ICS 35.040
A 90

GA

中华人民共和国公共安全行业标准

GA/T 671—2006

信息安全技术
终端计算机系统安全等级技术要求

Information security technology—
Technology requirement for terminal computer system of security classified protection

2006-12-28 发布　　2007-02-01 实施

中华人民共和国公安部　发布

目　次

标准分享网 www.bzfxw.com 免费下载

前　言

本标准由公安部信息系统安全标准化技术委员会提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心。

本标准主要起草人：邱梓华、顾健、景乾元、李毅、陆臻、赵婷、张笑笑、顾玮、吴其聪。

标准分享网 www.bzfxw.com 免费下载

引　言

本标准用以指导设计者如何设计和实现终端计算机系统，使其达到信息系统所需安全等级，主要从信息系统安全保护等级划分的角度来说明对终端计算机系统的技术要求，即主要说明终端计算机系统为实现 GB 17859—1999 中每一个保护等级的安全要求应采取的安全技术措施，以及各安全技术要求在不同安全等级中具体实现上的差异。

本标准首先对安全等级保护中终端计算机系统所涉及的安全功能技术要求做了比较全面的描述，然后按 GB 17859—1999 五个安全等级的划分，对每一个安全等级的安全功能技术要求和安全保证技术要求做了详细描述。

信息安全技术
终端计算机系统安全等级技术要求

1 范围

本标准规定了对终端计算机系统进行安全等级保护所需要的安全技术要求，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 GB 17859—1999 的安全保护等级要求所进行的终端计算机系统的设计和实现，对于按 GB 17859—1999 的要求对终端计算机系统进行的测试、管理也可参照使用。

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 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 20272—2006 信息安全技术 操作系统安全技术要求

3 术语、定义和缩略语

3.1 术语和定义

GB 17859—1999、GB/T 20271—2006 和 GB/T 20272—2006 确立的以及下列术语和定义适用于本标准。

3.1.1

终端计算机系统 terminal computer system

一种个人使用的计算机系统，是信息系统的重要组成部分，为用户访问网络服务器提供支持。终端计算机系统表现为桌面型计算机系统和膝上型计算机系统两种形态。终端计算机系统一般由硬件系统、操作系统和应用系统(包括为用户访问网络服务器提供支持的工具软件和其他应用软件)等部分组成。

3.1.2

可信 trusted

一种特性，具有该特性的实体总是以预期的行为和方式达到既定目的。

3.1.3

完整性度量(简称度量) measurement of integrity

一种使用密码学杂凑算法对实体计算其杂凑值的过程。

3.1.4

完整性基准值(简称基准值) criteria of integrity measurement

实体在可信状态下度量得到的杂凑值，可用来作为完整性校验基准。

3.1.5

度量根 root of trust for measurement

一个可信的实体，是终端计算机系统内进行可信度量的基点。

标准分享网 www.bzfxw.com 免费下载

3.1.6

动态度量根　dynamic root of trust for measurement

度量根的一种，支持终端计算机系统对动态启动的程序模块进行实时可信度量。

3.1.7

存储根　root of trust for storage

一个可信的实体，是终端计算机系统内进行可信存储的基点。

3.1.8

报告根　root of trust for reporting

一个可信的实体，是终端计算机系统内进行可信报告的基点。

3.1.9

可信根　trusted root

度量根、存储根和报告根的集合，是保证终端计算机系统可信的基础。

3.1.10

可信硬件模块　trusted hardware module

嵌入终端计算机硬件系统内的一个硬件模块。它必须包含存储根、报告根，能独立提供密码学运算功能，具有受保护的存储空间。

3.1.11

信任链　trusted chains

一种在终端计算机系统启动过程中，基于完整性度量的方法确保终端计算机系统可信的技术。

3.1.12

可信计算平台　trusted computing platform

基于可信硬件模块或可信软件模块构建的计算平台，支持系统身份标识服务、密码学服务和信任服务，并为系统提供信任链保护和运行安全保护。

3.1.13

终端计算机系统安全子系统　security subsystem of terminal computer system (SSOTCS)

终端计算机系统内安全保护装置的总称，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的终端计算机系统安全保护环境，并提供终端计算机系统所要求的附加用户服务。终端计算机系统安全子系统应从硬件系统、操作系统、应用系统和系统运行等方面对终端计算机系统进行安全保护。

注：按照 GB 17859—1999 对 TCB(可信计算基)的定义，SSOTCS(终端计算机系统安全子系统)就是终端计算机系统的 TCB。

3.1.14

SSOTCS 安全功能　SSOTCS security function

正确实施 SSOTCS 安全策略的全部硬件、固件、软件所提供的功能。每一个安全策略的实现，组成一个安全功能模块。一个 SSOTCS 的所有安全功能模块共同组成该 SSOTCS 的安全功能。

3.1.15

SSOTCS 安全控制范围　SSOTCS scope of control

SSOTCS 的操作所涉及的主体和客体。

3.1.16

SSOTCS 安全策略　SSOTCS security policy

对 SSOTCS 中的资源进行管理、保护和分配的一组规则。一个 SSOTCS 中可以有一个或多个安全策略。

3.2　缩略语

下列缩略语适用于本标准。

SSOTCS　终端计算机系统安全子系统　security subsystem of terminal computer system
SSF　SSOTCS 安全功能　SSOTCS security function
SSC　SSOTCS 控制范围　SSOTCS scope of control
SSP　SSOTCS 安全策略　SSOTCS security policy
TCP　可信计算平台　trusted computer platform

4　安全功能技术要求

4.1　物理安全

4.1.1　设备安全可用

根据不同安全等级的不同要求，终端计算机系统的设备安全可用分为：

a)　基本运行支持：终端计算机系统的设备应提供基本的运行支持，并有必要的容错和故障恢复能力；

b)　基本安全可用：终端计算机系统的设备应满足基本安全可用的要求，包括主机、外部设备、网络连接部件及其他辅助部件等均应基本安全可用；

c)　不间断运行支持：终端计算机系统的设备应通过故障容错和故障恢复等措施，为终端计算机系统的不间断运行提供支持。

4.1.2　设备防盗防毁

根据不同安全等级的不同要求，终端计算机系统的设备防盗防毁分为：

a)　设备标记要求：终端计算机系统的设备应有明显的无法除去的标记，以防更换和方便查找；

b)　主机实体安全：终端计算机系统的主机应有机箱封装保护，防止部件损害或被盗；

c)　设备的防盗和自销毁要求：终端计算机系统的设备应提供拥有者可控的防盗报警功能和系统自销毁功能。

4.1.3　设备高可靠

根据特殊环境应用要求，终端计算机系统设备高可靠分为：

a)　防水要求：终端计算机系统应具有高密封性，防止水滴进入；

b)　防跌落和防震要求：终端计算机系统应加固保护，防止跌落和震动引起的系统损坏；

c)　抗高低温与高低气压要求：终端计算机系统应能适应高低温和高低气压环境；

d)　抗电磁辐射与干扰：终端计算机系统应能抵御电磁干扰和电磁辐射对系统的安全威胁。

4.2　运行安全

4.2.1　系统安全性检测分析

根据不同安全等级的不同要求，终端计算机系统的安全性检测分析分为：

a)　操作系统安全性检测分析：应从终端计算机操作系统的角度，以管理员身份评估文件许可、文件宿主、网络服务设置、账户设置、程序真实性以及一般的与用户相关的安全点、入侵迹象等，从而检测和分析操作系统的安全性，发现存在的安全隐患，并提出补救措施；

b)　硬件系统安全性检测分析：应对支持终端计算机系统运行的硬件系统进行安全性检测，通过扫描硬件系统中与系统运行和数据保护有关的特定安全脆弱性，分析其存在的缺陷和漏洞，提出补救措施；

c)　应用程序安全性检测分析：应对运行在终端计算机系统中的应用程序进行安全性检测分析，通过扫描应用软件中与鉴别、授权、访问控制和系统完整性有关的特定的安全脆弱性，分析其存在的缺陷和漏洞，提出补救措施；

d)　电磁泄露发射检测分析：应对运行中的终端计算机系统环境进行电磁泄露发射检测，采用专门的检测设备，检查系统运行过程中由于电磁干扰和电磁辐射对终端计算机系统的安全性所造成的威胁，并提出补救措施。

标准分享网 www.bzfxw.com 免费下载

4.2.2 安全审计

4.2.2.1 安全审计的响应

根据不同安全等级的不同要求，终端计算机系统的安全审计的响应分为：

a) 记审计日志：当检测到可能有安全侵害事件时，将审计数据记入审计日志；

b) 实时报警生成：当检测到可能有安全侵害事件时，生成实时报警信息；

c) 违例进程终止：当检测到可能有安全侵害事件时，将违例进程终止，违例进程可以包括但不限于服务进程、驱动、用户进程；

d) 用户账号断开与失效：当检测到可能有安全侵害事件时，将当前的用户账号断开，并使其失效。

4.2.2.2 安全审计数据产生

根据不同安全等级的不同要求，终端计算机系统的安全审计数据的产生分为：

a) 为下述可审计事件产生审计记录：审计功能的启动和关闭、终端计算机对用户使用身份鉴别机制、管理员用户和普通用户所实施的与安全相关的操作；

b) 对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件类别，及其他与审计相关的信息；

c) 对于身份鉴别事件，审计记录应包含请求的来源；

d) 将每个可审计事件与引起该事件的用户或进程相关联；

e) 为下述可审计事件产生审计记录：将客体引入用户地址空间(例如：打开文件、服务初始化)、其他与系统安全有关的事件或专门定义的可审计事件；

f) 对于客体被引入用户地址空间的事件，审计记录应包含客体名及客体的安全等级；

g) 对机密性数据的创建、使用与删除事件，审计记录应包含机密性数据的安全标记。

4.2.2.3 安全审计分析

根据不同安全等级的不同要求，终端计算机系统的安全审计分析分为：

a) 潜在侵害分析：应能用一系列规则去监控审计事件，并根据这些规则指出 SSP 的潜在侵害；

b) 基于异常检测的描述：应能确立用户或进程的质疑度(或信誉度)，该质疑度表示该用户或进程的现行活动与已建立的使用模式的一致性程度。当用户或进程的质疑等级超过门限条件时，SSF 应能指出将要发生对安全性的威胁；

c) 简单攻击探测：应能检测到对 SSF 实施有重大威胁的签名事件的出现，并能通过对一个或多个事件的对比分析或综合分析，预测一个攻击的出现以及出现的时间或方式。为此，SSF 应维护指出对 SSF 侵害的签名事件的内部表示，并将检测到的系统行为记录与签名事件进行比较，当发现两者匹配时，指出一个对 SSF 的攻击即将到来；

d) 复杂攻击探测：在上述简单攻击探测的基础上，要求 SSF 应能检测到多步入侵情况，并能根据已知的事件序列模拟出完整的入侵情况，还应指出发现对 SSF 的潜在侵害的签名事件或事件序列的时间。

