ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29240—2012

信息安全技术　终端计算机通用安全技术要求与测试评价方法

Information security technology—General security technique requirements and testing evaluation method for terminal computer

2012-12-31 发布　　2013-06-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

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、联想控股有限公司。

本标准主要起草人:邱梓华、韦卫、宋好好、王京旭、张艳、顾健、吴秋新、顾玮、赵婷、宁晓魁、邹春明、张笑笑、俞优、冯荣峰。

引　言

本标准包含两部分内容，一部分是终端计算机的通用安全技术要求，用以指导设计者如何设计和实现终端计算机，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的通用安全技术要求和测试评价方法，即主要说明终端计算机为实现 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。本标准将终端计算机划分为五个安全等级，与信息系统的五个等级一一对应。考虑到可信计算是当今终端计算机安全技术主流发展方向，所以在整个终端计算机安全体系设计中凸显可信计算技术理念，特别是在高安全等级（指 3 至 5 级）的安全技术措施设置方面，强调采用基于自主可信计算技术标准的可信计算功能特性，而且我国主流终端计算机厂商已建立起相关产业环境，因此，本标准的技术路线选择能够适应我国终端计算机安全技术产业发展水平；另一部分是依据技术要求，提出了具体的测试评价方法，用以指导评估者对各安全等级的终端计算机评估，同时也对终端计算机的开发者提供指导作用。

本标准部分条款引用了其他标准的内容，有些是直接引用的，有些是间接引用的，对于直接引用的，请参考被引用标准的具体条款。对于间接引用的，以本标准文本的描述为准。

为清晰表示每一个安全等级比较低一级安全等级的安全技术要求的增加和增强，在第 4 章的描述中，每一级的新增部分用**“宋体加粗”**表示。

信息安全技术　终端计算机
通用安全技术要求与测试评价方法

1　范围

本标准按照国家信息安全等级保护的要求，规定了终端计算机的安全技术要求和测试评价方法。

本标准适用于指导终端计算机的设计生产企业、使用单位和信息安全服务机构实施终端计算机等级保护安全技术的设计、实现和评估工作。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999　计算机信息系统　安全保护等级划分准则

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

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　术语和定义、缩略语

3.1　术语和定义

GB 17859—1999、GB/T 20271—2006 和 GB/T 20272—2006 界定的以及下列术语和定义适用于本文件。

3.1.1

终端计算机　terminal computer

供个人使用的、能独立进行数据处理及提供网络服务访问的计算机系统。

注：终端计算机一般为台式微型计算机系统和便携微型计算机系统两种形态，终端计算机通常由硬件系统、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

完整性度量　integrity measurement

使用杂凑算法对被度量对象计算其杂凑值的过程。

3.1.3

完整性度量值　integrity measurement value

部件被杂凑算法计算后得到的杂凑值。

3.1.4

完整性基准值　predefined integrity value

部件在发布时或在可信状态下被度量得到的杂凑值，作为完整性校验的参考基准。

3.1.5

可信度量根　root of trust for measurement

一个能够可靠进行完整性度量的计算引擎，是信任传递链的起始点。

3.1.6

可信存储根　root of trust for storage

一个能够可靠进行安全存储的计算引擎。

3.1.7

动态可信度量根　dynamic root of trust for measurement

可信度量根的一种，支持终端计算机对动态启动的程序模块进行实时可信度量。

3.1.8

可信报告根　root of trust for reporting

一个能够可靠报告可信存储根所保存信息的计算引擎。

3.1.9

可信密码模块　trusted cryptography module

可信计算平台的硬件模块，为可信计算平台提供密码运算功能，具有受保护的存储空间。

3.1.10

信任链　trusted chain

在计算系统启动和运行过程中，使用完整性度量方法在部件之间所建立的信任传递关系。

3.1.11

安全支撑系统　security support system

终端计算机在操作系统安全基础上构建系统身份标识与鉴别、数据保护和运行安全防护等安全功能的系统，支撑终端计算机的安全运行、管理与维护。

3.1.12

终端计算机安全子系统　security subsystem of terminal computer

终端计算机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。

注1：按照GB 17859—1999对TCB(可信计算基)的定义，SSOTC(终端计算机安全子系统)就是终端计算机的TCB。

注2：终端计算机安全子系统建立了一个基本的终端计算机安全保护环境，并提供终端计算机所要求的附加用户服务。终端计算机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进行安全保护。

