标准规定了对称加密算法的实体鉴别机制。其中有四种是两个实体间无可信第三方参与的鉴别机制，而这四种机制中有两种是单个实体鉴别（单向鉴别），另两种是两个实体相互鉴别。其余的机制都要求有一个可信第三方参与，以便建立公共的秘密密钥，实现相互或单向的实体鉴别。本标准中规定的机制采用诸如时间标记，顺序号或随机数等时变参数，防止先前有效的鉴别信息以后又被接受。如果没有可信第三方参与，又采取使用随机数的询问-应答方法时，单向需传送两次信息，而相互鉴别则需要传送三次。如果有可信第三方参与，则一个实体与可信第三方之间的任何一次附加通信都需要在通信交换中增加两次传送。

9).GB/T 15843.3-1998 信息技术 安全技术 实体鉴别 第3部分：用非对称签名技术的机制（等同国际标准ISO/IEC 9798-3:1997）

本标准规定了用非对称鉴别技术的实体鉴别机制。两种鉴别机制属单个实体（单向）的鉴别，期于的属两个实体相互鉴别的机制。数字简明用于验证实体的身份，也有可能可信的第三方参与。本标准规定的机制，使用时变参数，如：时间标记、顺序号或随机数，可防止先前有效的鉴别信息以后又被接受。若使用时间标记或顺序号，则单向鉴别只需要一次传递，而完成相互鉴别则需两次传递。若使用带有随机数的询问和响应方法，则单向鉴别需要两次传递，而当完成相互鉴别，则需要三次或四次传递（依赖于所使用的机制）

10).GB/T 15843.4-1999 信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制（等同国际标准ISO/IEC 9798-4:1995）

本标准规定了采用密码校验函数的实体鉴别机制。其中两个是单个实体的鉴别（单向鉴别），其余的是两个实体的互相鉴别。本标准所规定的机制采用诸如时间标记，顺序号或随机数等时变参数，以防止有效的鉴别信息以后又被接受。如果采用时间标记或顺序号，对于单向鉴别只需一次传递，而要达到相互鉴别则需两次传递。如果采用了使用随机数的询问和应答方法，单向鉴别需两次传递，而达到相互鉴别需要三次传递。

11).GB/T 15843.5-2005 信息技术 安全技术 实体鉴别 第5部分：使用零知识技术的机制(等同国际标准ISO/IEC 9798-5:2004)

本部分详细说明了三种使用零知识技术的实体鉴别机制。所有在ISO/IEC 9798本部分中阐述的机制都提供单向鉴别。这些机制应用零知识的原理所构造，但是根据附录A所勾画的严格定义，对所有参数的选择，这些机制本身并不是零知识的。

2.2 授权与访问

1).GB/T 17903.1-1999 信息技术 安全技术-抗抵赖 第1 部分：概述（等同国际标准 ISO/IEC 13888-1:1998）

抗抵赖服务旨在生成、收集、维护有关已声明的事件或动作的证据，并使该证据可得并且确认该证据。以此来解决关于此事件或动作发生或未发生而引起的争议。本标准描述了基于密码技术提供证据的抗抵赖机制的一种模型，并且描述了如何适应对称或非对称密码技术生成校验值并以此形成证据。首先描述的是通用于不同抗抵赖服务的抗抵赖机制，然后将这些抗抵赖机制应用于一系列的特殊抗抵赖服务，如：原发抗抵赖，交付抗抵赖，提交抗抵赖，传输抗抵赖。抗抵赖生成证据，证据用于确定某事件或动作的责任。就产生证据所针对的动作或事件而言，对该动作负责或与事件相关的实体，称为证据主体。主要有两类证据，从本质上讲他们都依赖于所使用的密码技术。本标准可作为其他几部分中，规定使用密码技术的抗抵赖机制时的一般模型。GB/T 17903为以下抗抵赖阶段提供抗抵赖机制：证据生成，证据传输、存储和检索、证据验证。

2).GB/T 17903.2-1999 信息技术 安全技术 抗抵赖 第2 部分：使用对称技术的机制（等同国际标准ISO/IEC 13888-2:1998）

本标准利用可信第三方防止抵赖的发生，一般需要在线的可信第三方。抗抵赖机制提供专用于每一个抗抵赖服务的抗抵赖权标的交换协议。抗抵赖权标由安全信封和附加数据组成。抗抵赖权标应作为抗抵赖信息予以存储，以后发生争议时使用。按照特殊应用下所使用抗抵赖策略以及该应用所处的合法环境，抗抵赖信息可能包括以下附加信息：1、包括一个由时间标记机构所生成的可信时间标记的证据；2、公证人提供的证据，为一个或多个实体执行的动作或事件提供保证。抗抵赖一词只能在特定的应用及其合法环境所清晰定义的安全策略中才可以有效。

3).GB/T 17903.3-1999 信息技术 安全技术 抗抵赖 第3 部分：使用非对称技术的机制（等同国际标准ISO/IEC 13888-3:1998）

本标准利用可信第三方防止抵赖的发生，一般需要在线的可信第三方。抗抵赖机制提供专用于每一个抗抵赖服务的抗抵赖权标的交换协议。抗抵赖权标由安全信封和附加数据组成。抗抵赖权标应作为抗抵赖信息予以存储，以后发生争议时使用。按照特殊应用下所使用抗抵赖策略以及该应用所处的合法环境，抗抵赖信息可能包括以下附加信息：1、包括一个由时间标记机构所生成的可信时间标记的证据；2、公证人提供的证据，为一个或多个实体执行的动作或事件提供保证。抗抵赖一词只能在特定的应用及其合法环境所清晰定义的安全策略中才可以有效。

4).GB/T 19713-2005 信息技术 安全技术 公钥基础设施 在线证书状态协议

本标准规定了一种无需请求证书撤销列表（CRL）即可查询数字证书状态的机制（即在线证书状态协议—OCSP）。该机制可代替CRL或作为周期性检查CRL的一种补充方式，以便及时获得证书撤销状态的有关信息。

5).GB/T 19714-2005 信息技术 安全技术 公钥基础设施 证书管理协议

本标准描述了公钥基础设施（PKI）中的证书管理协议，定义了与证书产生和管理相关的各方面所需要的协议消息，这些消息主要包括申请证书、撤销证书、密钥更新、密钥恢复、交叉认证等。

本标准主要适用于在安全或不安全环境中实施PKI组件并实施管理，可作为PKI运营机构、PKI组件开发者的参考指南。

6).GB/T 19771-2005 信息技术 安全技术 公钥基础设施 PKI组件最小互操作规范

本标准支持大规模公钥基础设施（PKI负责发布、撤销和管理用于数字签名及密钥管理的公钥证书）的互操作性。本标准为不同的PKI开发者所开发的组件产品提供了基本的互操作性参考。

本标准适用于那些有兴趣开发具有互操作能力的PKI组件的公司、制订统一规范的政府机构以及其他感兴趣的部门。

7).信息技术 安全技术 公钥基础设施 数字证书格式(即将颁布)

本标准规定我国数字证书的基本结构,并对数字证书中的各数据项内容进行了描述。本标准规定了一些标准的证书扩展域,并对每个扩展域的结构进行了定义,特别是增加了一些专门面向国内应用的扩充项。本标准还对证书中所应支持的签名算法、散列(哈希)函数、公开密钥算法进行了描述,另外在附录C中列举了中国目前通用的数字证书结构,附录D中提供了证书DER编码供参考。

8). 信息技术 安全技术 公钥基础设施 时间戳规范(即将报批)

本标准对时间戳系统部件组成、时间戳的产生方式、时间戳的颁发方式、时间戳的存储、销毁、备份和检索、时间戳的格式和时间戳系统安全管理等方面对时间戳系统相关部件做出规定。

本标准适用于时间戳系统的设计和实现,时间戳系统的测试和产品采购亦可参照使用。

9).信息技术 安全技术 CA认证机构建设和运营管理规则(即将报批)

本标准规定CA认证机构在建设和运营管理方面的要求,适用于在开放的互联网环境中提供数字证书服务的认证机构,对于在封闭环境中(如在特定团体或某个行业内)运行的认证机构可根据自身安全风险评价以及国家有关的法律法规有选择性地参考本标准。国家有关的测评机构、监管部门也可以将本标准作为测评和监管的依据。

10).信息技术 安全技术 安全支撑平台技术框架(即将报批)