4.2.2.4 安全审计查阅

根据不同安全等级的不同要求，终端计算机系统的安全审计查阅分为：

a) 审计查阅：提供从审计记录中读取信息的能力，即要求 SSF 为授权用户提供获得和解释审计信息的能力；

b) 受控审计查阅：审计查阅工具应只允许授权用户读取审计信息，并根据某种逻辑关系的标准提供对审计数据进行搜索、分类、排序的能力。

4.2.2.5 安全审计事件选择

应根据以下属性选择终端计算机系统的可审计事件：

a) 客体身份、用户身份、主体身份、主机身份、事件类型；

b) 作为审计选择性依据的附加属性。

4.2.2.6 安全审计事件存储

根据不同安全等级的不同要求，终端计算机系统的安全审计事件存储分为：

a) 受保护的审计踪迹存储：要求审计踪迹的存储受到应有的保护，应能检测或防止对审计记录的修改；

b) 审计数据的可用性确保：在意外情况出现时，应能检测或防止对审计记录的修改，以及在发生审计存储已满、存储失败或存储受到攻击以及意外情况出现时，应采取相应的保护措施，确保有实效性的审计记录不被破坏；

c) 审计数据可能丢失情况下的措施：当审计跟踪超过预定的门限时，应采取相应的措施，进行审计数据可能丢失情况的处理；

d) 防止审计数据丢失：在审计踪迹存储已满或超过预定的门限时，应采取相应措施，防止审计数据丢失。

4.2.3 信任链

应通过在终端计算机系统启动过程中提供的信任链支持，确保终端计算机系统的运行处于真实可信状态。根据不同安全等级的不同要求，信任链功能分为：

a) 静态信任链建立：利用终端计算机系统上的度量根，在系统启动过程中对 BIOS、MBR、OS 部件模块进行完整性度量。每个部件模块在加载前应确保其真实性和完整性；

b) 静态信任链中操作系统(OS)的完整性度量基准值接受国家专门机构管理，支持在线或离线校验；

c) 动态信任链建立：利用终端计算机系统上的动态度量根，对操作系统上应用程序进行实时的完整性度量，确保每个应用程序在启动和运行中的真实性和完整性；

d) 动态信任链中应用程序的完整性度量基准值接受国家专门机构管理，支持在线或离线校验；

e) 信任链模块修复：支持在被授权的情况下，对信任链建立过程中出现的不可信模块进行实时修复；

f) 信任链模块升级：支持在被授权的情况下，对信任链建立过程中涉及的各个部件的模块进行升级。每个升级模块均应确保其真实性和完整性。

4.2.4 运行时防护

4.2.4.1 恶意代码防护

恶意代码是对用户使用终端计算机系统造成破坏或影响的程序代码，比如：病毒、蠕虫、特洛伊木马和恶意软件等。

根据不同安全等级要求，终端计算机系统的恶意代码防护应分为：

a) 外来介质使用控制：严格控制各种外来介质的使用，防止恶意代码通过介质传播；

b) 特征码扫描：对文件系统和内存采用特征码扫描，并根据扫描结果采取相应措施，清除或隔离恶意代码。恶意代码特征库应及时更新；

c) 基于 CPU 的数据执行保护：防止缓冲区溢出，阻止从受保护的内存位置执行恶意代码；

d) 进程隔离：采用进程逻辑隔离或物理隔离的方法，保护进程免受恶意代码破坏；

e) 进程行为分析：基于专家系统，对进程行为的危险程度进行等级评估，根据评估结果，采取相应防护措施。

4.2.4.2 网络攻击防护

终端计算机系统应采取必要措施监控主机与外部网络的数据通信，确保系统免受外部网络侵害或恶意远程控制。应采取的措施包括：

a) 防火墙功能：

——IP 包过滤：应能够支持基于源地址、目的地址的访问控制，将不符合预先设定策略的数据包丢弃；

标准分享网 www.bzfxw.com 免费下载

——网络协议分析：应能够支持基于网络协议类型的访问控制；

——应用程序监控：应能够设置应用程序对网络的访问控制规则，包括对端口、协议、访问方向的控制；

——内容过滤：应能对网页内容进行基于关键字匹配的过滤。

b) 入侵检测功能：

——实时阻断：及时阻断严重的网络入侵行为；

——文件监控：防止用户对保护文件的非法访问与误操作；

——注册表监控：防止用户对注册表的非法访问与误操作；

——事件监测：及时检测到主机异常事件；

——实时流量分析：对主机网络流量进行实时监测与分析，并据此判断是否有入侵事件发生。

4.2.4.3 网络接入控制

终端计算机系统应能对所接入网络进行可信度评价，并根据不同可信度评价等级采取不同的安全接入策略。

4.2.5 备份与故障恢复

为了实现确定的恢复功能，应在终端计算机系统正常运行时定期地或按某种条件实施备份。根据不同安全等级的不同要求，备份与故障恢复分为：

a) 用户数据备份与恢复：应提供用户有选择地备份重要数据的功能，当由于某种原因引起终端计算机系统中用户数据丢失或破坏时，应能提供用户数据恢复的功能；

b) 增量信息备份与恢复：应提供由终端计算机系统定时对新增信息进行备份的功能；当由于某种原因引起终端计算机系统中的某些信息丢失或破坏时，应提供用户按增量信息备份所保留的信息进行信息恢复的功能；

c) 局部系统备份与恢复：应提供定期对终端计算机系统的某些重要的局部系统的运行现场进行定期备份的功能；当由于某种原因引起终端计算机系统某一局部发生故障时，应提供用户按局部系统备份所保留的现场信息进行局部系统恢复的功能；

d) 全系统备份与恢复：应提供定期对终端计算机系统全系统的运行现场进行备份的功能；当由于某种原因引起终端计算机系统全系统发生故障时，应提供用户按全系统备份所保留的现场信息进行全系统恢复的功能；

e) 备份保护措施：数据在备份、存储和恢复过程中应有安全保护措施，并应设置不被用户操作系统管理的系统来实现系统数据的备份与恢复功能，系统备份数据是用户操作系统不可访问的。

4.2.6 可信时间戳

终端计算机系统应为其运行提供可靠的时钟和时钟同步系统，并按 GB/T 20271—2006 的要求提供可信时间戳服务。

4.2.7 I/O 接口配置

终端计算机系统应根据不同的环境要求，配置串口、并口、PCI、USB、网卡、硬盘等各类 I/O 接口和设备的启用/禁用等状态：

a) 用户自主配置：应支持用户基于 BIOS 和操作系统提供的功能自主配置各类接口的状态；

b) 集中管理配置：终端计算机系统应接受所接入网络的接口配置管理，并确保只有授权用户才能修改接口配置；

c) 自适应配置：终端计算机系统应能根据网络环境安全状况，基于安全策略，自动配置接口状态，以确保系统自身安全。

4.3 数据安全

4.3.1 密码支持

4.3.1.1 密码算法要求

应采用国家有关主管部门批准的密码算法及使用指南来实现终端计算机系统密码支持功能。密码算法种类和范围包括：对称密码算法、公钥密码算法、杂凑算法、随机数生成算法。

根据不同安全等级要求，密码算法实现分为：

a) 密码算法采用软件实现；

b) 密码算法采用硬件实现。

4.3.1.2 密码操作

应按照密码算法要求实现密码操作，并至少支持如下操作：密钥生成操作、数据加密和解密操作、数字签名生成和验证操作、数据完整性度量生成和验证操作、消息认证码生成与验证操作、随机数生成操作。

4.3.1.3 密钥管理

应对密码操作所使用的密钥进行全生命周期管理，包括密钥生成、密钥交换、密钥存取、密钥废除。密钥管理应符合国家密钥管理标准要求(参见：GB/T 17901.1—1999)。

4.3.2 身份标识与鉴别

4.3.2.1 系统标识

终端计算机系统应在用户使用之前对系统进行身份标识：

a) 唯一性标识：应通过唯一绑定的可信硬件模块产生的密钥来标识系统身份；系统身份标识应与审计相关联；

b) 标识可信性：身份标识可信性应通过权威机构颁发证书来实现；

c) 隐秘性：需要时应使系统身份标识在某些特定条件下具有不可关联性。可以基于第三方权威机构颁发特定证书实现系统身份标识的隐秘性；

d) 标识信息管理：应对终端计算机系统身份标识信息进行管理、维护，确保其不被非授权地访问、修改或删除。

4.3.2.2 系统鉴别

应对请求访问的终端计算机系统进行身份鉴别，鉴别时请求方应提供系统完整性度量值报告。

4.3.2.3 用户标识

应对注册到终端计算机系统的用户进行标识。根据不同安全等级的不同要求，用户标识分为：

a) 基本标识：应在 SSF 实施所要求的动作之前，先对提出该动作要求的用户进行标识；

b) 唯一性标识：应确保所标识用户在信息系统生命周期内的唯一性，并将用户标识与审计相关联；

c) 标识信息管理：应对用户标识信息进行管理、维护，确保其不被非授权地访问、修改或删除。

4.3.2.4 用户鉴别

应对终端计算机系统用户进行身份真实性鉴别。通过对用户所提供的“鉴别信息”的验证，证明该用户确有所声称的某种身份，这里“鉴别信息”可以是用户口令、数字证书、IC 卡、指纹、虹膜等。

根据不同安全等级的不同要求，用户鉴别分为：

a) 基本鉴别：应在 SSF 实施所要求的动作之前，先对提出该动作要求的用户成功地进行鉴别；

b) 不可伪造鉴别：应检测并防止使用伪造或复制的鉴别信息。一方面，要求 SSF 应检测或防止由任何别的用户伪造的鉴别数据，另一方面，要求 SSF 应检测或防止当前用户从任何其他用户处复制的鉴别数据的使用；

c) 一次性使用鉴别：应能提供一次性使用鉴别数据操作的鉴别机制，即 SSF 应防止与已标识过的鉴别机制有关的鉴别数据的重用；

d) 多机制鉴别：应能提供不同的鉴别机制，用于鉴别特定事件的用户身份，并且 SSF 应根据所描述的多种鉴别机制如何提供鉴别的规则，来鉴别任何用户所声称的身份；

标准分享网 www.bzfxw.com 免费下载

e) 重新鉴别：应有能力规定需要重新鉴别用户的事件，即 SSF 应在需要重鉴别的条件表所指示的条件下，重新鉴别用户。例如，用户操作超时被断开后，重新连接时需要进行重鉴别。

4.3.2.5 用户鉴别失败处理

要求 SSF 为不成功的鉴别尝试次数（包括尝试次数和时间的阈值）定义一个值，以及明确规定达到该值时所应采取的动作。鉴别失败的处理应包括检测出现相关的不成功鉴别尝试的次数与所规定的数目相同的情况，并进行预先定义的处理。应通过对不成功的鉴别尝试次数（包括尝试次数和时间的阈值）的值进行预先定义，以及明确规定达到该值时所应采取的动作来实现鉴别失败的处理。

4.3.2.6 用户-主体绑定

在 SSC 之内，对一个已标识和鉴别的用户，为了要求 SSF 完成某个任务，需要激活另一个主体（如进程），这时，要求通过用户-主体绑定将该用户与该主体相关联，从而将用户的身份与该用户的所有可审计行为相关联。