3.1.13

SSOTC安全功能　SSOTC security function

正确实施SSOTC安全策略的全部硬件、固件、软件所提供的功能。

注：每一个安全策略的实现，组成一个安全功能模块。一个SSOTC的所有安全功能模块共同组成该SSOTC的安全功能。

3.1.14

SSOTC安全控制范围　SSOTC scope of control

SSOTC的操作所涉及的主体和客体。

3.1.15

SSOTC安全策略　SSOTC security policy

对SSOTC中的资源进行管理、保护和分配的一组规则。

注：一个SSOTC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文件：

BIOS	基本输入输出系统	(basic input output system)
MBR	主引导记录	(master boot recorder)

SSC	SSOTC 控制范围	(SSOTC scope of control)
SSF	SSOTC 安全功能	(SSOTC security function)
SSOTC	终端计算机安全子系统	(security subsystem of terminal computer)
SSP	SSOTC 安全策略	(SSOTC security policy)
TCM	可信密码模块	(trusted cryptography module)

4 安全技术要求

4.1 第一级

4.1.1 安全功能要求

4.1.1.1 硬件系统

4.1.1.1.1 设备安全可用

应按 GB/T 20271—2006 中 6.1.1.2 的要求，从以下方面设计和实现终端计算机的设备安全可用功能：

a) 基本运行支持：终端计算机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。

4.1.1.1.2 设备防盗

应按 GB/T 20271—2006 中 6.1.1.2 的要求，从以下方面设计和实现终端计算机的设备防盗功能：

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

4.1.1.2 操作系统

应按 GB/T 20272—2006 中 4.1.1 的要求，从身份鉴别、自主访问控制两个方面，来设计、实现或选购第一级终端计算机所需要的操作系统。

4.1.1.3 安全支撑系统

4.1.1.3.1 运行时防护

应按 GB/T 20271—2006 中 6.1.2.5 的要求，从以下方面设计和实现终端计算机的运行时防护功能：

a) 恶意代码防护：

——对文件系统、内存和使用时的外来介质采用特征码扫描，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。

4.1.1.3.2 备份与故障恢复

为实现确定的恢复功能，应在终端计算机正常运行时定期地或按某种条件实施备份。应根据以下要求，实现备份与故障恢复功能：

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中用户数据丢失或破坏时，应能提供用户数据恢复的功能。

4.1.2 SSOTC 自身安全保护

4.1.2.1 操作系统的自身安全保护

应按 GB/T 20272—2006 中 4.1.2 的要求，设计和实现操作系统的自身安全保护。

4.1.3 SSOTC 设计和实现

SSOTC 的设计和实现要求如下：

a) 配置管理：按 GB/T 20271—2006 中 6.1.5.1 的要求，实现终端计算机第一级的配置管理；

b) 分发和操作：按 GB/T 20271—2006 中 6.1.5.2 的要求，实现终端计算机第一级的分发和操作；

c) 开发：按 GB/T 20271—2006 中 6.1.5.3 的要求，实现终端计算机第一级的开发；

d) 文档要求：按 GB/T 20271—2006 中 6.1.5.4 的要求，实现终端计算机第一级的文档要求；

e) 生存周期支持：按 GB/T 20271—2006 中 6.1.5.5 的要求，实现终端计算机第一级的生存周期支持；

f) 测试：按 GB/T 20271—2006 中 6.1.5.6 的要求，实现终端计算机第一级的测试。

4.1.4 SSOTC 管理

应按 GB/T 20271—2006 中 6.1.6 的要求，从以下方面实现终端计算机第一级的 SSOTC 安全管理：

a) 对相应的 SSOTC 的访问控制、鉴别控制、审计等相关的安全功能，以及与一般的安装、配置和维护有关的功能，制定相应的操作、运行规程和行为规章制度。

4.2 第二级

4.2.1 安全功能要求

4.2.1.1 硬件系统

4.2.1.1.1 设备安全可用

应按 GB/T 20271—2006 中 6.2.1.2 的要求，从以下方面设计和实现终端计算机的设备安全可用功能：

a) 基本运行支持：终端计算机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。

4.2.1.1.2 设备防盗

应按 GB/T 20271—2006 中 6.2.1.2 的要求，从以下方面设计和实现终端计算机的设备防盗功能：

a) 设备标记要求：终端计算机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：终端计算机的主机应有机箱封装保护，防止部件损害或被盗。