本标准规定电子政务和电子商务建设过程中基于公钥基础设施的安全支撑平台的技术框架。

本标准适用于电子政务和电子商务系统中安全支撑平台的设计、建设、检测、运营及管理,指导电子政务和电子商务安全支撑平台的设计、建设和检测;规范电子政务和电子商务系统中安全支撑平台的建设,为实现各系统的互联互通、信息共享及信息安全提供统一的技术支持。对于特定的安全支撑平台的建设,可根据具体的业务需求和情况进行灵活配置。同时此标准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。

11).信息技术 安全技术 权限管理中心技术规范(即将报批)

本标准规定一套作为PMI安全管理中心的技术框架,并规定了相关服务的要求。本标准主要规定了以下两个方面的框架:

a)权限管理中心架构;

b)相关安全协议。

本标准可应用于权限管理中心基础设施的建设,适用于电子政务和电子商务系统中权限管理系统的设计、建设、检测、运营及管理,指导电子政务和电子商务权限管理中心的设计、建设和检测;对于特定的应用系统,可根据具体的业务需求和情况进行灵活配置。

本标准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。

12).信息技术 安全技术 公钥基础设施 证书策略与认证业务声明框架(即将报批)

本标准规定证书策略（CP）和认证业务声明（CPS）应共同遵守的框架，范围限制在讨论CP或CPS所能包括的主题上，特别是在CP或CPS中所应包含的信息类型。尽管本标准提出的框架一般假设使用GB/T16264.8证书格式，并不意味着此框架被限于使用这种证书格式。相反，此框架的目的在于适用于其他格式的证书。

本标准不会扩展到通用安全策略的定义（如组织安全策略、系统安全策略或数据标记策略），也不定义特定的CP或CPS。本标准所给出的框架应作为一个灵活的工具来使用，用以指明在特定的CP或CPS中所应考虑的主题，而不是作为生成CP或CPS的固定公式。

13). 信息技术 安全技术 证书载体应用程序接口(即将报批)

本标准制定智能卡、安全存储介质、其他存储设备的使用接口。

本标准主要描述以下内容：制定智能卡、安全存储介质、其他存储设备的使用接口，包括：

存储格式、密钥产生方式、文件结构、具体调用接口等等。

本标准适用于规范PKI行业内使用的证书、密钥的载体的使用接口，同时可作为CA介质研发单位，生产厂家的参考指南。

14). 信息技术 安全技术 CA密码设备应用程序接口(即将报批)

本标准规定一种CA系统密码设备应用程序接口标准。本标准主要描述了以下内容：

- 具体描述对信息签名、验证操作的实现形式；
- 具体描述对信息加密、解密操作的实现形式；
- 具体描述对信息进行摘要操作的实现形式；
- 具体描述对密钥进行生成、导入、导出等操作的实现形式；
- 具体描述对证书进行导入、导出等操作的实现形式；

15). 信息技术 安全技术 PKI应用支撑平台(即将报批)

基于PKI技术，面向电子政务、电子商务等具体应用，提供安全的应用开发、应用运行、应用整合环境。主要包括接入认证、应用整合、信息交换、Portalet等技术。规范国内PKI应用支撑平台的制订和使用，充分考虑到国内的实际国情与国际的先进经验相结合。对现有电子政务、电子商务等安全的应用开发整合具有支持作用。

16). 信息技术 安全技术 公钥基础设施 简易在线证书状态协议 (计划研制)

本标准规定一种轻量级的在线证书状态协议（即简单在线证书状态协议—S-OCSP）。该机制可作为标准OCSP协议的补充。本标准主要描述了以下内容：

- 1 具体描述简单在线证书状态协议的请求形式；
- 2 具体描述简单在线证书状态协议的响应形式；
- 3 分析处理简单在线证书状态协议响应时可能出现的各种异常情况；
- 4 说明简单在线证书状态协议基于超文本传输协议（HTTP）的应用方式。

本标准的附录B提供了采用抽象语法表示法（ASN.1）描述的简单在线证书状态协议。

本标准主要适用于各类基于公开密钥基础设施的应用验证系统和计算环境，满足应用系统快速验证用户证书有效性的需求。

17). 信息技术 安全技术 公开密钥基础设施 电子签名卡应用接口(计划研制)

本规范适用于电子签名相关的IC卡及应用。其适用对象主要是电子签名应用相关的卡制造商、PKI应用开发商等。本规范是一个电子签名卡应用接口的最小集，卡制造商、PK应用开发商可在此基础上依据相关标准进行功能扩展。

2.3 管理技术

1).GB/T 17143.1-1997 信息技术 开放系统互连 系统管理 第1部分:客体管理功能

本标准定义了一种系统管理功能,它供应用进程在集中式或分散式管理环境中交互,以便用于管理框架标准(GB/T 9387.4)所定义的系统管理。本标准定义的客体管理功能由服务、功能单元和类属定义组成。

本标准详细规定了客体管理的模型;类属定义,包括事件类型、事件信息和事件应答;创建、删除、活动等9种服务定义;客体管理的各种功能单元;各种协议,包括规程元素、抽象语法和功能单元协商的协议;与其他功能的关系;一致性要求。

2).GB/T 17143.2-1997 信息技术 开放系统互连 系统管理 第2部分:状态管理功能

本标准定义了一种系统管理功能,它供应用进程在集中式或分散式管理环境中交互,以便用于管理框架标准(GB/T 9387.4)所定义的系统管理。本标准定义的状态管理功能由服务和类属定义组成。

本标准详细规定了状态管理的模型,包括类属状态和状况属性;类属定义,包括类属属性、类属通知和被管客体;各种服务定义;功能单元;各种协议,包括规程元素、抽象语法和功能单元协商的协议;与其他功能的关系;一致性要求。

3).GB/T 17143.3-1997 信息技术 开放系统互连 系统管理 第3部分:表示关系的属性

本标准定义了一种系统管理功能,它供应用进程在集中式或分散式管理环境中交互,以便用于管理框架标准(GB/T 9387.4)所定义的系统管理。本标准定义的表示关系的属性由服务和类属定义组成。

本标准详细规定了表示关系属性的模型,包括表示关系的分类、关系的类型和关系的角色;类属定义,包括类属属性、类属通知和被管客体;各种服务定义;功能单元;各种协议,包括规程元素、抽象语法和功能单元协商的协议;与其他功能的关系;一致性要求。

4).GB/T 17143.4-1997 信息技术 开放系统互连 系统管理 第4部分:告警报告功能

本标准定义了一种系统管理功能,它供应用进程在集中式或分散式管理环境中交互,以便用于管理框架标准(GB/T 9387.4)所定义的系统管理。本标准定义的告警报告功能由服务、类属定义和功能单元组成。

本标准详细规定了告警报告的模型;类属定义,包括类属通知和被管客体;各种服务定义;功能单元;各种协议,包括规程元素、抽象语法和功能单元协商的协议;与其他功能的关系;一致性要求。

5).GB/T 17143.5-1997 信息技术 开放系统互连 系统管理 第5部分:事件报告管理功能

本标准定义了一种系统管理功能,它供应用进程在集中式或分散式管理环境中交互,以便用于管理框架标准(GB/T 9387.4)所定义的系统管理。本标准定义的事件报告管理功能由服务和两种功能单元组成。

本标准详细规定了事件报告管理的模型;类属定义,包括被管客体和引入的类属定义;各种服务定义;功能单元,包括事件报告管理和监控事件报告管理两种功能单元;各种协议,包括规程元素、抽象语法和功能单元协商的协议;与其他功能的关系;一致性要求。

6).GB/T 17143.6-1997 信息技术 开放系统互连 系统管理 第6部分:日志控制功能

本标准定义了一种系统管理功能，它供应用进程在集中式或分散式管理环境中交互，以便用于管理框架标准（GB/T 9387.4）所定义的系统管理。本标准定义的日志控制功能由服务和两种功能单元组成。

本标准详细规定了日志控制的模型；类属定义，包括被管客体 and 引入的类属定义；各种服务定义；功能单元，包括日志控制和监控日志两种功能单元；各种协议，包括规程元素、抽象语法和功能单元协商的协议；与其他功能的关系；一致性要求。