4.3.2.7 隐秘

应为用户提供其身份不被其他用户发现或滥用的保护，可分为以下四种情况：

a) 匿名：用户在其使用资源或服务时，不暴露身份。要求 SSF 应确保用户和/或主体集，无法确定与主体和/或操作相关联的实际用户，并在对主体提供服务时不询问实际的用户名；

b) 假名：用户在使用资源或设备时，不暴露其真实名称，但仍能对该次使用负责。要求 SSF 应确保用户和/或主体集，不能确定与主体和/或操作相关联的真实的用户名，并要求 SSF 应能给一个主体提供多个假名，以及验证所使用的假名是否符合假名的度量；

c) 不可关联性：一个用户可以多次使用资源和服务，但任何人都不能将这些使用联系在一起。具体讲，要求 SSF 应确保用户和/主体不能确定系统中的某些操作是否由同一用户引起；

d) 不可观察性：用户在使用资源和服务时，其他人，特别是第三方不能观察到该资源和服务正在被使用。要求 SSF 应确保用户和/或主体，不应观察到由受保护的用户和/或主体对客体所进行的操作。可通过将不可观察性信息分配给 SSF 的不同部分等方法实现。

4.3.3 自主访问控制

4.3.3.1 访问控制策略

应按确定的自主访问控制安全策略进行设计，实现对策略控制下的主体与客体间操作的控制。可以有多个自主访问控制安全策略，但它们应独立命名，且不应相互冲突。常用的自主访问控制策略包括：访问控制表访问控制、目录表访问控制、权能表访问控制等。

4.3.3.2 访问控制功能

应明确指出采用一条命名的访问控制策略所实现的特定功能，说明策略的使用和特征，以及该策略的控制范围。

无论采用何种自主访问控制策略，应有能力提供：

——在安全属性或命名的安全属性组的客体上，执行访问控制策略；

——在基于安全属性的允许主体对客体访问的规则的基础上，允许主体对客体的访问；

——在基于安全属性的拒绝主体对客体访问的规则的基础上，拒绝主体对客体的访问。

4.3.3.3 访问控制范围

根据不同安全等级的不同要求，自主访问控制的覆盖范围分为：

a) 子集访问控制：要求每个确定的自主访问控制，SSF 应覆盖由 SSOTCS 所定义的主体、客体及其之间的操作；

b) 完全访问控制：要求每个确定的自主访问控制，SSF 应覆盖终端计算机系统中所有的主体、客体及其之间的操作，即要求 SSF 应确保 SSC 内的任意一个主体和任意一个客体之间的所有操作将至少被一个确定的访问控制策略覆盖。

4.3.3.4 访问控制粒度

根据不同安全等级的不同要求，自主访问控制的粒度分为：

a) 主体为用户组/用户级，客体为文件级；

b) 主体为用户级，客体为文件级。

4.3.4 标记

4.3.4.1 主体标记

主体是指主动的实体，是SSC内发起操作的实体。主体通常包括人、进程和外部设备等。

应为主体分配标记，这些标记是等级分类和非等级类别的组合，是实施强制访问控制的依据。

4.3.4.2 客体标记

客体是被动的实体，是SSC内被主体访问的实体。客体包含或者接收主体关心的信息。客体通常包括文件、设备、状态信息等。

应为客体指定敏感标记，这些敏感标记是等级分类和非等级类别的组合，是实施强制访问控制的依据。

4.3.5 强制访问控制

4.3.5.1 访问控制策略

强制访问控制策略应包括策略控制下的主体、客体，及由策略覆盖的被控制的主体与客体间的操作。可以有多个访问控制安全策略，但它们应独立命名，且不应相互冲突。

4.3.5.2 访问控制功能

应明确指出采用一条命名的强制访问控制策略所实现的特定功能。应有能力提供：

——在标记或命名的标记组的客体上，执行访问控制策略；

——按受控主体和受控客体之间的允许访问规则，决定允许受控主体对受控客体执行受控操作；

——按受控主体和受控客体之间的拒绝访问规则，决定拒绝受控主体对受控客体执行受控操作。

4.3.5.3 访问控制范围

根据不同安全等级的不同要求，强制访问控制的覆盖范围分为：

a) 子集访问控制：要求每个确定的强制访问控制，应覆盖由策略所定义的主体、客体及其之间的操作；

b) 完全访问控制：要求每个确定的强制访问控制，应覆盖终端计算机系统中所有的主体、客体及其之间的操作，即要求终端计算机系统中的任意一个主体和任意一个客体之间的所有操作将至少被一个确定的访问控制策略覆盖。

4.3.5.4 访问控制粒度

根据不同安全等级的不同要求，强制访问控制的粒度分为：

a) 主体为用户组/用户级，客体为文件级；

b) 主体为用户级，客体为文件级。

4.3.6 数据保密性保护

4.3.6.1 数据存储保密性

应对存储在SSC内的重要用户数据进行保密性保护，确保除合法持有密钥者外，其余任何用户不应获得该数据。

a) 数据加密：应确保加密后的数据由密钥的合法持有者解密；

b) 数据绑定：基于存储根实现对数据的保密存储，应确保数据由密钥的合法持有者在特定终端计算机系统中解密；

c) 数据密封：基于存储根实现对数据的保密存储，应确保数据由密钥的合法持有者在特定终端计算机系统的特定状态下解密。

标准分享网 www.bzfxw.com 免费下载

4.3.6.2 数据传输保密性

对在不同 SSF 之间传输的用户数据，应根据不同数据类型的不同保密性要求，进行不同程度的保密性保护，确保数据在传输过程中不被泄漏和窃取。

4.3.6.3 客体安全重用

在对资源进行动态管理的系统中，客体资源（寄存器、内存、磁盘等记录介质）中的剩余信息不应引起信息的泄漏。根据不同安全等级对用户数据保密性保护的不同要求，客体安全重用分为：

a) 子集信息保护：由 SSOTCS 安全控制范围之内的某个子集的客体资源，在将其释放后再分配给某一用户或代表该用户运行的进程时，应不会泄漏该客体中的原有信息；

b) 完全信息保护：由 SSOTCS 安全控制范围之内的所有客体资源，在将其释放后再分配给某一用户或代表该用户运行的进程时，应不会泄漏该客体中的原有信息；

c) 特殊信息保护：在完全信息保护的基础上，对于某些需要特别保护的信息，应采用专门的方法对客体资源中的残留信息做彻底清除，如对剩磁的清除等。

4.3.7 数据完整性保护

4.3.7.1 存储数据的完整性

应对存储在 SSC 内的用户数据进行完整性保护，包括：

a) 完整性检测：要求 SSF 应对基于用户属性的所有客体，对存储在 SSC 内的用户数据进行完整性检测；

b) 完整性检测和恢复：要求 SSF 应对基于用户属性的所有客体，对存储在 SSC 内的用户数据进行完整性检测，并且当检测到完整性错误时，SSF 应采取必要的恢复措施。

4.3.7.2 传输数据的完整性

当用户数据在 SSF 和其他可信信息系统间传输时应提供完整性保护，包括：

a) 完整性检测：要求对被传输的用户数据进行检测，及时发现以某种方式传送或接收的用户数据被篡改、删除、插入等情况发生；

b) 数据交换恢复：由接收者 SSOTCS 借助于源可信信息系统提供的信息，或由接收者 SSOTCS 自己无须来自源可信信息系统的任何帮助，能恢复被破坏的数据为原始的用户数据。

4.3.7.3 处理数据的完整性

回退：对终端计算机系统中处理中的数据，应通过“回退”进行完整性保护，即要求 SSF 应执行访问控制策略，以允许对所定义的操作序列进行回退。

4.3.8 信任服务

信任服务是指终端计算机系统运行时对自身进行完整性度量，并将度量值向系统用户或系统外部实体进行可信报告的服务，即由报告根对度量值进行数字签名后，呈现给验证者。

4.3.8.1 完整性度量

终端计算机系统中的硬件、固件和软件等系统模块在运行之前应对其进行完整性度量，作为该模块的可信性判断依据。

应通过适当组合各模块的度量值，作为系统信任报告或系统特征绑定的依据。

4.3.8.2 完整性度量值存储

终端计算机系统应专门设置一组受保护的存储区域，用于存储被度量模块的完整性度量值。

所有度量值存取访问应受权限控制。

4.3.8.3 完整性度量值报告

报告完整性度量值时，系统报告根应对完整性度量值进行数字签名，报告接收方通过验证签名有效性以及校验完整性度量值来判断该系统的信任性。

4.3.9 可信路径

用户与 SSF 间的可信路径应满足：

a) SSF 应在 SSF 和本地或远程用户之间提供一个通信路径，通信路径之间彼此逻辑独立，提供真实的端点标识，并保护通信数据免遭修改和泄露；

b) SSF 应允许 SSF、本地或远程用户通过可信路径发起通信；

c) SSF 应对原发用户的鉴别、内部命令、所有用户命令和 SSF 响应使用可信路径。

5 终端计算机系统安全技术分等级要求

5.1 第一级：用户自主保护级

5.1.1 安全功能要求

5.1.1.1 物理系统

5.1.1.1.1 设备安全可用

应按 4.1.1 中基本运行支持的要求，设计和实现终端计算机系统设备安全可用的功能。

5.1.1.1.2 设备防盗防毁

应按 4.1.2 中设备标记的要求，设计和实现终端计算机系统的设备防盗防毁的功能。

5.1.1.2 操作系统

应按 GB/T 20272—2006 中 4.1.1 的要求，从以下方面来设计、实现或选购用户自主保护级终端计算机系统所需要的操作系统：

a) 用户身份标识与鉴别：根据 GB/T 20272—2006 中 4.1.1.1 描述，实现操作系统用户标识、用户鉴别、用户鉴别失败处理和用户-主体绑定的功能；

b) 自主访问控制：根据 GB/T 20272—2006 中 4.1.1.2 的描述，对操作系统的访问进行控制，允许合法操作，不允许非法操作；

c) 用户数据完整性：根据 GB/T 20272—2006 中 4.1.1.7 的描述，对操作系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能。

5.1.1.3 可信计算平台

5.1.1.3.1 密码支持

应以 4.3.1 的描述，并按以下要求，设计与实现自主保护级终端计算机系统密码支持功能：

a) 应采用国家有关主管部门批准的密码算法，利用软件实现相关密码算法和密码操作；

b) 密钥管理：所有密钥应受存储根保护。

5.1.1.3.2 信任链

应按 4.2.3 中信任链建立的要求，设计和实现终端计算机系统的静态信任链功能。

静态信任链所建立的度量值应存储在一个受保护的区域中。

5.1.1.3.3 运行时防护

应按 4.2.4 的运行时防护的要求，设计和实现如下功能：

恶意代码防护：根据 4.2.4.1 的描述，实现外来介质使用控制、特征码扫描的功能。

5.1.1.3.4 系统安全性检测分析

应按 4.2.1 终端计算机操作系统安全性检测分析的要求，运用有关工具，检测所选用或开发的操作系统，并通过对检测结果的分析，按用户自主保护级的要求，对存在的安全问题加以改进。

5.1.1.3.5 备份与故障恢复

应按 4.2.5 中用户数据备份与恢复、增量信息备份与恢复的要求，设计和实现终端计算机系统的备份与故障恢复功能。

5.1.1.3.6 I/O 接口配置

应按 4.2.7 中用户自主配置的要求，设计和实现 I/O 接口配置功能。

5.1.1.4 应用系统

应按 GB/T 20271—2006 中 6.1.3 的要求，从以下方面来设计、实现或选购用户自主保护级终端计

标准分享网 www.bzfxw.com 免费下载

算机系统所需要的应用系统：

a) 身份标识与鉴别：根据 GB/T 20271—2006 中 6.1.3.1 描述，实现用户标识、用户鉴别、用户鉴别失败处理和用户-主体绑定的功能；

b) 自主访问控制：根据 GB/T 20271—2006 中 6.1.3.2 的描述，对应用系统相关资源的访问进行控制，允许合法操作，不允许非法操作；

c) 数据完整性保护：根据 GB/T 20271—2006 中 6.1.3.3 的描述，对应用系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能。