4.2.1.2 操作系统

应按 GB/T 20272—2006 中 4.2.1 的要求，从身份鉴别、自主访问控制、安全审计、用户数据保密性、用户数据完整性 5 个方面，来设计、实现或选购第二级终端计算机所需要的操作系统。

4.2.1.3 安全支撑系统

4.2.1.3.1 密码支持

应按以下要求，设计与实现第二级终端计算机的密码支持功能：

a) 密码算法：应使用国家有关主管部门批准的密码算法，密码算法和密码操作应由硬件或受保护的软件支撑实现。

b) 密钥管理：应对密码算法操作所涉及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 GB/T 17901.1—1999 的相关要求。应建立一个可信存储根密钥，所有密钥应受可信存储根保护。可信存储根本身应由硬件密码模块保护。

4.2.1.3.2 运行时防护

应按 GB/T 20271—2006 中 6.2.2.4 和 6.2.2.6 的要求，从以下方面设计和实现终端计算机的运行时防护功能：

a) 恶意代码防护：

——对文件系统、内存和使用时的外来介质采用特征码扫描，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。

b) 网络攻击防护：终端计算机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。应采取的措施为：

——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。

4.2.1.3.3 系统身份标识与鉴别

应按以下要求，设计与实现系统身份标识与鉴别功能：

a) 系统身份标识：

应对终端计算机进行身份标识，确保其身份唯一性和真实性：

——唯一性标识：应通过唯一绑定的硬件密码模块或受保护的软件模块产生的密钥来标识系统身份；

b) 系统身份鉴别：

在进行终端计算机身份鉴别时，请求方应提供系统的身份标识，通过一定的认证协议完成身份鉴别过程。

4.2.1.3.4 数据保密性保护

应按 GB/T 20271—2006 中 6.2.3.4 的数据保密性要求，从以下方面设计和实现终端计算机的数据保密性功能：

a) 数据存储保密性：

应对存储在终端计算机内的重要用户数据进行保密性保护：

——例如数据加密：应确保加密后的数据由密钥的合法持有者解密，除合法持有密钥者外，其余任何用户不应获得该数据；

b) 数据传输保密性：

对在不同 SSF 之间基于网络传输的重要数据，设计和实现数据传输保密性保护功能，确保数据在传输过程中不被泄漏和窃取。

4.2.1.3.5 安全审计

应按 GB/T 20271—2006 中 6.2.2.3 的要求，从以下方面设计和实现安全支撑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、系统身份标识与鉴别、数据保密性保护等安全功能的设计紧密结合；

b) 支持审计日志；

——可为以下安全事件产生审计记录：

绑定于终端计算机的硬件密码模块应该能审计内部运行的可审计事件，能提供给上层应用软件查询审计情况的接口；

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；

——支持审计查阅：

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；

——提供审计事件选择：

应根据以下属性选择终端计算机的可审计事件：客体身份、用户身份、主体身份、主机身份、事件类型；作为审计选择性依据的附加属性。

4.2.1.3.6 备份与故障恢复

为了实现确定的恢复功能，应在终端计算机正常运行时定期地或按某种条件实施备份。应根据以下要求，实现备份与故障恢复功能：

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) 系统备份与恢复：应提供定期对终端计算机进行定期备份的功能；当由于某种原因引起终端计算机发生故障时，应提供用户按系统备份所保留的信息进行系统恢复的功能。