7).GB/T 17143.7-1997 信息技术 开放系统互连 系统管理 第7部分：安全报警报告功能（等同国际标准ISO/IEC 10164-7:1992）

本标准定义了安全告警报告功能。安全告警报告功能是一项系统管理功能，它了供应进程在集中式或分散式管理环境中交换信息，以便用于GB/T9387.4所定义的系统管理。本标准位于GB 9387的应用层，并按照GB/T17176提供的模型定义。系统管理功能的作用由GB/T17142描述。由本系统管理功能定义的安全告警通知提供关于操作条件和服务质量的信息，他们附属于安全。本标准为需要用来支持安全告警报告功能的服务定义建立用户需求；定义由安全告警报告功能提供的服务；规定为提供服务所需的协议；定义与其他系统管理功能之间的关系；规定一致性要求。

8).GB/T 17143.8-1997 信息技术 开放系统互连 系统管理 第8部分：安全审计跟踪功能（等同国际标准ISO/IEC 10164-8:1993）。

本标准定义了安全审计跟踪功能。安全审计跟踪功能是一项系统管理功能，它供应进程在集中式或分散式管理环境中交换信息和命令，以便用于GB/T9387.4所定义的系统管理。本标准位于GB/T9387的应用层，并按GB/T17176提供的模型定义。系统管理功能的作用由GB/T17142描述。本标准为需要用来支持安全审计跟踪报告功能的服务定义而建立用户需求；定义由安全审计跟踪报告功能提供的服务；规定为提供服务所必需的协议；定义服务与管理通知之间的关系；定义与其他系统管理功能之间的关系；规定一致性要求。

2.4 物理安全

1).GB/T 9361-1988 计算机场地安全要求

本标准规定了计算站场地的安全要求，适用于各类地面计算站，不建站的地面计算机机房，按本标准对计算机机房的有关要求执行，改建的计算机机房参照本标准执行非地面计算机机房参照本标准执行。

2).GB/T 2887-1989 计算机场地通用规范

本标准规定了电子计算机场地定义、要求、测试方法与验收规则。

本标准适用于各类电子计算机系统的场地，其他电子设备系统的场地可参照本标准执行。

3).GB 50174-1993 电子计算机机房设计规范

本标准适用于陆地上新建、改建和扩建的主机房建筑面积大于或等于140平方米的电子计算机机房的设计。本标准不适用于工业控制用计算机机房和微型计算机机房。

4).SJ/T 30003-1993 电子计算机机房施工及验收规范

5).GB 9254-1998信息技术设备的无线电干扰极限值和测量方法(等同国际标准CISPR 22:1997)。

本标准的适用范围扩展至整个无线电频率范围9kHz-400GHz,但只在有限的频段规定了骚扰限值,该限值被认为即可以保障有适当的发射电平来保护无线电广播和电信业务,又可以允许其他设备在合理的距离处按预定的要求工作。本标准适用于标准第3.1条所定义信息技术设备(ITE)。本标准规定了A级和B级设备的骚扰限值,并规定了测量ITE所产生的杂散信号电平的程序。适用的频率范围为9kHz-400GHz。对于尚未规定限值的频段,不必测量。本标准旨在对适用范围内的设备的无线电骚扰电平给出统一的要求,确定骚扰限值,规定测量方法,规范运行的条件和试验数据的处理。

6).GB/T 17618-1998 信息技术设备抗扰度限值和测量方法(等同国际标准CISPR 24:1997)。

本标准规定了ITE在0Hz-400Hz频率范围内的限值和测量方法。本标准的目的是对ITE内部抗扰度提出合适的要求,以便使设备在其预定的环境中正常工作。对特殊的环境条件,可能要求采取减缓措施。由于测试和性能评估的考虑,一些试验在规定的频段或选频情况下进行。在这些频率点上满足抗扰度要求的设备被认为在0Hz-400Hz全频段范围内也满足要求。本标准的目的是规定设备在连续和瞬变、传导和辐射骚扰包括静电放电(ESD)情况下抗扰度试验要求。在每个考虑的端口规定试验要求。

7).计算机信息系统安全等级保护技术要求 物理安全(计划研制)

本标准按照规定计算机信息系统物理安全等级划分所需的检验试验的技术要求。

本标准适用于对计算机信息系统物理安全等级划,适用于计算机信息系统物理安全的试验、检测、设计、施工、及相关产品的采购。

8).GB 4943-2001 信息技术设备的安全(等同国际标准IEC 60950:1999)。

3、信息安全管理

1).GB 17859-1999 计算机信息系统 安全保护等级划分准则

本标准规定了计算机信息系统安全保护能力的五个等级,即:

第一级:用户自主保护级;

第二级:系统审计保护级;

第三级:安全标记保护级;

第四级:结构化保护级;

第五级:访问验证保护级。

本标准适用于计算机信息系统安全保护技术能力等级的划分。计算机信息系统安全保护能力随着安全保护等级的增高,逐渐增强。

2).GB/T 19715.1-2005 信息技术 信息技术安全管理指南 第1部分:信息技术安全概念和模型(等同采用ISO/IEC TR 13335-1:1996)

第1部分提出了基本的管理概念和模型,将这些概念和模型引入IT安全管理是必要的。

3).GB/T 19715.2-2005 信息技术 信息技术安全管理指南 第2部分:管理和规划信息技术安全(等同采用ISO/IEC TR 13335-1:1996)

本部分中的指南提出IT安全管理的一些基本专题以及这些专题之间的关系。这些指南对标识和管理IT安全各个方面是有用的。

4).GB/T 19716-2005 信息技术 信息安全管理实用规则 (等同采用 ISO/IEC 17799:2000)

本标准对信息安全管理给出建议,供负责在其组织启动、实施或维护安全的人员使用。本标准为开发组织的安全标准和有效的安全管理做法提供公共基础,并提供组织间交往的信任。本标准的推荐内容应按照适用的我国法律和法规加以选择和使用。

5).信息安全等级保护 信息系统安全管理要求 (即将报批)

本标准规定按GB17859-1999的等级划分实现信息安全等级保护对信息系统安全的管理要求。

本标准适用于相关组织机构(部门)对信息系统实施等级保护所进行的安全管理。

6).信息安全等级保护 信息系统工程管理要求 (即将报批)

本标准规定信息系统安全等级保护工程(以下简称信息安全等级保护工程)管理的要求,是对信息安全等级保护工程中所涉及到的甲方、乙方与第三方工程实施的指导性文件,各方可以此为依据建立安全工程管理体系。

本标准按照GB17859-1999划分的五个安全保护等级,规定了对不同安全保护等级的计算机信息系统进行工程实施采用的不同要求。

本标准适用于安全系统的机构和开发商的工程管理,集成商、安全服务的提供商和安全工程的组织方也可参照使用。

对涉及国家秘密的信息系统,建议参考国家相关标准进行系统建设。

7).信息系统安全等级保护实施指南(计划研制)

为配合《信息系统安全等级保护办法》,从根本上解决我国计算机信息系统建设、运行、管理和使用等过程中的不规范现状,提高我国计算机信息系统安全保护的整体水平,公安部组织制定了《信息系统安全等级保护实施指南》(以下简称实施指南)。本实施指南在全面体现GB17859-1999的等级化标准思想的基础上,充分吸收近年来安全领域出现的信息系统安全保障理论模型和技术框架(如IATF等);风险评估方法和模型;以国标GB/T 18336-2000为基础的安全产品评估标准;信息安全管理标准ISO/IEC 17799:2000和ISO/IEC TR 13335系列标准;以及其他发达国家的国家标准中的精髓,根据我国的信息化发展现状和我国特有的行政管理模式,提出了安全保护等级的确定方法,并为指导各行各业信息系统的建设和改进,从安全等级保护技术体系和安全等级保护管理体系两个方面分别给出了5个等级的指导性建议。

本实施指南适用于计算机信息系统按等级保护要求所进行的计算机信息系统的设计、实现、测试和管理,计算机信息系统所使用的产品采购也可参照使用。

本实施指南中对安全部件、安全产品和安全技术提出的要求是功能要求,其保证要求将由以后相关产品的标准定义。

8).信息安全风险评估指南 (计划研制)

本标准提出信息安全风险评估的工作流程、评估内容、评估方法和风险判断准则,适用于信息系统使用单位进行自评估,以及风险评估机构对信息及其处理系统进行独立的风险评估。

9).信息系统灾难恢复指南(计划研制)