5.1.2 安全保证要求

5.1.2.1 SSOTCS 自身安全保护

a) 可信根安全保护：应按以下要求实现终端计算机系统的可信根：

——应保护存储根不被泄漏和窜改；

——应对度量根采取物理保护措施。

b) SSF 物理安全保护：按 GB/T 20271—2006 中 6.1.4.1 的要求，实现终端计算机系统用户自主保护级 SSF 的物理安全保护。

c) SSF 运行安全保护：按 GB/T 20271—2006 中 6.1.4.2 的要求，实现终端计算机系统用户自主保护级 SSF 的运行安全保护。

d) SSF 数据安全保护：按 GB/T 20271—2006 中 6.1.4.3 的要求，实现终端计算机系统用户自主保护级 SSF 的数据按保护。

e) 资源利用：按 GB/T 20271—2006 中 6.1.4.4 的要求，实现终端计算机系统用户自主保护级的资源利用。

f) SSOTCS 访问控制：按 GB/T 20271—2006 中 6.1.4.5 的要求，实现终端计算机系统用户自主保护级的 SSOTCS 访问控制。

5.1.2.2 SSOTCS 设计和实现

a) 配置管理：按 GB/T 20271—2006 中 6.1.5.1 的要求，实现终端计算机系统用户自主保护级的配置管理；

b) 分发和操作：按 GB/T 20271—2006 中 6.1.5.2 的要求，实现终端计算机系统用户自主保护级的分发和操作；

c) 开发：按 GB/T 20271—2006 中 6.1.5.3 的要求，实现终端计算机系统用户自主保护级的开发；

d) 指导性文档：按 GB/T 20271—2006 中 6.1.5.4 的要求，实现终端计算机系统用户自主保护级的指导性文档；

e) 生命周期支持：按 GB/T 20271—2006 中 6.1.5.5 的要求，实现终端计算机系统用户自主保护级的生命周期支持；

f) 测试：按 GB/T 20271—2006 中 6.1.5.6 的要求，实现终端计算机系统用户自主保护级的测试。

5.1.2.3 SSOTCS 管理

按 GB/T 20271—2006 中 6.1.6 的要求，实现终端计算机系统用户自主保护级的 SSOTCS 安全管理。

5.2 第二级：系统审计保护级

5.2.1 安全功能要求

5.2.1.1 物理系统

5.2.1.1.1 设备安全可用

应按 4.1.1 中基本运行支持的要求，设计和实现终端计算机系统设备安全可用的功能。

5.2.1.1.2 **设备防盗防毁**

应按 4.1.2 中设备标记要求和主机实体安全的要求，设计和实现终端计算机系统的设备防盗防毁的功能。

5.2.1.2 **操作系统**

应按 GB/T 20272—2006 中 4.2.1 的要求，从以下方面来设计、实现或选购系统审计保护级终端计算机系统所需要的操作系统：

a) 身份鉴别：根据 GB/T 20272—2006 中 4.2.1.1 的描述，实现操作系统用户标识、用户鉴别、用户鉴别失败处理和用户-主体绑定的功能；

b) 自主访问控制：根据 GB/T 20272—2006 中 4.2.1.2 的描述，对操作系统的访问进行控制，允许合法操作，不允许非法操作；

c) 安全审计：应根据 GB/T 20272—2006 中 4.2.1.3 的描述，提供操作系统安全审计功能；

d) 用户数据保密性：根据 GB/T 20272—2006 中 4.2.1.5 的描述，设计和实现操作系统的用户数据保密性保护功能；

e) 用户数据完整性：根据 GB/T 20272—2006 中 4.2.1.4 的描述，对操作系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能。

5.2.1.3 **可信计算平台**

5.2.1.3.1 **密码支持**

应以 4.3.1 的描述，并按以下要求，设计与实现安全标记级终端计算机系统密码支持功能：

a) 密码算法：应使用国家密码管理部门批准的密码算法，应支持密码算法和密码操作由硬件实现；

b) 密钥管理：所有密钥应受存储根保护，存储根本身应由可信硬件模块保护。

5.2.1.3.2 **信任链**

应按 4.2.3 中信任链建立的要求，基于可信硬件模块设计和实现终端计算机系统的静态信任链功能。

5.2.1.3.3 **运行时防护**

应按 4.2.4 的运行时防护的要求，设计和实现如下功能：

a) 恶意代码防护：根据 4.2.4.1 的描述，实现外来介质使用控制、特征码扫描的功能；

b) 网络攻击防护：根据 4.2.4.2 的描述，实现 IP 过滤、网络协议分析、应用程序监控、内容过滤的防火墙功能。

5.2.1.3.4 **系统安全性检测分析**

应按 4.2.1 终端计算机操作系统安全性检测分析和硬件系统安全性检测分析的要求，运用有关工具，检测所选用或开发的操作系统、硬件系统，并通过对检测结果的分析，按系统审计保护级的要求，对存在的安全问题加以改进。

5.2.1.3.5 **信任服务**

应根据 4.3.8 的描述及以下要求，设计与实现可信计算平台的系统审计保护级信任服务功能：

应在可信硬件模块中专门设置受保护区域存储所有静态信任链的完整性度量值。

5.2.1.3.6 **用户身份标识与鉴别**

应按 4.3.2 的要求，从以下方面设计和实现可信计算平台用户身份标识与鉴别功能：

a) 应按 4.3.2.3 的要求，设计与实现用户的基本标识、唯一性标识与标识信息管理功能；

b) 应按 4.3.2.4 的要求，设计与实现用户的基本鉴别、不可伪造鉴别功能；

c) 应按 4.3.2.4 的要求，支持以数字证书形式提供鉴别信息；

d) 应按 4.3.2.5 的要求，设计与实现用户鉴别失败处理功能；

e) 应按 4.3.2.6 的要求，设计与实现用户-主体绑定功能。

标准分享网 www.bzfxw.com 免费下载

5.2.1.3.7 自主访问控制

可按 4.3.3 自主访问控制的要求，从以下方面设计和实现可信计算平台的自主访问控制功能：

a) 按 4.3.3.1 的要求，确定自主访问控制策略；

b) 按 4.3.3.2 的要求，设计和实现自主访问控制功能；

c) 按 4.3.3.3 中子集访问控制的要求，确定自主访问控制的范围；

d) 按 4.3.3.4 中访问控制粒度的要求，确定自主访问控制的粒度。

5.2.1.3.8 数据保密性保护

应按 4.3.6 的要求，从以下方面设计和实现可信计算平台的数据保密性保护功能：

a) 应按 4.3.6.1 中数据加密的要求，按 4.3.1 所配置的密码支持，对需要进行存储保密性保护的数据，采用存储加密的措施，设计和实现数据存储保密性保护功能；

b) 应按 4.3.6.2 的要求，按 4.3.1 所配置的密码支持，对需要进行传输保密性保护的数据，采用传输加密的措施，设计和实现数据传输保密性保护功能。

5.2.1.3.9 数据完整性保护

根据 4.3.7 的描述，对可信计算平台内部存储、处理和传输的数据应提供保证数据完整性的功能。

5.2.1.3.10 安全审计

应根据 4.2.2 的描述，按 GB/T 20271—2006 中 6.2.2.3 的要求，从以下方面设计和实现可信计算平台的安全审计功能：

a) 安全审计功能的设计应与密码支持、身份标识与鉴别、自主访问控制、数据保密性保护、用户数据完整性保护、信任服务等安全功能的设计紧密结合；

b) 支持审计日志；支持安全审计事件产生；支持潜在侵害分析；支持基本审计查阅；提供审计事件选择和受保护的审计踪迹存储；

c) 能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问；

d) 能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏。

5.2.1.3.11 备份与故障恢复

应按 4.2.5 中用户数据备份与恢复、增量信息备份与恢复和局部系统备份与恢复的要求，设计和实现终端计算机系统备份与恢复功能。

5.2.1.3.12 I/O 接口配置

应按 4.2.7 中用户自主配置的要求，设计和实现 I/O 接口配置功能。

5.2.1.4 应用系统

应按 GB/T 20271—2006 中 6.2.3 的要求，从以下方面来设计、实现或选购系统审计保护级终端计算机系统所需要的应用系统：

a) 身份标识与鉴别：根据 GB/T 20271—2006 中 6.2.3.1 的描述，实现用户标识、用户鉴别、用户鉴别失败处理和用户-主体绑定的功能；

b) 自主访问控制：根据 GB/T 20271—2006 中 6.2.3.3 的描述，对应用系统相关资源的访问进行控制，允许合法操作，不允许非法操作；

c) 数据保密性保护：根据 GB/T 20271—2006 中 6.2.3.8 的描述，设计和实现应用系统的用户数据保密性保护功能；

d) 安全审计：应根据 GB/T 20271—2006 中 6.2.2.3 的描述，提供应用系统安全审计功能；

e) 数据完整性保护：根据 GB/T 20271—2006 中 6.2.3.7 的描述，对应用系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能。

5.2.2 **安全保证要求**

5.2.2.1 **SSOTCS 自身安全保护**

a) 可信根安全保护：应按以下要求实现终端计算机系统的可信根：
——存储根和报告根应设置在可信硬件模块内；
——可信硬件模块应通过国家专门机构测评认证；
——应对度量根采取物理保护措施。

b) SSF 物理安全保护：应按以下要求实现终端计算机系统审计保护级 SSF 的物理安全保护：
——应按 GB/T 20271—2006 中 6.2.4.1 的要求，实现终端计算机系统审计验证保护级 SSF 的物理安全保护。

c) SSF 运行安全保护：应按以下要求实现终端计算机系统审计保护级 SSF 的运行安全保护：
——应按 GB/T 20271—2006 中 6.2.4.2 的要求，实现终端计算机系统审计保护级 SSF 的运行安全保护；
——应采取适当的失电保护措施，确保在终端计算机系统退出休眠或待机状态后，能恢复到退出工作状态前的配置，确保信任链系统仍能正常工作。