4.2.2 SSOTC 自身安全保护

4.2.2.1 安全支撑系统的自身安全保护

a) 可信存储根安全保护：应按以下要求实现终端计算机的可信存储根：

——可信存储根应设置在硬件密码模块内；

——所采用的硬件密码模块和软件密码模块应符合国家相关密码管理要求；

b) 用户使用硬件密码模块前应进行身份鉴别。

4.2.2.2 操作系统的自身安全保护

应按 GB/T 20272—2006 中 4.2.2 的要求，设计和实现操作系统的自身安全保护。

4.2.3 SSOTC 设计和实现

SSOTC 的设计和实现要求如下：

a) 配置管理：应按 GB/T 20271—2006 中 6.2.5.1 的要求，实现终端计算机第二级的配置管理；

b) 分发和操作：应按 GB/T 20271—2006 中 6.2.5.2 的要求，实现终端计算机第二级的分发和操作；

c) 开发：应按 GB/T 20271—2006 中 6.2.5.3 的要求，实现终端计算机第二级的开发；

d) 文档要求：应按 GB/T 20271—2006 中 6.2.5.4 的要求，实现终端计算机第二级的文档要求；

e) 生存周期支持：应按 GB/T 20271—2006 中 6.2.5.5 的要求，实现终端计算机第二级的生存周期支持；

f) 测试：应按 GB/T 20271—2006 中 6.2.5.6 的要求，实现终端计算机第二级的测试。

4.2.4 SSOTC 管理

一般应按 GB/T 20271—2006 中 6.2.6 的要求，从以下方面实现终端计算机第二级的 SSOTC 安全

管理：

a) 对相应的 SSOTC 的访问控制、鉴别控制、审计等相关的安全功能，以及与一般的安装、配置和维护有关的功能，制定相应的操作、运行规程和行为规章制度；

b) 根据本级中安全功能技术要求和安全保证技术要求所涉及的安全属性，设计 SSOTC 安全属性管理。

4.3 第三级

4.3.1 安全功能要求

4.3.1.1 硬件系统

4.3.1.1.1 设备安全可用

应按 GB/T 20271—2006 中 6.3.1.2 的要求，从以下方面设计和实现终端计算机的设备安全可用功能：

a) 基本运行支持：终端计算机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。

4.3.1.1.2 设备防盗

应按 GB/T 20271—2006 中 6.3.1.2 的要求，从以下方面设计和实现终端计算机的设备防盗功能：

a) 设备标记要求：终端计算机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：终端计算机的主机应有机箱封装保护，防止部件损害或被盗。

4.3.1.2 操作系统

应按 GB/T 20272—2006 中 4.3.1 的要求，从身份鉴别、自主访问控制、**标记、强制访问控制**、安全审计、用户数据保密性、用户数据完整性**7 个**方面，来设计、实现或选购**第三级**终端计算机所需要的操作系统。

4.3.1.3 安全支撑系统

4.3.1.3.1 密码支持

应按以下要求，设计与实现第三级终端计算机密码支持功能。

a) 密码算法：应使用国家密码管理部门批准的密码算法，并**应采用密码硬件实现密码算法。**

b) 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。其中密钥生成、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：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 GB/T 17901.1—1999 的相关要求。应建立一个可信存储根密钥，所有密钥应受可信存储根保护，**可信存储根本身应由可信密码模块保护。**

4.3.1.3.2 运行时防护

应按 GB/T 20271—2006 中 6.3.2.5 和 6.3.2.7 的要求，从以下方面设计和实现第三级终端计算

机的运行时防护功能：

a） 恶意代码防护：

——特征码扫描：对文件系统、内存和使用时的外来介质采用特征码扫描，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。

b） 网络攻击防护：终端计算机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：

——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；

——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。

4.3.1.3.3 系统安全性检测分析

应按 GB/T 20271—2006 中 6.3.2.2 的要求，设计和实现终端计算机第三级的系统安全性检测分析功能：

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。

4.3.1.3.4 系统身份标识与鉴别

a） 系统身份标识：

应对终端计算机进行身份标识，确保其身份唯一性和真实性：

——唯一性标识：应通过唯一绑定的可信密码模块产生的密钥来标识系统身份，该身份密钥即为可信报告根。

——标识可信性：身份标识可信性应通过国家批准的权威机构颁发证书来实现。

——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。

——标识信息管理：应对终端计算机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。

b） 系统身份鉴别：

在进行终端计算机身份鉴别时，请求方应提供系统的身份证书和/或证书信任链验证路径，并通过一定的认证协议完成身份鉴别过程。

4.3.1.3.5 数据保密性保护

应按 GB/T 20271—2006 中 6.3.3.8 的数据保密性要求，从以下方面设计和实现终端计算机的数据保密性功能：

a） 数据存储保密性：

应对存储在终端计算机内的重要用户数据进行保密性保护：

——例如数据加密：应确保加密后的数据由密钥的合法持有者解密，除合法持有密钥者外，其余任何用户不应获得该数据。

——数据绑定：如果基于可信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中解密。

b） 数据传输保密性：

对在不同 SSF 之间基于网络传输的重要数据，设计和实现数据传输保密性保护功能，确保数据在传输过程中不被泄漏和窃取。

4.3.1.3.6 安全审计

应按 GB/T 20271—2006 中 6.3.2.4 的要求，从以下方面设计和实现安全支撑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、系统身份标识与鉴别、数据保密性保护等安全功能的设计紧密结合；

b） **支持审计日志；**

——可为以下安全事件产生审计记录：

内置于终端计算机的可信密码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，能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；