本指南规定重要信息系统的灾难恢复应遵循的基本要求。

本指南适用于指导重要信息系统的使用和管理单位(以下简称“单位”)进行灾难恢复的规划和准备工作,对重要信息系统灾难恢复项目的审批和监督管理也可参照使用。

10).网络与信息安全事件分类指南(计划研制)

本指南为技术性指导文件，可为负责在其组织内监测、处理网络与信息安全事故的人员和负责网络与信息安全事故管理及调查的人员/部门提供指导，适用于各种类型的组织。

11).信息技术 安全技术 信息安全事故管理(计划研制)

为信息安全管理者，信息系统、服务和网络管理者提供了关于信息安全事故管理的建议和指南。

本技术报告包括11章，按照下列方式组成。第1章描述了范围，第2章列出了参考文献列表，第3章中给出了术语和定义。第4章提供了信息安全事故管理的一些背景，紧跟着第5章总结了利益和关键问题。然后在第6章中给出了信息安全事故及其原因的示例。信息安全事故管理的规划和准备，包括文档生成，在第7章中描述。第8章描述了信息安全事故管理方案的运行使用。信息安全管理评审阶段，包括标识吸收的教训和安全以及信息安全事故管理方案的改进，在第9章中予以描述。改进阶段，例如，标识出对安全和信息安全事故管理方案的改进，在第10章中描述。最后，本文在第11章中进行了简短的总结。附录A包含了信息安全事件和事故报告单，附录B包含了用于评估信息安全事故负面结果的示例概述指南，包括在报告单中。附录后面是参考文献。

4、评估标准

4.1 评估基础标准

1).GB/T 18336.1-2001 信息技术 安全技术 信息技术安全性评估准则 第1 部分：简介和一般模型（等同国际标准ISO/IEC 15408-1:1999）

GB/T18336定义了作为评估信息技术产品和系统安全特性的基础准则，由于历史和连续性的原因，仍叫通用准则（CC）。通过建立这样的通用准则库，使信息技术安全评估的结构能被更多的人理解。针对在安全性评估过程中信息技术产品和系统的安全功能及相应的保证措施，CC提供了一组通用要求，使各种独立的安全评估结果具有可比性。评估过程为满足这些要求的产品和系统的安全功能以及相应的保证措施确定一个可信级。评估结果可以帮助用户确定信息技术产品和系统对他们的应用而言是否足够安全，以及在使用中隐藏的安全风险是够可以容忍。CC可用于具有信息技术安全功能的产品和系统的开发与采购指南。CC涉及信息保护，以避免未经授权的信息泄露、修改和无法使用。CC适用于硬件、固件和软件实现的信息技术安全措施。

2).GB/T 18336.2-2001 信息技术 安全技术 信息技术安全性评估准则 第2 部分：安全功能要求（等同国际标准ISO/IEC 15408-2:1999）。

本标准定义的安全功能组件是保护轮廓（PP）或安全目标（ST）中所表述的TOE IT 安全功能要求的基础。这些要求描述了对评估对象（TOE）所期望的安全行为，目的是满足PP或ST中陈述的安全目的。这些要求描述用户通过与TOE直接交互（即输入，输出）或通过TOE对刺激反应，可以检测到的安全特性。安全功能组件表达用于在假定的TOE运行环境中对抗威胁的要求，或涉及所有标识的组织安全策略和假设。

3).GB/T 18336.3-2001 信息技术 安全技术 信息技术安全性评估准则 第3 部分：安全保证要求（等同国际标准ISO/IEC 15408-3:1999）。

本标准定义了保证要求。它包括衡量保证尺度的评估保证级（EAL）、组成保证级的每个保证组件以及PP和ST的评估准则。

4). 保护轮廓和安全目标产生指南(即将报批)

本标准描述PP与ST中的内容及其各部分内容之间的相互关系的详细指南,并在附录中给出了若干实例,供感兴趣的读者参考。

本标准给出PP与ST文档内容的概述,给出了样本目录清单,给出了目标用户最关心的内容,陈述了PP与ST之间的关系,以及PP与ST的开发编写过程。

本标准给出编写指南,用于指导PP与ST的描述部分的编写,内容涵盖PP与ST的引言、针对用户和使用者的TOE描述以及针对ST作者和TOE开发者的PP应用注释。

本标准给出编写指南,用于指导TOE安全环境的定义。

本标准给出编写指南,用于指导编写安全目的,安全目的由TOE及其环境导出。

本标准给出编写指南,用于指导选择IT安全要求组件,描述了GB/T 18336中定义的功能组件和保证组件的使用方法,以及非GB/T 18336定义的组件的使用方法。

本标准给出了写指南,用于指导ST中TOE概要规范的编制。

本标准给出编写指南,用于指导基本原理的编制。

本标准给出编写指南,用于指导复合TOE的PP与ST的编制,复合TOE是由两个或多个TOE组成。

本标准给出编写指南,用于指导安全功能包和保证包的构成方法。

5). 信息系统安全保障评估框架 (即将报批)

信息系统安全保障评估框架第一部分：简介和一般模型：

《GB/T 18336-2001：信息技术 安全技术 信息技术安全性评估准则》中定义评估信息技术产品和系统安全特性的基础准则,它主要应用于具有安全功能的信息技术产品和系统的设计、开发和采购指南。在评估过程中,这样的产品和系统被称为评估对象(TOE—Target of Evaluation),如：操作系统、计算机网络、分布式系统以及应用等。信息技术安全性评估准则涉及信息保护,以避免未经授权的信息泄露、修改和无法使用,与此对应的保护类型分别称之为保密性、完整性和可用性。

“信息系统安全保障评估框架”是GB/T 18336在信息系统领域的扩展和补充,它的目的是以信息技术安全性评估准则为基础,吸取信息技术安全性评估准则的科学方法和结构,将信息技术安全性评估准则从产品和产品系统扩展到信息技术系统,然后进一步同其他信息系统运行环境所涉及的安全管理和安全工程等领域的标准和规范进行结合、扩展和补充,形成的覆盖信息系统全生命周期的、对信息系统安全保障能力进行评估的通用评估框架。

信息系统安全保障评估框架主要是以风险和策略为出发点和核心,即从信息系统所面临的风险和信息系统所处的环境出发制定组织机构信息系统安全保障策略,通过在信息系统的整个生命周期中从技术、工程、管理和人员等方面提出安全保障要求,确保信息的保密性、完整性和可用性特征,实现和贯彻组织机构策略并将风险降低到可接受的程度,达到保护组织机构信息和信息系统资产,从而保障组织机构实现其使命的最终目的。在信息系统安全保障评估框架中,评估对象的含义更加广泛,它不仅涉及具体产品和产品系统,而且还包含信息系统运行环境的管理、工程等范畴,即用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件等总和的信息系统。

信息系统安全保障评估框架可以用于对信息系统安全保障的综合保障能力进行评估,同时也可以根据信息系统安全保障评估框架不同分册所涉及的具体领域对信息系统安全保障的技术架构能力、工程能力和管理能力进行评估。信息系统安全保障可以应用的主要领域包

括但不限于以下内容：规范化描述信息系统安全保障的需求（编制信息系统安全保障要求 ISPP）、设计和规划符合信息系统安全保障需求的信息系统安全保障体系的方案和规范（根据信息系统安全保障要求 ISPP 来编制信息系统安全保障目标 ISST），评估信息系统安全保障能力，包括对安全保障方案进行评审（评估所编制的信息系统安全保障方案 ISST 同信息系统安全保障的需求 ISPP 的符合性）、对信息系统安全工程的实施和实施能力进行评估（依据其信息系统的信息系统安全保障目标 ISST 和信息系统安全保障准则中的工程保障，评估所实施工程的内容和工程实施的能力）、对信息系统的安全保障管理控制和管理能力进行审核（依据信息系统的信息系统安全保障目标 ISST 和信息系统安全保障准则中的管理保障，评估所实施的管理的内容和管理实施的能力）以及对信息系统在其运行环境中的信息系统安全保障能力整体进行综合评估（依据信息系统的信息系统安全保障目标 ISST 和综合信息系统安全保障准则中的技术、管理和工程保障，评估信息系统安全保障体系是否符合其信息系统安全保障需求和信息系统安全保障的能力）等。