d) SSF 数据安全保护：宜按 GB/T 20271—2006 中 6.2.4.3 的要求，实现终端计算机系统系统审计保护级 SSF 的数据按保护。

e) 资源利用：宜按 GB/T 20271—2006 中 6.2.4.4 的要求，实现终端计算机系统系统审计保护级的资源利用。

f) SSOTCS 访问控制：宜按 GB/T 20271—2006 中 6.2.4.5 的要求，实现终端计算机系统系统审计保护级的 SSOTCS 访问控制。

5.2.2.2 **SSOTCS 设计和实现**

a) 配置管理：应按 GB/T 20271—2006 中 6.2.5.1 的要求，实现终端计算机系统系统审计保护级的配置管理；

b) 分发和操作：应按 GB/T 20271—2006 中 6.2.5.2 的要求，实现终端计算机系统系统审计保护级的分发和操作；

c) 开发：应按 GB/T 20271—2006 中 6.2.5.3 的要求，实现终端计算机系统系统审计保护级的开发；

d) 指导性文档：应按 GB/T 20271—2006 中 6.2.5.4 的要求，实现终端计算机系统系统审计保护级的指导性文档；

e) 生命周期支持：应按 GB/T 20271—2006 中 6.2.5.5 的要求，实现终端计算机系统系统审计保护级的生命周期支持；

f) 测试：应按 GB/T 20271—2006 中 6.2.5.6 的要求，实现终端计算机系统系统审计保护级的测试。

5.2.2.3 **SSOTCS 管理**

按 GB/T 20271—2006 中 6.2.6 的要求，实现终端计算机系统系统审计保护级的 SSOTCS 安全管理。

5.3 **第三级：安全标记保护级**

5.3.1 **安全功能要求**

5.3.1.1 **物理系统**

5.3.1.1.1 **设备安全可用**

应按 4.1.1 中基本运行支持和基本安全可用的要求，设计和实现终端计算机系统设备安全可用的功能。

5.3.1.1.2 **设备防盗防毁**

应按 4.1.2 中设备标记要求、设备实体安全与防盗的要求，设计和实现终端计算机系统的设备防盗防毁的功能。

标准分享网 www.bzfxw.com 免费下载

5.3.1.2 操作系统

应按 GB/T 20272—2006 中 4.3.1 的要求，从以下方面来设计、实现或选购安全标记保护级终端计算机系统所需要的操作系统：

a) 身份鉴别：根据 GB/T 20272—2006 中 4.3.1.1 的描述，实现操作系统用户标识、用户鉴别、用户鉴别失败处理和用户-主体绑定的功能；

b) 自主访问控制：根据 GB/T 20272—2006 中 4.3.1.2 的描述，对操作系统的访问进行控制，允许合法操作，不允许非法操作；

c) 标记：根据 GB/T 20272—2006 中 4.3.1.3 的描述，设计和实现操作系统标记功能，为主、客体设置所需要的敏感标记；

d) 强制访问控制：根据 GB/T 20272—2006 中 4.3.1.4 的描述，对操作系统的访问进行控制，允许合法操作，不允许非法操作；应对操作系统实现包括系统文件、服务、驱动、注册表及进程在内的强制访问控制功能；

e) 数据流控制：对于以数据流方式实现数据交换的操作系统，根据 GB/T 20272—2006 中 4.3.1.5 的描述，设计和实现操作系统的数据流控制功能；

f) 安全审计：根据 GB/T 20272—2006 中 4.3.1.6 的描述，提供操作系统安全审计功能；

g) 用户数据保密性：根据 GB/T 20272—2006 中 4.3.1.8 的描述，设计和实现操作系统的用户数据保密性保护功能；

h) 用户数据完整性：根据 GB/T 20272—2006 中 4.3.1.7 的描述，对操作系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能。

5.3.1.3 可信计算平台

5.3.1.3.1 密码支持

应以 4.3.1 的描述，并按以下要求，设计与实现安全标记级终端计算机系统密码支持功能：

a) 密码算法：应使用国家密码管理部门批准的密码算法，应采用硬件实现密码算法；

b) 密码操作：密钥生成、数字签名与验证等关键密码操作应基于密码硬件支持；

c) 密钥管理：所有密钥应受存储根保护，存储根本身应由安全硬件保护。

5.3.1.3.2 信任链

应按 4.2.3 的描述及以下要求，设计和实现终端计算机系统的信任链功能：

a) 应基于可信硬件模块实现静态信任链和动态信任链的建立；

b) 静态信任链中操作系统(OS)的完整性度量基准值应由国家专门机构管理，支持离线校验，基准值应存储在受存储根保护的区域中，若度量值与基准值不一致，应停止操作系统启动；

c) 根据 4.2.3 的要求设计和实现信任链模块升级和信任链模块实时修复功能。

5.3.1.3.3 运行时防护

应按 4.2.4 的运行时防护的要求，设计和实现如下功能：

a) 恶意代码防护：根据 4.2.4.1 的描述，实现外来介质使用控制、特征码扫描、基于 CPU 的数据执行保护的功能；

b) 网络攻击防护：根据 4.2.4.2 的描述，实现 IP 过滤、网络协议分析、应用程序监控、内容过滤的防火墙功能。实现实时阻断、文件监控、注册表监控的入侵检测功能；

c) 网络接入控制：应按 4.2.4.3 的要求，实现网络接入控制功能。

5.3.1.3.4 系统安全性检测分析

应按 4.2.1 终端计算机操作系统安全性检测分析、硬件系统安全性检测分析、应用程序安全性检测分析和电磁泄漏发射检测分析的要求，运用有关工具，检测所选用或开发的操作系统、硬件系统、应用程序的安全性和电磁泄漏，并通过对检测结果的分析，按安全标记保护级的要求，对存在的安全问题加以改进。

5.3.1.3.5 **信任服务**

应根据4.3.8的描述及以下要求，设计与实现可信计算平台的安全标记保护级信任服务功能：

a) 应在可信硬件模块中专门设置受保护区域存储所有静态信任链的完整性度量值；

b) 应设置一个可信硬件模块保护的区域来存储所有动态信任链的完整性度量值；

c) 必要时应向国家专门机构报告操作系统完整性度量值。

5.3.1.3.6 **身份标识与鉴别**

5.3.1.3.6.1 **系统身份标识与鉴别**

应按4.3.2的要求，从以下方面实现系统的身份标识与鉴别功能

a) 应按4.3.2.1的要求，设计与实现终端计算机系统的唯一性标识、标识可信性、隐秘性和标识信息管理功能，确保终端计算机系统可信计算平台的身份唯一性和真实性；

b) 应按4.3.2.2的要求，设计与实现系统身份鉴别功能。

5.3.1.3.6.2 **用户身份标识与鉴别**

应按4.3.2的要求，从以下方面设计和实现用户身份标识与鉴别功能：

a) 应按4.3.2.3的要求，设计与实现用户的基本标识、唯一性标识与标识信息管理功能；

b) 应按4.3.2.4的要求，设计与实现用户的基本鉴别和一次性使用鉴别；

c) 应按4.3.2.4的要求，支持以数字证书、指纹、IC卡等形式提供鉴别信息；

d) 应按4.3.2.5的要求，设计与实现用户鉴别失败处理功能；

e) 应按4.3.2.6的要求，设计与实现用户-主体绑定功能。

5.3.1.3.7 **自主访问控制**

可按4.3.3自主访问控制的要求，从以下方面设计和实现可信计算平台的自主访问控制功能：

a) 按4.3.3.1的要求，确定自主访问控制策略；

b) 按4.3.3.2的要求，设计和实现自主访问控制功能；

c) 按4.3.3.3中子集访问控制的要求，确定自主访问控制的范围；

d) 按4.3.3.4中访问控制粒度的要求，确定自主访问控制的粒度。

5.3.1.3.8 **标记**

应按4.3.4标记的要求，从以下方面设计和实现可信计算平台的标记功能：

a) 按4.3.4.1的要求，设计和实现主体标记功能；

b) 按4.3.4.2的要求，设计和实现客体标记功能。

5.3.1.3.9 **强制访问控制**

应按4.3.5强制访问控制的要求，从以下方面设计和实现可信计算平台的强制访问控制功能：

a) 按4.3.5.1的要求，确定强制访问控制策略；

b) 按4.3.5.2的要求，设计和实现强制访问控制功能；

c) 按4.3.5.3中子集访问控制的要求，确定强制访问控制的范围；

d) 按4.3.5.4中访问控制粒度的要求，确定强制访问控制的粒度。

5.3.1.3.10 **数据保密性保护**

应按4.3.6的要求，从以下方面设计和实现可信计算平台的数据保密性保护功能：

a) 应按4.3.6.1中数据加密、数据绑定和数据密封的要求，按4.3.1所配置的密码支持，对需要进行存储保密性保护的数据，采用存储加密的措施，设计和实现数据存储保密性保护功能；

b) 应按4.3.6.2的要求，按4.3.1所配置的密码支持，对需要进行传输保密性保护的数据，采用传输加密的措施，设计和实现数据传输保密性保护功能；

c) 应按4.3.6.3子集信息保护的要求，设计和实现客体安全重用功能。

5.3.1.3.11 **数据完整性保护**

根据4.3.7的描述，对可信计算平台内部存储、处理和传输的数据应提供保证数据完整性的功能。

标准分享网 www.bzfxw.com 免费下载

5.3.1.3.12 **安全审计**

应根据4.2.2的描述，按GB/T 20271—2006中6.3.2.4的要求，从以下方面设计和实现可信计算平台的安全审计功能：

a) 安全审计功能的设计应与密码支持、身份标识与鉴别、自主访问控制、数据保密性保护、用户数据完整性保护、信任服务、标记、强制访问控制等安全功能的设计紧密结合；

b) 支持审计日志、实时报警生成和违例进程终止；支持安全审计事件产生；支持潜在侵害分析和基于异常检测；支持基本审计查阅和受控审计查阅；提供审计事件选择、受保护的审计踪迹存储和审计数据的可用性确保；

c) 能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问；

d) 能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏；

e) 内置可信硬件模块的终端计算机系统，可信硬件模块应该能审计内部命令运行情况、维护事件、用户密钥的创建、使用与删除事件或其他专门的可审计事件，提供给上层应用软件查询审计情况的接口，并存储审计记录。

5.3.1.3.13 **备份与故障修复**

应按4.2.5中用户数据备份与恢复、增量信息备份与恢复、局部系统备份与恢复、全系统备份与恢复、备份保护措施，设计和实现终端计算机系统的备份与恢复功能。

5.3.1.3.14 **I/O接口配置**

应按4.2.7中用户自主配置的要求，设计和实现I/O接口配置功能。

5.3.1.3.15 **可信时间戳**

根据4.2.6中可信时间戳的要求，设计和实现终端计算机系统的可信时间戳功能。

5.3.1.4 **应用系统**

应按GB/T 20271—2006中6.3.3的要求，从以下方面来设计、实现或选购安全标记保护级终端计算机系统所需要的应用系统：

a) 身份标识与鉴别：根据GB/T 20271—2006中6.3.3.1的描述，实现用户标识、用户鉴别、用户鉴别失败处理和用户-主体绑定的功能；

b) 自主访问控制：根据GB/T 20271—2006中6.3.3.3的描述，对应用系统相关资源的访问进行控制，允许合法操作，不允许非法操作；

c) 标记：根据GB/T 20271—2006中6.3.3.4的描述，设计和实现应用系统标记功能，为应用系统中的主、客体设置所需要的敏感标记；

d) 强制访问控制：根据GB/T 20271—2006中6.3.3.5的描述，对应用系统相关资源的访问进行控制，允许合法操作，不允许非法操作；

e) 安全审计：应根据GB/T 20271—2006中6.3.2.4的描述，提供应用系统安全审计功能；

f) 数据保密性保护：根据GB/T 20271—2006中6.3.3.8的描述，设计和实现应用系统的用户数据保密性保护功能；

g) 数据完整性保护：根据GB/T 20271—2006中6.3.3.7的描述，对应用系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能。