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；

——支持潜在侵害分析：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；

——支持审计查阅：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；**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提供对审计数据进行搜索、分类、排序的能力；**

——提供审计事件选择：应根据以下属性选择终端计算机的可审计事件：客体身份、用户身份、主体身份、主机身份、事件类型；作为审计选择性依据的附加属性；

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。**

4.3.1.3.7 备份与故障修复

为实现确定的恢复功能，应在终端计算机正常运行时定期地或按某种条件实施备份。应根据以下要求，实现备份与故障恢复功能：

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） 系统备份与恢复：应提供定期对终端计算机的**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发生故障时，应提供用户按系统备份所保留的**现场信息**进行系统恢复的功能；

c） **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。**

4.3.1.3.8 I/O 接口配置

应配置终端计算机的 USB、网卡、硬盘等各类 I/O 接口和设备的启用/禁用等状态，并按以下要求，设计和实现终端计算机的 I/O 接口配置功能：

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。**

4.3.2 SSOTC 自身安全保护

4.3.2.1 安全支撑系统的自身安全保护

a） **可信存储根安全保护：应按以下要求实现终端计算机的可信存储根：**

——可信存储根应设置在可信密码模块内；

——可信密码模块应符合国家密码管理部门的相关规范和管理要求；

b) 可信报告根安全保护：应按以下要求实现终端计算机的可信报告根：

——可信报告根应设置在可信密码模块内；

——可信报告根对应的公钥证书应由国家批准的权威机构发行和管理；

c) 用户使用可信密码模块之前需进行身份鉴别。

4.3.2.2 操作系统的自身安全保护

应按 GB/T 20272—2006 中 4.3.2 的要求，设计和实现操作系统的自身安全保护。

4.3.3 SSOTC 设计和实现

SSOTC 的设计和实现要求如下：

a) 配置管理：应按 GB/T 20271—2006 中 6.3.5.1 的要求，实现终端计算机第三级的配置管理；

b) 分发和操作：应按 GB/T 20271—2006 中 6.3.5.2 的要求，实现终端计算机第三级的分发和操作；

c) 开发：应按 GB/T 20271—2006 中 6.3.5.3 的要求，实现终端计算机第三级的开发；

d) 文档要求：应按 GB/T 20271—2006 中 6.3.5.4 的要求，实现终端计算机第三级的文档要求；

e) 生存周期支持：应按 GB/T 20271—2006 中 6.3.5.5 条的要求，实现终端计算机第三级的生存周期支持；

f) 测试：应按 GB/T 20271—2006 中 6.3.5.6 的要求，实现终端计算机第三级的测试；

g) 脆弱性评定：应按 GB/T 20271—2006 中 6.3.5.7 的要求，实现第三级的脆弱性评定。

4.3.4 SSOTC 管理

一般应按 GB/T 20271—2006 中 6.3.6 的要求，从以下方面实现终端计算机第三级的 SSOTC 安全管理：

a) 对相应的 SSOTC 的访问控制、鉴别控制、审计等相关的安全功能，以及与一般的安装、配置和维护有关的功能，制定相应的操作、运行规程和行为规章制度；

b) 根据本级中安全功能技术要求和安全保证技术要求所涉及的安全属性，设计 SSOTC 安全属性管理；

c) 根据本级中安全功能技术要求和安全保证技术要求所涉及的安全数据，设计 SSOTC 安全数据管理；

d) 应将系统管理员、安全员和审计员等重要安全角色分别设置专人担任，并按“职能分离原则”分别授予他们各自为完成自身任务所需的权限，并形成相互制约的关系。

4.4 第四级

4.4.1 安全功能要求

4.4.1.1 硬件系统

4.4.1.1.1 设备安全可用

应按 GB/T 20271—2006 中 6.4.1.2 的要求，从以下方面设计和实现终端计算机的设备安全可用功能：

a) 基本运行支持：终端计算机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) **设备安全可用：终端计算机的设备应满足安全可用的要求，包括主机、外部设备、网络连接部件及其他辅助部件等均应安全可用。**