信息系统安全保障评估框架中，不包含以下内容：

- b) 针对人员技能和能力的评估内容，但对人员安全的要求在管理保障中体现。
- c) 系统评估方法学。
- d) 密码算法固有质量的评价。

信息技术 安全技术 信息系统安全保障评估框架 第二部分：技术保障：

本标准定义的技术组件描述信息系统安全保障评估框架—技术保障，它是信息系统生命周期中信息系统技术要求的基础，它主要用于评估信息系统安全保障中技术部分，即主要用于对信息技术系统（作为信息系统一部分的执行组织机构信息功能的用于采集、创建、通信、计算、分发、处理、存储和/或控制数据或信息的计算机硬件、软件和/或固件的任何组合）进行评估的框架。

本标准的读者包括信息系统的用户、开发人员和评估人员。这些读者可按如下方式使用本标准：

- 1 用户，当选择组件来表达功能要求以达到其安全技术保障时，使用本标准。
- 2 开发者，开发者在这里的含义包括开发信息系统安全保障解决方案的组织机构内部或外部技术人员。开发者在应实际的或假设的用户的安全保障要求而建立安全保障技术框架这个评估目标 TOE 时，可以在本标准中找到理解这些技术要求的标准化的方法。他们也可以将标准的内容作为进一步定义符合这些要求的 TOE 的基础。
- 3 评估者，使用这部分定义的功能要求来验证安全保障技术框架要求是否达到信息系统安全目标，以及所有的依赖关系是否满足。评估者也应使用本标准内容来帮助决定一个给定的 TOE 是否满足给定的要求。

这里描述的相关技术要求，并不意味着所有的信息系统技术安全保障问题都是确定的答案。确切地说，标准提供一系列容易理解的安全功能要求，用于根据市场需要来达到可信的安全保障技术能力。提出的这些技术要求体现了要求规范和评估的最佳方法。

本标准不足以包括所有可能的技术要求，而是包含那些在发布时作者所知道并认为是有价值的那些内容。

因为用户的理解和要求可能变化，因此需要维护本标准的功能要求。

信息系统安全保障评估框架-技术保障主要用于评估信息系统中系统级的技术框架和技术解决方案，即对信息技术系统（信息技术系统：作为信息系统一部分的执行组织机构信息功能的用于采集、创建、通信、计算、分发、处理、存储和/或控制数据或信息的计算机硬件、软件和/或固件的任何组合）进行评估。在信息系统安全保障评估框架的技术、管理和工程保障中，技术保障同 GB/T 18336 信息技术安全性评估准则间有着最直接和紧密的关系；

信息系统安全保障评估准的技术框架和技术解决方案直接建立在经过GB/T 18336准则评估认可的产品和产品系统之上。

在信息系统安全保障评估框架技术保障中，它的评估对象TOE是构成信息系统的所有计算机硬件、软件和/或固件的任何组合。信息系统安全保障评估框架技术保障，首先要求信息系统的用户为其评估对象TOE（即信息技术系统）完善其技术体系构架建设过程，建立其信息技术系统的技术体系构架；在完成其信息技术系统技术体系构架后，然后基于此技术体系构架，对信息技术系统进行高层分析和确定相关安全目的；最后用规范和标准化的技术组件进行描述。

技术体系构架建设过程，是组织机构根据其策略的要求和风险评估的结果，参考相关技术体系构架的标准和最佳实践，结合组织机构信息技术系统的具体现状和需求，建立的符合组织机构信息技术系统战略发展规划的信息技术系统整体体系框架，它是组织机构信息技术系统战略管理的具体体现。技术体系架构能力是组织机构执行安全技术整体能力的放映，它反映了组织机构在执行信息安全技术体系框架管理达到预定的成本、功能和质量目标上的度量。

6). 信息系统安全等级保护测评准则（计划研制）

本标准规定对信息系统进行等级测评的基本内容，使用到的测评方法，涉及到的具体测评对象，实施测评的过程，以及对测评结果进行判定的基本规则。

7). 信息技术安全通用评估方法（计划研制）

信息技术安全通用评估方法 第一部分：简介和一般模型：

通用评估方法（CEM）是为应用通用准则（CC）进行评估而开发的一种公认方法。CEM支持安全评估的相互认可。

评估过程由其中待执行的行为、以及评估方法要求的开发过程和监督过程中的行为组成。也有一些行为，虽然包含在开发过程和监督过程中，但却不包含在评估过程和CEM之中。本文档将提出用于IT安全评估的原则、程序和过程（行为）。但不涉及这些规则（即体制）的本地或局部化实现细节。

信息技术安全通用评估方法 第二部分：评估方法：

信息技术安全评估通用方法（CEM）是信息技术安全评估通用准则（CC）的配套文档。CEM描述了评估者在用CC中定义的评估证据进行评估时，所需要完成的基本活动。

该版CEM仅限于PP评估和EAL1~EAL4级的TOE评估，没有提供EAL5~EAL7级的评估指南，也不提供用其它保证包进行评估的指南。CEM基于CC2.1版，以及CC解释管理委员会（CCIMB）解释反馈信息。

CEM的目标读者主要面对应用CC进行评估的评估者和认可评估者行为的认证员，还有评估申请者、开发者、PP/ST作者和其它对IT安全感兴趣的人员。

诚然，CEM并不能回答有关IT安全评估的所有问题，因此需要进一步解释。尽管这些解释应服从于互认协议，但是各评估体制可以自己决定如何处理解释。附录B.9给出了相关于评估活动的方法，各评估体系可对其进行相应的处理。

CEM第一部分（VO.6）定义了CEM的通用模型，现正在修订。因此，CEM第二部分的版本高于CEM第一部分的版本，甚至可能有表面上的不一致。将来的CEM第一部分升级版会解决这些矛盾。

4.2 产品测评标准

1). GB/T 17900-1999 网络代理服务器的安全技术要求

本标准规定了网络代理服务器的安全技术要求,并作为网络代理服务器的安全技术检测依据。

网络代理服务器以各种代理服务为基础,通过它提供集中的应用服务。只有合法有效的客户要求才由代理服务器提交给真正的服务器。

本标准详细规定了代理服务器的安全环境,包括安全条件假设、对安全的威胁;安全目标,包括信息技术和非信息技术安全目标;信息技术安全要求,包括各种功能要求和各种保证要求;基本原理,包括信息技术安全目标、非信息技术安全目标、信息技术功能要求的基本原理。标准以附录的形式给出了符号结构及含义。

2). GB/T 18018-1999 路由器安全技术要求

路由器是连接两个或多个计算机网络,并能在这些网络之间转发数据包的专用网络设备。为防止经路由器对网络的攻击,及保护路由器自身的安全,则要求路由器要达到规定的安全目标。

标准给出了路由器的基本概念,包括安全目标、安全技术要求(含安全功能类、安全功能组和安全组件)的描述方法、路由器安全功能要求;本标准详细规定了各类安全功能的具体要求,这些功能类包括加密、鉴别、审计路由器管理安全、路由器信息安全、服务访问安全、包过滤、虚拟专网、路由器初始化。标准以附录的形式给出了路由器安全级别划分的建议规则。

3). GB/T 18019-1999 信息技术 包过滤防火墙安全技术要求

本标准规定了采用“传输控制协议/网间协议(TCP/IP)”的包过滤防火墙产品或系统的安全技术要求。适用于防火墙产品或系统安全功能的研制、开发、测试、评估和产品的采购。

防火墙产品主要分为包过滤和应用网关两大类,本标准规定的是包过滤防火墙的最低安全要求。设置防火墙的目的是要在内部网和外部网之间建立一个安全控制点,通过允许、拒绝或重新定向经过防火墙的数据流,实现对进、出内部网的服务和访问的审计和控制。

本标准详细规定了安全环境(包括安全使用条件、防火墙面临的威胁、运行环境面临的威胁);信息技术性和非信息技术的安全目标;功能要求和保证要求;基本原理(包括信息技术安全目标、非信息技术安全目标、信息技术功能要求、保证要求的基本原理)。

4). GB/T 18020-1999 信息技术 应用级防火墙安全技术要求

本标准规定了应用级防火墙产品或系统的安全技术要求。适用于应用级防火墙产品或系统安全功能的研制、开发、测试、评估和产品的采购。

防火墙产品主要分为包过滤和应用级两大类,本标准规定的是应用级防火墙在低风险环境下的最低安全要求。设置防火墙的目的是要在内部网和外部网之间建立一个安全控制点,通过允许、拒绝或重新定向经过防火墙的数据流,实现对进、出内部网的服务和访问的审计和控制。