5.3.2 **安全保证要求**

5.3.2.1 **SSOTCS自身安全保护**

a) 可信根安全保护：应按以下要求实现终端计算机系统的可信根：

——存储根和报告根应设置在可信硬件模块内；

——可信硬件模块应通过国家专门机构测评认证；

——应对度量根采取物理保护措施。

b) SSF 物理安全保护：应按以下要求实现终端计算机系统安全标记保护级 SSF 的物理安全保护：

——应按 GB/T 20271—2006 中 6.3.4.1 的要求，实现终端计算机系统安全标记保护级 SSF 的物理安全保护；

——应采取适当硬件保护措施防止对可信硬件模块中密码运算模块的能量攻击。

c) SSF 运行安全保护：应按以下要求实现终端计算机系统安全标记保护级 SSF 的运行安全保护：

——应按 GB/T 20271—2006 中 6.3.4.2 的要求，实现终端计算机系统安全标记保护级 SSF 的运行安全保护；

——应采取适当的失电保护措施，确保在终端计算机系统退出休眠或待机状态后，能恢复到退出工作状态前的配置，确保信任链系统仍能正常工作。

d) SSF 数据安全保护：应按 GB/T 20271—2006 中 6.3.4.3 的要求，实现终端计算机系统安全标记保护级 SSF 的数据按保护。

e) 资源利用：应按 GB/T 20271—2006 中 6.3.4.4 的要求，实现终端计算机系统安全标记保护级的资源利用。

f) SSOTCS 访问控制：应按 GB/T 20271—2006 中 6.3.4.5 的要求，实现终端计算机系统安全标记保护级的 SSOTCS 访问控制。

5.3.2.2 SSOTCS 设计和实现

a) 配置管理：应按 GB/T 20271—2006 中 6.3.5.1 的要求，实现终端计算机系统安全标记保护级的配置管理；

b) 分发和操作：应按 GB/T 20271—2006 中 6.3.5.2 的要求，实现终端计算机系统安全标记保护级的分发和操作；

c) 开发：应按 GB/T 20271—2006 中 6.3.5.3 的要求，实现终端计算机系统安全标记保护级的开发；

d) 指导性文档：应按 GB/T 20271—2006 中 6.3.5.4 的要求，实现终端计算机系统安全标记保护级的指导性文档；

e) 生命周期支持：应按 GB/T 20271—2006 中 6.3.5.5 的要求，实现终端计算机系统安全标记保护级的生命周期支持；

f) 测试：应按 GB/T 20271—2006 中 6.3.5.6 的要求，实现终端计算机系统安全标记保护级的测试；

g) 脆弱性评定：应按 GB/T 20271—2006 中 6.3.5.7 的要求，实现安全标记保护级的脆弱性评定。

5.3.2.3 SSOTCS 管理

应按 GB/T 20271—2006 中 6.3.6 的要求，实现终端计算机系统安全标记保护级的 SSOTCS 安全管理。

5.4 第四级：结构化保护级

5.4.1 安全功能要求

5.4.1.1 物理系统

5.4.1.1.1 设备安全可用

应按 4.1.1 中基本运行支持和基本安全可用的要求，设计和实现终端计算机系统设备安全可用功能。

标准分享网 www.bzfxw.com 免费下载

5.4.1.1.2 设备防盗防毁

应按 4.1.2 中设备标记要求和设备实体安全的要求，设计和实现终端计算机系统的设备防盗防毁的功能。

5.4.1.2 操作系统

应按 GB/T 20272—2006 中 4.4.1 的要求，从以下方面来设计、实现或选购满足结构化保护级终端计算机系统保密性功能要求的操作系统：

a) 身份鉴别：根据 GB/T 20272—2006 中 4.4.1.1 的描述，实现操作系统用户标识、用户鉴别、用户鉴别失败处理和用户-主体绑定的功能；

b) 自主访问控制：根据 GB/T 20272—2006 中 4.4.1.2 的描述，对操作系统的访问进行控制，允许合法操作，不允许非法操作；

c) 标记：根据 GB/T 20272—2006 中 4.4.1.3 的描述，设计和实现操作系统标记功能，为主、客体设置所需要的敏感标记；

d) 强制访问控制：根据 GB/T 20272—2006 中 4.4.1.4 的描述，对操作系统的访问进行控制，允许合法操作，不允许非法操作；应对操作系统实现包括系统文件、服务、驱动、注册表及进程在内的强制访问控制功能；

e) 数据流控制：对于以数据流方式实现数据交换的操作系统，根据 GB/T 20272—2006 中 4.4.1.5 的描述，设计和实现操作系统的数据流控制功能；

f) 安全设计：应根据 GB/T 20272—2006 中 4.4.1.6 的描述，设计和实现操作系统安全审计功能；

g) 用户数据保密性：根据 GB/T 20272—2006 中 4.4.1.8 的描述，设计和实现操作系统的用户数据保密性保护功能；

h) 用户数据完整性：根据 GB/T 20272—2006 中 4.4.1.7 的描述，对操作系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能；

i) 可信路径：根据 GB/T 20272—2006 中 4.4.1.9 的描述，在用户进行初始登录和/或鉴别时，应建立一条安全的数据传输通路。

5.4.1.3 可信计算平台

5.4.1.3.1 密码支持

应以 4.3.1 的描述，并按以下要求，设计与实现访问验证保护级终端计算机系统密码支持功能：

a) 密码算法：应使用国家密码管理部门批准的密码算法，应采用硬件实现对称密码算法、公钥密码算法、杂凑算法和随机数生成器算法；

b) 密码操作：所有密码操作均应基于可信硬件模块或其他密码硬件模块支持；

c) 密钥管理：所有密钥应受存储根保护，存储根本身应由安全硬件保护。

5.4.1.3.2 信任链

应按 4.2.3 的描述及以下要求，设计和实现终端计算机系统的信任链功能：

a) 应基于可信硬件模块实现静态信任链和动态信任链的建立；

b) 静态信任链中操作系统(OS)的完整性度量基准值应由国家专门机构管理，支持在线或离线校验，若度量值与基准值不一致，应停止操作系统启动；

c) 动态信任链中关键应用程序的完整性度量基准值应由国家专门机构管理，支持离线校验，基准值应存储在受存储根保护的区域中，若度量值与基准值不一致，应立即停止应用程序运行；

d) 根据 4.2.3 的要求设计和实现信任链模块实时修复和信任链模块升级功能。

5.4.1.3.3 运行时防护

应按 4.2.4 的运行时防护的要求，设计和实现如下功能：

a) 恶意代码防护：根据 4.2.4.1 的描述，实现外来介质使用控制、特征码扫描、基于 CPU 的数据执行保护、进程隔离、进程行为分析的功能；

b) 网络攻击防护：根据4.2.4.2的描述，实现IP过滤、网络协议分析、应用程序监控、内容过滤的防火墙功能。实现实时阻断、文件监控、注册表监控、事件监测、实时流量分析的入侵检测功能；

c) 网络接入控制：应按4.2.4.3的要求，实现网络接入控制功能。

5.4.1.3.4 系统安全性检测分析

应按4.2.1终端计算机操作系统安全性检测分析、硬件系统安全性检测分析、应用程序安全性检测分析和电磁泄漏发射检测分析的要求，运用有关工具，检测所选用或开发的操作系统、硬件系统、应用程序的安全性和电磁泄漏，并通过对检测结果的分析，按结构化保护级的要求，对存在的安全问题加以改进。

5.4.1.3.5 信任服务

应根据4.3.8的描述及以下要求，设计与实现可信计算平台的结构化保护级信任服务功能：

a) 应在可信硬件模块中专门设置受保护区域存储所有静态信任链的完整性度量值；

b) 应设置一个可信硬件模块保护的区域来存储所有动态信任链的完整性度量值；

c) 必要时应向国家专门机构报告操作系统和关键应用程序完整性度量值。

5.4.1.3.6 身份标识与鉴别

5.4.1.3.6.1 系统身份标识与鉴别

应按4.3.2的要求，从以下方面实现系统的身份标识与鉴别功能：

a) 应按4.3.2.1的要求，设计与实现终端计算机系统的唯一性标识、标识可信性、隐秘性和标识信息管理功能，确保终端计算机系统可信计算平台的身份唯一性和真实性；

b) 系统身份标识应由国家权威管理机构进行管理；

c) 应按4.3.2.2的要求，设计与实现系统身份鉴别功能。

5.4.1.3.6.2 用户身份标识与鉴别

应按4.3.2的要求，从以下方面设计和实现用户身份标识与鉴别功能：

a) 应按4.3.2.3的要求，设计与实现用户的基本标识、唯一性标识与标识信息管理功能；

b) 应按4.3.2.4的要求，设计与实现用户的基本鉴别、一次性使用鉴别、多机制鉴别功能；

c) 应按4.3.2.4的要求，支持以数字证书、IC卡、指纹、虹膜等形式提供鉴别信息；

d) 应按4.3.2.5的要求，设计与实现用户鉴别失败处理功能；

e) 应按4.3.2.6的要求，设计与实现用户-主体绑定功能；

f) 应按4.3.2.4的要求，对IC卡、指纹、虹膜等形式的鉴别信息，应建立鉴别设备与可信硬件模块的通信通道，确保可信硬件模块获得不被窜改和泄漏的原始身份鉴定信息；

g) 应按4.3.2.7的要求，设计与实现匿名和不可关联性的隐秘功能。

5.4.1.3.7 自主访问控制

可按4.3.3自主访问控制的要求，从以下方面设计和实现可信计算平台的自主访问控制功能：

a) 按4.3.3.1的要求，确定自主访问控制策略；

b) 按4.3.3.2的要求，设计和实现自主访问控制功能；

c) 按4.3.3.3中完全访问控制的要求，确定自主访问控制的范围；

d) 按4.3.3.4中访问控制粒度的要求，确定自主访问控制的粒度。

5.4.1.3.8 标记

应按4.3.4标记的要求，从以下方面设计和实现可信计算平台的标记功能：

a) 按4.3.4.1的要求，设计和实现主体标记功能；

b) 按4.3.4.2的要求，设计和实现客体标记功能。

5.4.1.3.9 强制访问控制

应按4.3.5强制访问控制的要求，从以下方面设计和实现可信计算平台的强制访问控制功能：

标准分享网 www.bzfxw.com 免费下载

a) 按 4.3.5.1 的要求，确定强制访问控制策略；

b) 按 4.3.5.2 的要求，设计和实现强制访问控制功能；

c) 按 4.3.5.3 中完全访问控制的要求，确定强制访问控制的范围；

d) 按 4.3.5.4 中访问控制粒度的要求，确定强制访问控制的粒度。

5.4.1.3.10 数据保密性保护

应按 4.3.6 的要求，从以下方面设计和实现可信计算平台的数据保密性保护功能：

a) 应按 4.3.6.1 中数据加密、数据绑定和数据密封的要求，按 4.3.1 所配置的密码支持，对需要进行存储保密性保护的数据，采用存储加密的措施，设计和实现数据存储保密性保护功能；

b) 应按 4.3.6.2 的要求，按 4.3.1 所配置的密码支持，对需要进行传输保密性保护的数据，采用传输加密的措施，设计和实现数据传输保密性保护功能；

c) 应按 4.3.6.3 完全信息保护的要求，设计和实现客体安全重用功能。

5.4.1.3.11 数据完整性保护

根据 4.3.7 的描述，对可信计算平台内部存储、处理和传输的数据应提供保证数据完整性的功能。

5.4.1.3.12 安全审计

应根据 4.2.2 的描述，按 GB/T 20271—2006 中 6.4.2.4 的要求，从以下方面设计和实现应用系统的安全审计功能：

a) 安全审计功能的设计应与密码支持、身份标识与鉴别、自主访问控制、数据保密性保护、用户数据完整性保护、信任服务、标记、强制访问控制、可信路径等安全功能的设计紧密结合；

b) 支持审计日志、实时报警生成和违例进程终止；支持安全审计事件产生；支持潜在侵害分析、基于异常检测和简单攻击探测；支持基本审计查阅和受控审计查阅；提供审计事件选择、受保护的审计踪迹存储、审计数据的可用性确保、审计数据可能丢失情况下的安全措施；

c) 能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问；

d) 能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏；

e) 内置可信硬件模块的终端计算机系统，可信硬件模块应该能审计内部命令运行情况、维护事件、用户密钥的创建、使用与删除事件或其他专门的可审计事件，提供给上层应用软件查询审计情况的接口，并存储审计记录。