4.4.1.1.2 设备防盗

应按 GB/T 20271—2006 中 6.4.1.2 的要求，从以下方面设计和实现终端计算机的设备防盗功能：

a) 设备标记要求：终端计算机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：终端计算机的主机应有机箱封装保护，防止部件损害或被盗；

c) 设备防盗要求：终端计算机的设备应提供拥有者可控的防盗报警功能。

4.4.1.2 操作系统

应按 GB/T 20272—2006 中 4.4.1 的要求，从身份鉴别、自主访问控制、标记、强制访问控制、安全审计、用户数据保密性、用户数据完整性、**可信路径 8 个**方面，来设计、实现或选购**第四级**终端计算机所需要的操作系统。

4.4.1.3 安全支撑系统

4.4.1.3.1 密码支持

应按以下要求，设计与实现**第四级**终端计算机密码支持功能：

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

b) 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。其中密钥生成、数字签名生成和验证等关键密码操作应基于可信密码模块或其他硬件密码模块支持；

c) 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 GB/T 17901.1—1999 的相关要求。应建立一个可信存储根密钥，所有密钥应受可信存储根保护，可信存储根本身应由可信密码模块保护。

4.4.1.3.2 信任链

应通过在终端计算机启动过程中提供的信任链支持，确保终端计算机的运行处于真实可信状态。并按以下要求，设计和实现终端计算机第四级的信任链功能：

a) 静态信任链建立：基于可信密码模块，利用终端计算机上的可信度量根，在系统启动过程中对 BIOS、MBR、OS 部件模块进行完整性度量，度量值应存储于可信密码模块中。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的完整性度量基准接受国家主管机构管理，支持离线校验；完整性度量基准应存储在受可信存储根保护的区域中，若度量值与完整性度量基准不一致，应停止操作系统启动。

c) 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。

4.4.1.3.3 运行时防护

应按 GB/T 20271—2006 中 6.4.2.5 和 6.4.2.7 的要求，从以下方面设计和实现第四级终端计算机的运行时防护功能：

a) 恶意代码防护：

——特征码扫描：对文件系统、内存和使用时的外来介质采用特征码扫描，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。

——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。

——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。

b) 网络攻击防护：终端计算机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：

——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；

——内容过滤：应能对网页内容进行基于关键字匹配的过滤；

——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；

——实现注册表监控、文件监控、事件监测、实时流量分析、实时阻断的入侵检测功能；

c) 网络接入控制：终端计算机应能对所接入网络进行可信度评价（包含以下方面：网络提供者是否可信、网络状态和接入条件是否符合设定策略、网络提供的服务是否符合需求，等），并根据不同可信度评价等级采取不同的安全接入策略。

4.4.1.3.4 系统安全性检测分析

应按 GB/T 20271—2006 中 6.4.2.2 的要求，设计和实现终端计算机第四级的系统安全性检测分析功能：

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) 电磁泄漏发射检测分析：应对运行中的终端计算机环境进行电磁泄漏发射检测，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的安全性所造成的威胁，并提出补救措施。

4.4.1.3.5 信任服务

终端计算机建立静态信任链后，可以在对完整性度量值由可信报告根进行数字签名后，对系统用户或系统外部实体实现信任报告。

应根据以下要求，设计与实现终端计算机的第四级信任服务功能：

a) 应在可信密码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，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，所有度量值存取访问应受权限控制；