本标准详细规定了安全环境(包括安全使用条件、防火墙面临的威胁、运行环境面临的威胁);信息技术性和非信息技术的安全目标;功能要求和保证要求;基本原则(包括信息技术安全目标、非信息技术安全目标、信息技术功能要求、保证要求的基本原则)。

5). 操作系统安全保护等级评估准则(即将颁布)

本标准适用于计算机通用操作系统的安全保护等级的评估,对于通用操作系统安全功能的研制、开发和测试亦可参照使用。

6). 数据库管理系统安全保护等级评估准则(即将颁布)

本标准适用于数据库管理系统的安全保护等级的评估,对于数据库管理系统安全功能的研制、开发和测试亦可参照使用

7). 路由器安全保护等级评估准则(即将颁布)

本标准适用于路由器安全保护等级的评估,对路由器的研制、开发、测试和产品采购也可参照使用

8). 包过滤防火墙安全保护等级评估准则 (即将颁布)

本标准适用于包过滤防火墙安全保护等级的评估,对于包过滤防火墙的研制、开发、测试和产品采购也可参照使用

9).信息安全等级保护 操作系统安全技术要求(即将报批)

本标准依据GB17859-1999的五个安全保护等级的划分,根据操作系统在信息系统中的作用,规定操作系统安全所需要的安全技术的各个安全等级的要求。

本标准适用于按等级化要求进行的安全操作系统的设计和实现,对按等级化要求进行的操作系统安全的测试和管理可参照使用。

10).信息安全等级保护 数据库管理系统安全技术要求(即将报批)

本标准依据GB17859-1999的五个安全保护等级的划分,根据数据库管理系统在信息系统中的作用,规定数据库管理系统所需要的安全技术的各个安全等级的要求。

本标准适用于按等级化要求进行的安全数据库管理系统的设计和实现,对按等级化要求进行的数据库管理系统安全的测试和管理可参照使用。

11).智能卡嵌入式软件安全技术要求 (EAL4 增强级) (即将报批)

本标准规定对智能卡嵌入式软件进行安全保护所需要的安全技术要求。

本标准适用于智能卡嵌入式软件的研制、开发、测试、评估和产品的采购。

本标准适用于如下领域或行业的智能卡嵌入式软件 (EAL 4 增强级) :

金融领域

交通领域

电子商务

电子政务

通信领域

政府推广的身份标识、医疗保险、社会保险卡等

基于网络的事务处理或交易处理的其它领域或行业等

12).信息安全等级保护 隔离产品安全技术要求(即将报批)

本标准规定对隔离产品进行安全保护等级划分所需要的详细技术要求,并给出了每一个安全保护等级的不同技术要求。

本标准适用于按照《计算机信息系统安全保护等级划分准则》(以下简称《准则》)的安全等级保护要求所进行的隔离产品的设计和实现,按照《准则》安全等级保护的要求对隔离产品进行的测试、管理也可参照使用。

如不做特殊说明,本标准中的安全技术要求,适用于各种类型的隔离产品,包括物理断开、单向隔离、协议隔离与网闸产品。

13).信息安全等级保护 隔离产品评估准则(即将报批)

本标准规定对评估隔离产品安全功能所能达到的安全保护等级的准则,并给出每一个评估准则的不同测试评估方法。

本标准适用于按照《计算机信息系统安全保护等级划分准则》(以下简称《准则》)的安全等级保护要求所进行的隔离产品的测试和评估。

如不做特殊说明,本标准中的安全技术要求,适用于各种类型的隔离产品,包括物理断开、单向隔离、协议隔离与协议转换隔离。

14). 网络脆弱性扫描产品技术要求(即将报批)

本标准规定采用传输控制协议/网际协议(TCP/IP)的网络脆弱性扫描产品的技术要求,提出网络脆弱性扫描产品实现的安全目标及环境,给出产品基本功能、增强功能和安全保证要求。

本标准适用于通过网络对系统和设备进行脆弱性扫描的安全产品的研制、生产和认证。
本标准不适用于专门对数据库系统进行脆弱性扫描的产品。

15). 网络脆弱性扫描产品测评方法(即将报批)

本标准规定对采用传输控制协议/网际协议(TCP/IP)的网络脆弱性扫描产品的测试、评估方法。

本标准适用于对计算机信息系统进行人工或自动的网络脆弱性扫描的安全产品的评测、研发和应用。

本标准不适用于专门对数据库系统进行脆弱性扫描的产品。

16). 入侵检测系统技术要求和测评方法(即将报批)

本标准规定入侵检测系统的技术要求和测评方法,技术要求包括产品功能要求、产品安全要求、产品保证要求,并提出了入侵检测系统的分级要求。除非明确指明属于网络型或主机型入侵检测系统,否则本标准中的所有条款均适用于两类系统。

本标准适用于入侵检测系统的设计、开发、测试和评估。

17). 防火墙技术要求和测评方法(即将报批)

本标准规定采用“传输控制协议/网际协议(TCP/IP)”的防火墙类信息安全产品的技术要求和测评方法。

本标准适用于采用“传输控制协议/网际协议(TCP/IP)”的防火墙类信息安全产品的研制、生产、测试和评估。

18). 虹膜特征鉴别技术要求(计划研制)

本标准规定按照GB17859-1999安全保护等级的要求,实现用虹膜技术进行用户身份鉴别的安全系统的技术要求。

本标准适用于按GB17859-1999安全保护等级的要求所进行的虹膜特征身份鉴别系统的设计与实现,对于按GB17859-1999安全等级保护要求对虹膜特征身份鉴别系统进行的测试、管理也可参照使用

19). 智能卡芯片安全技术要求(EAL4 增强级)(计划研制)

本标准规定对智能卡芯片进行安全保护所需要的安全技术要求。

本标准适用于智能卡芯片的研制、开发、测试、评估和产品的采购。

20). 信息技术 安全技术 交换机 安全技术要求(EAL3增强级)(计划研制)

本标准描述服从本保护轮廓的交换机和路由器进行保护的安全要求。需要保护的信息是组织(或单位)的重要信息,它的破坏可能导致单位或组织的财产损失、影响计划执行或影响职员的工作状态。与符合本标准的交换机和路由器相结合,可以配置其它的安全性机制用

于进一步保障组织实现信息保护策略，其它的安全性机制可以包括配置防火墙、守卫和加密装置。本标准面向所有公私企业的读者，另外本标准也适用于下列情形。

- 1) 买方拥有和管理它自己的设备，并进行专用网络通信。
- 2) 买方拥有设备，但委托网络供应商或商业组织管理，设备一般位于网络供应商或商业组织处。
- 3) 买方不拥有也不管理任何设备，但是从供应商处购买服务。

上述情形在下一章中将进行了较全面的描述。交换机和路由器依赖网络管理系统实现相应的功能，网络管理系统已经定义好连接参数。虽然网络管理系统是交换机和路由器正常运行不可缺少的部分，但不包含在本标准的TOE中。

本保护轮廓给出的交换机和路由器安全要求，适合于保护任何环境下的、涉及网络基础设施控制管理的、日积月累的私有敏感信息，同时，本标准明确地界定了穿越网络基础设施的用户数据的保护不属于本保护轮廓考虑的范围。本保护轮廓接着定义了交换机和路由器的安全假设、威胁和组织策略；并进一步给出交换机和路由器的安全环境以及与实现无关的安全目的；同时定义了安全功能要求和安全保证要求；最后给出了安全目的和满足安全要求的基本原理说明。在第6章的基本原理中还提供了本保护轮廓满足增强的评估保证级3(EAL3+)的强度说明。

21). 路由器安全等级保护技术要求 (计划研制)

本标准按照GB 17859—1999《计算机信息系统安全保护等级划分准则》的内容规定不同等级的路由器应达到的技术要求。

本标准适用于按照GB 17859—1999的安全等级所进行的路由器产品的设计和实现，按照我国信息安全等级保护的有关规定对路由器产品所进行的测试、评估和管理也可参照使用。

22). 信息技术 审计跟踪产品技术要求(计划研制)

本标准规定采用传输控制协议/网间协议的审计跟踪产品技术要求。

本标准适用于对计算机网络及信息系统进行人工或自动的审计跟踪、保存和维护审计记录的安全产品的开发、测评和应用。

23). 服务器安全技术要求 (计划研制)