5.4.1.3.13 备份与故障恢复

应按 4.2.5 中用户数据备份与恢复、增量信息备份与恢复、局部系统备份与恢复、全系统备份与恢复、备份保护措施的要求，设计和实现终端计算机系统的备份与恢复功能。

5.4.1.3.14 I/O 接口配置

应按 4.2.7 中用户自主配置、集中管理配置的要求，设计和实现 I/O 接口配置功能。

5.4.1.3.15 可信路径

根据 4.3.9 的描述，按 GB/T 20271—2006 中 6.4.3.9 的要求，在用户进行初始登录和/或鉴别时，应建立一条安全的数据传输通路。

5.4.1.3.16 可信时间戳

根据 4.2.6 中可信时间戳的要求，设计和实现终端计算机系统的可信时间戳功能。

5.4.1.4 应用系统

应按 GB/T 20271—2006 中 6.4.3 的要求，从以下方面设计、实现或选购满足结构化保护级终端计算机系统保密性功能要求的应用系统：

a) 身份标识与鉴别：根据 GB/T 20271—2006 中 6.4.3.1 的描述，实现用户标识、用户鉴别、用户鉴别失败处理和用户-主体绑定的功能；

b) 自主访问控制：根据 GB/T 20271—2006 中 6.4.3.3 的描述，对应用系统相关资源的访问进行控制，允许合法操作，不允许非法操作；

c) 标记：根据 GB/T 20271—2006 中 6.4.3.4 的描述，设计和实现应用系统标记功能，为应用系统中的主、客体设置所需要的敏感标记；

d) 强制访问控制：根据 GB/T 20271—2006 中 6.4.3.5 的描述，对应用系统相关资源的访问进行控制，允许合法操作，不允许非法操作；

e) 安全审计：应根据 GB/T 20271—2006 中 6.4.2.4 的描述，设计和实现应用系统安全审计功能；

f) 数据保密性保护：根据 GB/T 20271—2006 中 6.4.3.8 的描述，设计和实现应用系统的用户数据保密性保护功能；

g) 数据完整性保护：根据 GB/T 20271—2006 中 6.4.3.7 的描述，对应用系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能；

h) 可信路径：根据 GB/T 20271—2006 中 6.4.3.9 的描述，设计和实现应用系统的可信路径功能。

5.4.2 安全保证要求

5.4.2.1 SSOTCS 自身安全保护

a) 可信根安全保护：应按以下要求实现终端计算机系统的可信根：

——存储根和报告根应设置在可信硬件模块内；

——可信硬件模块应由国家专门机构研制；

——应对度量根采取物理保护措施。

b) 键盘输入保护：应按以下要求实现键盘的输入保护：

——应有物理路径支持键盘输入与可信硬件模块的直接通信；

——应有物理开关控制是否启用键盘输入与可信硬件模块的通信路径。

c) SSF 物理安全保护：应按以下要求实现终端计算机系统结构化保护级 SSF 的物理安全保护：

——应按 GB/T 20271—2006 中 6.4.4.1 的要求，实现终端计算机系统结构化保护级 SSF 的物理安全保护；

——应采取适当硬件保护措施防止对可信硬件模块中密码运算模块的能量攻击。

d) SSF 运行安全保护：应按以下要求实现终端计算机系统结构化保护级 SSF 的运行安全保护：

——应按 GB/T 20271—2006 中 6.4.4.2 的要求，实现终端计算机系统结构化保护级 SSF 的运行安全保护；

——应采取适当的失电保护措施，确保在终端计算机系统退出休眠或待机状态后，能恢复到退出工作状态前的配置，确保信任链系统仍能正常工作。

e) SSF 数据安全保护：应按 GB/T 20271—2006 中 6.4.4.3 的要求，实现终端计算机系统结构化保护级 SSF 的数据按保护。

f) 资源利用：应按 GB/T 20271—2006 中 6.4.4.4 的要求，实现终端计算机系统结构化保护级的资源利用。

g) SSOTCS 访问控制：应按 GB/T 20271—2006 中 6.4.4.5 的要求，实现终端计算机系统结构化保护级的 SSOTCS 访问控制。

5.4.2.2 SSOTCS 设计和实现

a) 配置管理：应按 GB/T 20271—2006 中 6.4.5.1 的要求，实现终端计算机系统结构化保护级的配置管理；

b) 分发和操作：应按 GB/T 20271—2006 中 6.4.5.2 的要求，实现终端计算机系统结构化保护级的分发和操作；

标准分享网 www.bzfxw.com 免费下载

c) 开发：应按 GB/T 20271—2006 中 6.4.5.3 的要求，实现终端计算机系统结构化保护级的开发；

d) 指导性文档：应按 GB/T 20271—2006 中 6.4.5.4 的要求，实现终端计算机系统结构化保护级的指导性文档；

e) 生命周期支持：应按 GB/T 20271—2006 中 6.4.5.5 的要求，实现终端计算机系统结构化保护级的生命周期支持；

f) 测试：应按 GB/T 20271—2006 中 6.4.5.6 的要求，实现终端计算机系统结构化保护级的测试；

g) 脆弱性评定：应按 GB/T 20271—2006 中 6.4.5.7 的要求，实现网络结构化保护级的脆弱性评定。

5.4.2.3 SSOTCS 管理

应按 GB/T 20271—2006 中 6.4.6 的要求，实现终端计算机系统结构化保护级的 SSOTCS 安全管理。

5.5 第五级：访问验证保护级

5.5.1 安全功能要求

5.5.1.1 物理系统

5.5.1.1.1 设备安全可用

应按 4.1.1 中基本运行支持、基本安全可用和不间断运行支持的要求，设计和实现终端计算机系统设备安全可用的功能。

5.5.1.1.2 设备防盗防毁

应按 4.1.2 中设备标记要求、设备实体安全、防盗和自销毁的要求，设计和实现终端计算机系统的设备防盗防毁的功能。

5.5.1.1.3 设备高可靠

应按 4.1.3 中的要求设计和实现设备高可靠功能。

5.5.1.2 操作系统

应按 GB/T 20272—2006 中 4.5.1 的要求，从以下方面来设计、实现或选购满足访问验证保护级终端计算机系统保密性功能要求的操作系统：

a) 身份鉴别：根据 GB/T 20272—2006 中 4.5.1.1 的描述，实现操作系统用户标识、用户鉴别、用户鉴别失败处理和用户-主体绑定的功能；

b) 自主访问控制：根据 GB/T 20272—2006 中 4.5.1.2 的描述，对操作系统的访问进行控制，允许合法操作，不允许非法操作；

c) 标记：根据 GB/T 20272—2006 中 4.5.1.3 的描述，设计和实现操作系统标记功能，为主、客体设置所需要的敏感标记；

d) 强制访问控制：根据 GB/T 20272—2006 中 4.5.1.4 的描述，对操作系统的访问进行控制，允许合法操作，不允许非法操作；应对操作系统实现包括系统文件、服务、驱动、注册表及进程在内的强制访问控制功能；

e) 数据流控制：对于以数据流方式实现数据交换的操作系统，应根据 GB/T 20272—2006 中 4.5.1.5 的描述，设计和实现操作系统的数据流控制功能；

f) 安全审计：应根据 GB/T 20272—2006 中 4.5.1.6 的描述，设计和实现操作系统安全审计功能；

g) 用户数据保密性：根据 GB/T 20272—2006 中 4.5.1.8 的描述，设计和实现操作系统的用户数据保密性保护功能；

h) 用户数据完整性：根据 GB/T 20272—2006 中 4.5.1.7 的描述，对操作系统内部存储、处理和

传输的用户数据应提供保证用户数据完整性的功能；

i) 可信路径：根据 GB/T 20272—2006 中 4.5.1.9 的描述，在用户进行初始登录和/或鉴别时，应建立一条安全的数据传输通路。

5.5.1.3 可信计算平台

5.5.1.3.1 密码支持

应以 4.3.1 的描述，并按以下要求，设计与实现访问验证保护级终端计算机系统密码支持功能：

a) 密码算法：应使用国家密码管理部门指定的密码算法，应采用硬件实现对称密码算法、公钥密码算法、杂凑算法和随机数生成器算法；

b) 密码操作：所有密码操作均应基于可信硬件模块或其他密码硬件模块支持；

c) 密钥管理：所有密钥应受存储根保护，存储根本身应由安全硬件保护。

5.5.1.3.2 信任链

应按 4.2.3 的描述及以下要求，设计和实现终端计算机系统的信任链功能：

a) 应基于可信硬件模块实现静态信任链和动态信任链的建立；

b) 静态信任链中操作系统(OS)的完整性度量基准值应由国家专门机构管理，支持在线或离线校验，若度量值与基准值不一致，应停止操作系统启动；

c) 动态信任链中所有应用程序的完整性度量基准值应由国家专门机构管理，支持在线或离线校验，若度量值与基准值不一致，应立即停止应用程序运行；

d) 根据 4.2.3 的要求设计和实现信任链模块实时修复和信任链模块升级功能。

5.5.1.3.3 运行时防护

应按 4.2.4 的运行时防护的要求，设计和实现如下功能：

a) 恶意代码防护：根据 4.2.4.1 的描述，实现外来介质使用控制、特征码扫描、基于 CPU 的数据执行保护、进程隔离、进程行为分析的功能；

b) 网络攻击防护：根据 4.2.4.2 的描述，实现 IP 过滤、网络协议分析、应用程序监控、内容过滤的防火墙功能。实现实时阻断、文件监控、注册表监控、事件监测、实时流量分析的入侵检测功能；

c) 网络接入控制：应按 4.2.4.3 的要求，实现网络接入控制功能。

5.5.1.3.4 系统安全性检测分析

应按 4.2.1 终端计算机操作系统安全性检测分析、硬件系统安全性检测分析、应用程序安全性检测分析和电磁泄漏发射检测分析的要求，运用有关工具，检测所选用或开发的操作系统、硬件系统、应用程序的安全性和电磁泄漏，并通过对检测结果的分析，按访问验证保护级的要求，对存在的安全问题加以改进。

5.5.1.3.5 信任服务

应根据 4.3.8 的描述及以下要求，设计与实现可信计算平台的访问验证级信任服务功能：

a) 应在可信硬件模块中专门设置受保护区域存储所有静态信任链的完整性度量值；

b) 应设置一个可信硬件模块保护的区域来存储所有动态信任链的完整性度量值。

必要时应向国家专门机构报告操作系统和应用程序完整性度量值。

5.5.1.3.6 身份标识与鉴别

5.5.1.3.6.1 系统身份标识与鉴别

应按 4.3.2 的要求，从以下方面实现可信计算平台的身份标识与鉴别功能：

a) 应按 4.3.2.1 的要求，设计与实现终端计算机系统的唯一性标识、标识可信性、隐秘性和标识信息管理功能，确保终端计算机系统可信计算平台的身份唯一性和真实性；

b) 系统身份标识应由国家权威管理机构进行管理；

c) 应按 4.3.2.2 的要求，设计与实现系统身份鉴别功能。

标准分享网 www.bzfxw.com 免费下载

5.5.1.3.6.2 用户身份标识与鉴别

应按 4.3.2 的要求，从以下方面设计和实现用户身份标识与鉴别功能：

a) 应按 4.3.2.3 的要求，设计与实现用户的基本标识、唯一性标识与标识信息管理功能；

b) 应按 4.3.2.4 的要求，设计与实现用户的基本鉴别、不可伪造鉴别、一次性使用鉴别、多机制鉴别和重新鉴别功能；

c) 应按 4.3.2.4 的要求，支持以数字证书、IC 卡、指纹、虹膜等形式提供鉴别信息；

d) 应按 4.3.2.5 的要求，设计与实现用户鉴别失败处理功能；

e) 应按 4.3.2.6 的要求，设计与实现用户-主体绑定功能；

f) 应按 4.3.2.4 的要求，对 IC 卡、指纹、虹膜等形式的鉴别信息，应建立鉴别设备与可信硬件模块的通信通道，确保可信硬件模块获得不被窜改和泄漏的原始身份鉴定信息；

g) 应按 4.3.2.7 的要求，设计与实现匿名、假名、不可关联性和不可观察性的隐秘功能。

5.5.1.3.7 自主访问控制

可按 4.3.3 自主访问控制的要求，从以下方面设计和实现可信计算平台的自主访问控制功能：

a) 按 4.3.3.1 的要求，确定自主访问控制策略；

b) 按 4.3.3.2 的要求，设计和实现自主访问控制功能；

c) 按 4.3.3.3 中完全访问控制的要求，确定自主访问控制的范围；

d) 按 4.3.3.4 中访问控制粒度的要求，确定自主访问控制的粒度。

5.5.1.3.8 标记

应按 4.3.4 标记的要求，从以下方面设计和实现可信计算平台的标记功能：

a) 按 4.3.4.1 的要求，设计和实现主体标记功能；

b) 按 4.3.4.2 的要求，设计和实现客体标记功能。

5.5.1.3.9 强制访问控制

应按 4.3.5 强制访问控制的要求，从以下方面设计和实现可信计算平台的强制访问控制功能：

a) 按 4.3.5.1 的要求，确定强制访问控制策略；

b) 按 4.3.5.2 的要求，设计和实现强制访问控制功能；

c) 按 4.3.5.3 中完全访问控制的要求，确定强制访问控制的范围；

d) 按 4.3.5.4 中访问控制粒度的要求，确定强制访问控制的粒度。

5.5.1.3.10 数据保密性保护

应按 4.3.6 的要求，从以下方面设计和实现可信计算平台的数据保密性保护功能：

a) 应按 4.3.6.1 中数据加密、数据绑定和数据密封的要求，按 4.3.1 所配置的密码支持，对需要进行存储保密性保护的数据，采用存储加密的措施，设计和实现数据存储保密性保护功能；

b) 应按 4.3.6.2 的要求，按 4.3.1 所配置的密码支持，对需要进行传输保密性保护的数据，采用传输加密的措施，设计和实现数据传输保密性保护功能；

c) 应按 4.3.6.3 特殊信息保护的要求，设计和实现客体安全重用功能。

5.5.1.3.11 数据完整性保护

根据 4.3.7 的描述，对可信计算平台内部存储、处理和传输的数据应提供保证数据完整性的功能。

5.5.1.3.12 安全审计

应根据 4.2.2 的描述，按 GB/T 20271—2006 中 6.5.2.4 的要求，从以下方面设计和实现可信计算平台的安全审计功能：

a) 安全审计功能的设计应与密码支持、身份标识与鉴别、自主访问控制、数据保密性保护、用户数据完整性保护、信任服务、标记、强制访问控制、可信路径等安全功能的设计紧密结合；

b) 支持审计日志、实时报警生成、违例进程终止和用户账号断开与失效；支持安全审计事件产生，潜在侵害分析、基于异常检测、简单攻击探测和复杂攻击探测；支持基本审计查阅和受控审

计查阅；支持审计事件选择；提供受保护的审计踪迹存储、审计数据的可用性确保、审计数据可能丢失情况下措施和防止审计数据丢失的措施；

c) 能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问；

d) 能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏；

e) 内置可信硬件模块的终端计算机系统，可信硬件模块应该能审计内部命令运行情况、维护事件、用户密钥的创建、使用与删除事件或其他专门的可审计事件，提供给上层应用软件查询审计情况的接口，并存储审计记录。

5.5.1.3.13 备份与故障修复

应按 4.2.5 中用户数据备份与恢复、增量信息备份与恢复、局部系统备份与恢复、全系统备份与恢复、备份保护措施的要求，设计和实现终端计算机系统的备份与恢复功能。

5.5.1.3.14 I/O 接口配置

应按 4.2.7 中用户自主配置、集中管理配置和自适应配置的要求，设计和实现 I/O 接口配置功能。

5.5.1.3.15 可信路径

根据 4.3.9 的描述，按 GB/T 20271—2006 中 6.5.3.9 的要求，在用户进行初始登录和/或鉴别时，应建立一条安全的数据传输通路。

5.5.1.3.16 可信时间戳

根据 4.2.6 中可信时间戳的要求，设计和实现终端计算机系统的可信时间戳功能。

5.5.1.4 应用系统

应按 GB/T 20271—2006 中 6.5.3 的要求，从以下方面设计、实现或选购满足访问验证保护级终端计算机系统保密性功能要求的应用系统：

a) 身份标识与鉴别：根据 GB/T 20271—2006 中 6.5.3.1 的描述，实现用户标识、用户鉴别、用户鉴别失败处理和用户-主体绑定的功能；

b) 自主访问控制：根据 GB/T 20271—2006 中 6.5.3.3 的描述，对应用系统相关资源的访问进行控制，允许合法操作，不允许非法操作；

c) 标记：根据 GB/T 20271—2006 中 6.5.3.4 的描述，设计和实现应用系统标记功能，为应用系统中的主、客体设置所需要的敏感标记；

d) 强制访问控制：根据 GB/T 20271—2006 中 6.5.3.5 的描述，对应用系统相关资源的访问进行控制，允许合法操作，不允许非法操作；

e) 数据保密性保护：根据 GB/T 20271—2006 中 6.5.3.8 的描述，设计和实现应用系统的用户数据保密性保护功能；

f) 安全审计：应根据 GB/T 20271—2006 中 6.5.2.4 的描述，设计和实现应用系统安全审计功能；

g) 可信路径：根据 GB/T 20271—2006 中 6.5.3.9 的描述，设计和实现应用系统的可信路径功能；

h) 数据完整性保护：根据 GB/T 20271—2006 中 6.5.3.7 的描述，对应用系统内部存储、处理和传输的用户数据应提供保证用户数据完整性的功能。

5.5.2 安全保证要求

5.5.2.1 SSOTCS 自身安全保护

a) 可信根安全保护：应按以下要求实现终端计算机系统的可信根：

——存储根和报告根应设置在可信硬件模块内；

——可信硬件模块应由国家专门机构研制；

标准分享网 www.bzfxw.com 免费下载

——应对度量根采取物理保护措施。

b) 键盘输入保护：应按以下要求实现键盘的输入保护：

——应有物理路径支持键盘输入与可信硬件模块的直接通信；

——应有物理开关控制是否启用键盘输入与可信硬件模块的通信路径。

c) SSF 物理安全保护：应按以下要求实现终端计算机系统访问验证保护级 SSF 的物理安全保护：

——应按 GB/T 20271—2006 中 6.5.4.1 的要求，实现终端计算机系统访问验证保护级 SSF 的物理安全保护；

——应采取适当硬件保护措施防止对可信硬件模块中密码运算模块的能量攻击。

d) SSF 运行安全保护：应按以下要求实现终端计算机系统访问验证保护级 SSF 的运行安全保护：

——应按 GB/T 20271—2006 中 6.5.4.2 的要求，实现终端计算机系统访问验证保护级 SSF 的运行安全保护；

——应采取适当的失电保护措施，确保在终端计算机系统退出休眠或待机状态后，能恢复到退出工作状态前的配置，确保信任链系统仍能正常工作。

e) SSF 数据安全保护：应按 GB/T 20271—2006 中 6.5.4.3 的要求，实现终端计算机系统访问验证保护级 SSF 的数据按保护。

f) 资源利用：应按 GB/T 20271—2006 中 6.5.4.4 的要求，实现终端计算机系统访问验证保护级的资源利用。

g) SSOTCS 访问控制：应按 GB/T 20271—2006 中 6.5.4.5 的要求，实现终端计算机系统访问验证保护级的 SSOTCS 访问控制。

5.5.2.2 SSOTCS 设计和实现

a) 配置管理：应按 GB/T 20271—2006 中 6.5.5.1 的要求，实现终端计算机系统访问验证保护级的配置管理；

b) 分发和操作：应按 GB/T 20271—2006 中 6.5.5.2 的要求，实现终端计算机系统访问验证保护级的分发和操作；

c) 开发：应按 GB/T 20271—2006 中 6.5.5.3 的要求，实现终端计算机系统访问验证保护级的开发；

d) 指导性文档：应按 GB/T 20271—2006 中 6.5.5.4 的要求，实现终端计算机系统访问验证保护级的指导性文档；

e) 生命周期支持：应按 GB/T 20271—2006 中 6.5.5.5 的要求，实现终端计算机系统访问验证保护级的生命周期支持；

f) 测试：应按 GB/T 20271—2006 中 6.5.5.6 的要求，实现终端计算机系统访问验证保护级的测试；

g) 脆弱性评定：应按 GB/T 20271—2006 中 6.5.5.7 的要求，实现网络访问验证保护级的脆弱性评定。

5.5.2.3 SSOTCS 管理

应按 GB/T 20271—2006 中 6.5.6 的要求，实现终端计算机系统访问验证保护级的 SSOTCS 安全管理。

参 考 文 献

[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

[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

[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

[4] GB/T 17901.1—1999 信息技术 安全技术 密钥管理 第1部分:框架

[5] Trusted Computing Group TPM Main Specification Version 1.2:Part 1 Design Principles, May 2004

标准分享网 www.bzfxw.com 免费下载

中华人民共和国公共安全
行业标准
信息安全技术
终端计算机系统安全等级技术要求
GA/T 671—2006
*
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 2.25 字数 60 千字
2007年3月第一版 2007年3月第一次印刷
*
书号:155066·2-17470

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68533533

GA/T 671-2006