按照《计算机信息系统安全保护等级划分准则 GB 17859-1999》要求，参照《Trusted Computer System Evaluation Criteria (TCSEC Orange Book)》、《Common Criteria for Information Technology Security Evaluation》(简称CC)、《计算机信息系统安全等级保护通用技术要求》等国内外相关技术标准，在实体、应用和管理三个层面上，从设备物理、硬件、固件和软件等几个方面，针对服务器产品，深入研究服务器应具备的安全要素和安全特性(主要包括物理安全、运行安全、信息安全、TCB自身安全、TCB设计实现和TCB安全管理)，适当增加服务器产品特有的安全要素和特性，结合中国国情，编制“服务器安全技术要求”和“服务器安全等级保护技术要求”，对服务器产品安全技术应达到的要求进行详细而严格的描述，在用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级五个保护等级中每个等级应达到的技术标准进行严格的界定，用以指导服务器产品的技术开发

4.3 系统测评标准

1). 信息安全等级保护 信息系统安全通用技术要求(即将报批)

本标准依据GB17859-1999的五个安全保护等级的划分，规定信息系统安全所需要的安全技术的各个安全等级要求。

本标准适用于按等级化要求进行的安全信息系统的设计和实现，对按等级化要求进行的信息系统安全的测试和管理可参照使用。

2). 信息安全等级保护网络安全基础技术要求(即将报批)

本标准依据GB17859-1999的五个安全保护等级，规定各个安全等级的网络系统所需要的基础安全技术的要求。

本标准适用于按等级化的要求进行的网络系统的设计和实现，对按等级化要求进行的网络系统安全的测试和管理可参照使用。

3). PKI系统安全等级保护技术要求 (计划研制)

本标准从信息技术方面规定按照GB17859-1999的五个安全保护等级对PKI系统安全保护等级划分给定技术要求。

本标准适用于PKI系统的设计和实现，对于PKI系统安全功能的研制、开发、测试和产品采购亦可参照使用。

4). PKI系统安全等级保护评估准则 (计划研制)

本标准从信息技术方面规定按照GB17859-1999的五个安全保护等级对PKI系统安全保护等级划分所需要的评估内容。

本标准适用于PKI系统的安全保护等级的评估，对于PKI系统安全功能的研制、开发、测试和产品采购亦可参照使用。

附录

1. 术语表

见 GB/T 5271.8 《信息技术 词汇 第 8 部分：安全》

2. 电子政务信息系统安全实施的一般步骤与采标指南

2.1 电子政务信息系统安全实施的一般步骤描述

电子政务信息安全工程的一般过程如下图所示：

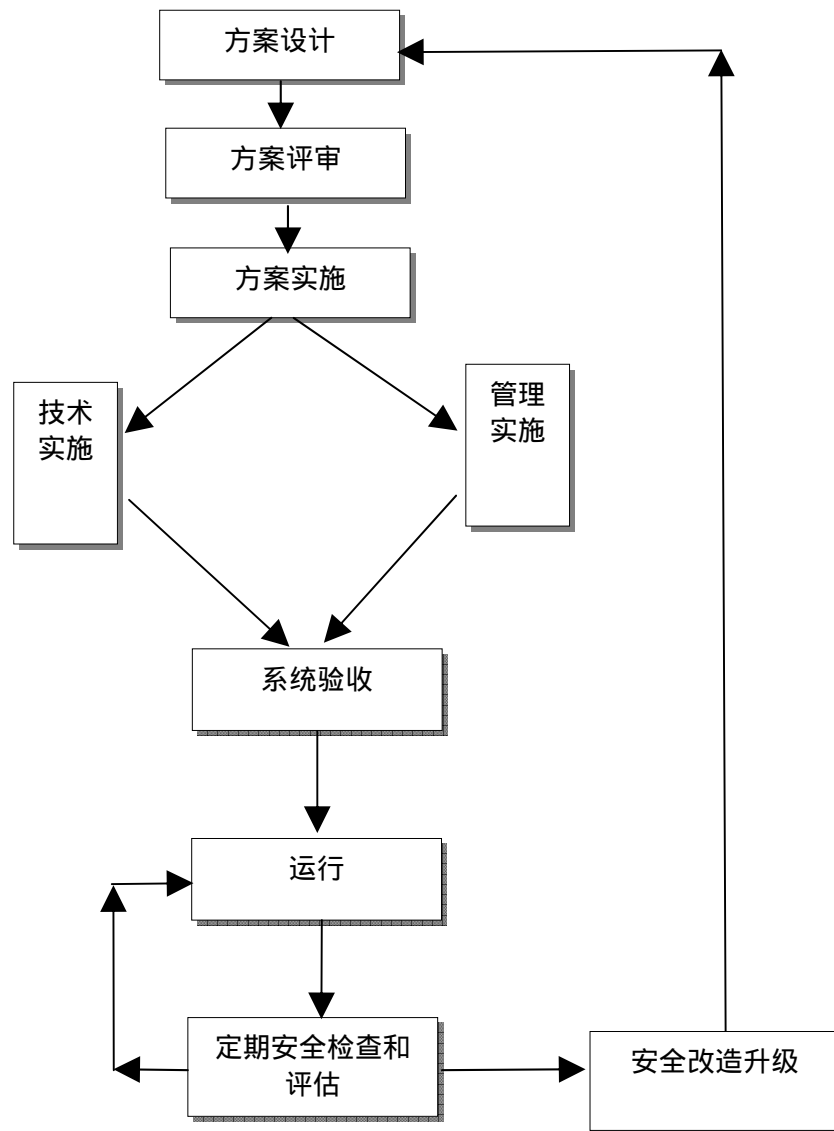


图 3 安全工程的一般过程

1) 方案设计和评审

在此阶段需要完成以下工作：

- 电子政务系统安全目标制定
在方案设计阶段，首先应明确系统的安全目标。制定安全目标时应考虑以下内容：
 - a) 系统业务内容规划
 - b) 系统的业务内容、信息种类和敏感性划分、系统建设的阶段划分
 - c) 系统涉及的政务机关行政关系和安全性特点
 - d) 系统所放置的地理位置、地理位置的安全性特点和需求
 - e) 系统用户对象和安全特点
 - f) 系统的用户对象划分、用户对象与系统安全性的关系。
- 电子政务信息系统结构设计分析
通过分析电子政务信息系统的体系结构、设备（信道、网络设备、计算设备、平台软件）构成，提取他们的安全性特点。
- 电子政务信息系统业务流程分析
通过分析电子政务信息系统中主要业务的流程、相关对象（设备和人）与流程的关系，抽取各种明确的安全功能需求。此阶段的分析一定要特别关注是否存在对政务业务明确的法令和法规的规定。电子政务的安全需求必须首先满足相应法令、法规的要求。
- 方案前安全风险分析
在前面分析的基础上，根据所建设电子政务信息系统的业务特点，考虑相应的安全威胁，对关键政务信息资产的安全风险进行分析，以明确系统的安全状态。
- 系统安全解决方案
电子政务安全方案应包括以下内容：
 - a) 安全解决方案的设计原则和理由；
 - b) 主要的安全策略和采用理由；
 - c) 系统边界描述，指出系统的主要安全风险和防护办法；
 - d) 系统的安全目标/需求，分析系统安全性保障能力。
 - e) 安全解决方案的详细描述；安全解决方案包括管理和技术两个方面；
 - f) 系统安全性的论证，必要时再次进行风险分析，以确保前一阶段分析出的风险得到了有效控制；

2) 方案的实施

方案的实施基本分为两个方面，一个是技术实施，一个是管理实施。

技术实施一般由专业的实施方负责完成，用户负责监督。电子政务信息系统安全工程的实施应该由有相应资质的单位负责完成。实施方应该制定详细的技术实施方案、工程实施方案、验收方案。

技术实施方案一般包括：

- ◆ 系统安全解决方案的技术和设备构成；
- ◆ 详细描述安全解决方案的技术和设备构成，提供必要的产品资质；
- ◆ 安全技术和设备的性能描述和分析。
- ◆ 对所采用的技术和设备的安全原理做必要的描述和安全性分析。

工程实施方案一般包括：

- ◆ 所需的场地、人员、设备、过程等关键要素描述；
- ◆ 工程实施中的安全保证；
- ◆ 论述工程实施中的安全风险和安全性保障措施；

- ◆ 工程实施进度计划；
- ◆ 工程实施质量保证体系规划。

管理实施一般由用户负责,必要时也可以邀请有资质的信息安全服务机构以咨询者的身份参与工作。管理实施也需要制定详细的计划、保障相应的人力和资源投入。管理实施一般涉及以下内容：

- 组织结构设置；
- 规章制定；
- 培训体系建立；
- 宣传体系建立；
- 安全管理评审体系建立；

3) 系统验收

系统验收是系统正式运行前的重要工作。电子政务信息安全系统的验收一般由主管部门主持完成。电子政务系统信息安全工程验收的一般程序如下：

- a) 用户单位向相应的主管部门提出验收申请；
- b) 主管部门委托国家授权的信息安全测评机构对申请验收的信息系统实施系统安全性测评，提出测评结论；
- c) 在主管部门主持下，召开系统验收会议，参加单位一般包括业主单位、承建方、安全工程监理方等。

4) 系统运行

转入运行阶段的电子政务信息系统主要在以下几方面开展信息安全相关工作：

- 按照所建立的信息安全管理体系，定期开展系统的安全宣传、安全培训、安全检查和处理等工作；
- 根据安全策略、安全管理计划的要求，定期对系统开展风险分析、安全性评估等方面的工作；
- 对系统中生成的各类安全相关数据，如：审计记录、安全事件报告、敏感操作记录等，进行分析和处理；
- 运行系统数据备份和恢复系统；
- 建立并维护系统相关的安全知识库，如：漏洞库、入侵检测库、病毒库、补丁库、安全工具库等；
- 建立并维护系统应急响应体系；
- 对系统整体安全策略、管理制度、技术手段等定期进行管理评审。

5) 定期的安全检查和评估

运行阶段要定期对电子政务信息系统开展安全检查和评估，重点的工作内容有：

- 密切跟踪业务系统需求的变化，分析可能的系统调整、升级方式，并分析相应的安全问题；
- 对系统将要发生的调整（如配置修改、软件升级等）进行安全分析，了解这些调整对在用部分造成的安全风险；
- 分析系统调整部分的安全需求和升级后整个系统安全风险的变化。
- 制定系统调整时的安全解决方案；
- 对系统调整后的整体安全性进行分析；

在上述工程实施过程中，需要根据具体的工作内容选择相应的标准开展工作。其中比较重要内容的采标如下节所述。

2.2 采标指南

2.2.1 采标原则

- 必须满足相关主管部门的政策性要求。涉密信息系统，必须优先采用涉密信息系统相关标准。
- 电子政务信息安全领域必须按照相关政策和规定采用国家和国内标准，如需要采用国际和国外标准时，信息系统建设单位应根据国家法规、公共信息安全主管部门、上级行政主管部门、同级信息安全主管部门的相关规定执行。

2.2.2 基础标准和技术与机制标准的采标

我国对密码技术实施严格管理，所有密码相关技术的采用，应以密码主管部门的规定为准。

2.2.3 安全策略

安全策略是电子政务信息系统实施安全工作的出发点，每一个开展电子政务工作的机构都必须制定安全策略，安全策略应该反映组织机构的政务业务。

安全策略规定一个具体的电子政务信息系统中各种信息资产（如：设备、软件、数据等）所允许的操作行为和不允许的操作行为。与一般的具体操作手册、指南不同，安全策略的层面比较高，规定的是更加宏观、原则的内容。安全策略还有一个重要的特点是：与政务机关业务关系密切，要充分反映业务过程中的安全需求。不存在通用的安全策略。

信息安全策略一般包括以下内容：

- a) 信息安全定义，政务机关总目标和范围，信息安全的重要性；
- b) 政务工作说明，以支持信息安全的目的和原则；
- c) 对政务机关特别重要的安全策略、原则、标准和符合性要求的简要说明，例如：法律要求、安全教育要求、业务连续性管理、违反安全策略的后果等。
- d) 安全信息管理（包括：报告安全事故）的总职责和特定职责的定义；
- e) 引用可以支持策略的文件，例如，特定政务系统的更详细的安全策略和规程，或用户应遵守的安全规则。

政务系统的特点决定了电子政务信息系统的安全策略是一个多层次的结构，这与政务机关的组织结构和运行体制是一致的。

信息安全策略是电子政务信息系统安全的基础,要充分反映相应政务机关机构的运行和业务的实际需求,应体现组织、机构核心任务的要求,因此,电子政务的安全策略的制定、认可、实施必须由相应机关的最高领导人负责。我国政务机关实行的是“首长负责制”,信息安全策略的制定是部门、机关最高行政领导的职责之一。

对于指定的政务机关机构来说,制定安全策略必须依据:

- 国家的法令法规;
- 国家的信息安全标准;
- 同级政务机关部门颁布的信息安全规定、标准、规范;
- 上级业务主管部门颁布的信息安全规定、标准、规范;
- 自身政务业务特点的需求。

为安全策略的制定,可以参考的标准有:

- 安全保护等级相关标准:可以参考等级保护相关标准对安全策略的规定,建立电子政务系统等级保护的相关策略;
- 安全管理相关标准:可以根据安全管理相关标准对安全策略制定的规定和建议,利用安全管理相关的标准提供的方法、工具,制定电子政务系统的信息安全策略。安全管理相关的标准总结了经过实践的信息系统安全管理要素,其中包含了安全策略制定的惯例和常用方法,对电子政务系统安全策略的制定有重要的参考意义。

2.2.4. 安全管理

1. 安全域的划分与管理

安全域是指同一个安全策略有效的范围。电子政务信息系统应划分安全域。按照国家政策,电子政务信息系统分为涉密域和非涉密域。每一个域内还可以根据业务性质、信息重要性、单位架构、业务流程等化分为若干子域。安全域相关安全策略的实现必须靠一定的安全措施予以保障。域的划分、实现和管理提可以参考以下标准和规范:

- 国家保密标准
- 等级保护相关标准

2. 安全管理体制

电子政务安全管理体制的建立可以参考安全管理相关标准和国家保密相关标准。其中:

- **GB/T 19716-2005 信息技术 信息安全管理实用规则(等同采用 ISO/IEC 17799:2000)**

本标准是国际标准的等同采用,是对国际上信息安全的最佳实践经验的总结。该标准对信息安全管理涉及的要素进行了描述,对于电子政务系统建立相应的信息安全管理体制有较大的参考意义。在使用该标准时要注意跟国内的实际情况相结合,注意根据自身的实际情况进行裁减和定制。

- **信息安全等级保护 信息系统安全管理要求(即将报批)**

该标准是根据信息安全等级保护的原则而制定的,电子政务系统可以参考该标准建立自己的信息安全“等级化”管理体系。

- **涉及国家秘密的计算机信息系统保密技术要求、涉及国家秘密的计算机信息系统安全保密方案设计指南、涉及国家秘密的计算机信息系统安全保密测评指南、涉及国家秘密的信息系统分级保护技术要求、涉及国家秘密的信息系统分级测评准**

则、涉及国家秘密的信息系统数据备份要求、涉及国家秘密的信息系统应急响应要求

这些标准是对涉及国家秘密的信息系统的规定,其中所包含的有关信息安全管理的内容是电子政务系统,尤其是涉密电子政务系统建立相关管理体系的依据。

2.2.5.安全产品的管理与采购

可以参考相应的技术和机制标准、应用标准。信息安全产品的安全功能实现应该参照技术和机制标准的规定,具体产品的技术指标要求则可以参考应用类安全标准中安全产品和系统相关的标准(标准内容简介可见三章 4.2 节)。

2.2.6. 安全风险分析

安全风险分析是电子政务信息系统建设中最重要的工作之一,是了解信息系统现状,评估安全体系有效性的重要手段。电子政务风险分析可以参考的标准:

- **信息安全风险评估指南(计划研制)**

2.2.7. 安全测试与评估

测试与评估作为是电子政务信息安全体系中不可或缺的、重要一环,对于电子政务系统而言,系统性安全评估是非常重要的一个系统环节。电子政务系统不仅要在建设验收阶段进行系统性的安全评估,运行阶段也需要定期进行安全评估。电子政务系统可以参考的安全评估标准有:

- **GB/T 18336-2001 信息技术 安全技术 信息技术安全性评估准则**
- **信息系统安全保障评估框架(即将报批)**