b) 必要时应向国家主管机构报告操作系统和关键应用程序完整性度量值。

4.4.1.3.6 系统身份标识与鉴别

a) 系统身份标识：

应对终端计算机进行身份标识，确保其身份唯一性和真实性：

——唯一性标识：应通过唯一绑定的可信密码模块产生的密钥来标识系统身份，该身份密钥即为终端计算机的可信报告根。

——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。

——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。

——标识信息管理：应对终端计算机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。

b) 系统身份鉴别：

在进行终端计算机身份鉴别时，请求方应提供系统的身份证书和/或证书信任链验证路径，并通过一定的认证协议完成身份鉴别过程。

4.4.1.3.7 数据保密性保护

应按 GB/T 20271—2006 中 6.4.3.8 的数据保密性要求，从以下方面设计和实现安全支撑系统的数据保密性功能：

a) 数据存储保密性：

应对存储在终端计算机内的重要用户数据进行保密性保护：

——例如数据加密：应确保加密后的数据由密钥的合法持有者解密，除合法持有密钥者外，其余任何用户不应获得该数据；

——数据绑定：如果基于可信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中解密；

——数据密封：如果基于可信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的特定状态下解密；

b) 数据传输保密性：

对在不同 SSF 之间传输的数据，设计和实现数据传输保密性保护功能，确保数据在传输过程中不被泄漏和窃取；

c) **客体安全重用：**

对安全支撑系统进行动态资源管理过程中，对客体资源中的剩余信息不应引起信息的泄漏。根据本安全等级要求，应实现安全支撑系统如下客体安全重用功能：

——子集信息保护：由安全支撑系统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；

——完全信息保护：由安全支撑系统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。

4.4.1.3.8 数据完整性保护

应按以下要求，实现安全支撑系统内部存储、传输和处理的数据的完整性保护功能。

a) **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：

——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；

——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；

b) **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：

——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；

——数据交换恢复：由接收者借助于源可信信息系统提供的信息，或由接收者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；

c) **处理数据的完整性：**

回退：对终端计算机中处理中的数据，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。

4.4.1.3.9 安全审计

应按 GB/T 20271—2006 中 6.4.2.4 的要求，从以下方面设计和实现安全支撑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、系统身份标识与鉴别、**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；**

——可为以下安全事件产生审计记录：

内置于终端计算机的可信密码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，能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；

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；

——支持安全审计分析

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；

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；

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；

——支持审计查阅：

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；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；

——提供审计事件选择：

应根据以下属性选择终端计算机的可审计事件：客体身份、用户身份、主体身份、主机身份、事件类型；作为审计选择性依据的附加属性；

——提供审计事件存储：

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；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；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；

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地访问、修改和破坏。

4.4.1.3.10 备份与故障恢复

为实现确定的恢复功能，应在终端计算机正常运行时定期地或按某种条件实施备份。应根据以下要求，实现备份与故障恢复功能：

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) 系统备份与恢复：应提供定期对终端计算机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发生故障时，应提供用户按系统备份所保留的现场信息进行系统恢复的功能；

c) 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。

4.4.1.3.11 I/O 接口配置

应配置终端计算机的串口、并口、USB、网卡、硬盘等各类 I/O 接口和设备的启用/禁用等状态，并按以下要求，设计和实现终端计算机的 I/O 接口配置功能：

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。

4.4.1.3.12 可信时间戳

终端计算机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 中 5.1.2.7 的要求提供可信时间戳服务。

4.4.2 SSOTC 自身安全保护

4.4.2.1 安全支撑系统的自身安全保护

a) 可信存储根安全保护：应按以下要求实现终端计算机的可信存储根：

——可信存储根应设置在可信密码模块内；

——可信密码模块应由国家主管机构研制；

b) 可信报告根安全保护：应按以下要求实现终端计算机的可信报告根：

——可信报告根应设置在可信密码模块内；

——可信报告根对应的公钥证书应有国家专门权威机构发行和管理；

c) 可信度量根安全保护：应按以下要求实现终端计算机的可信度量根：

——可信度量根应设置在终端计算机启动的固件模块内；

——应对可信度量根采取物理保护措施；

d) 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密码模块的直接通信；

——应有物理开关控制是否启用键盘输入与可信密码模块的通信路径；

e) 用户使用可信密码模块之前需进行身份鉴别。

4.4.2.2 操作系统的自身安全保护

应按 GB/T 20272—2006 中 4.4.2 的要求，设计和实现操作系统的自身安全保护。

4.4.3 SSOTC 设计和实现

SSOTC 的设计和实现要求如下：

a) **配置管理：应按 GB/T 20271—2006 中 6.4.5.1 的要求，实现终端计算机第四级的配置管理；**

b) **分发和操作：应按 GB/T 20271—2006 中 6.4.5.2 的要求，实现终端计算机第四级的分发和操作；**

c) **开发：应按 GB/T 20271—2006 中 6.4.5.3 的要求，实现终端计算机第四级的开发；**

d) **文档要求：应按 GB/T 20271—2006 中 6.4.5.4 的要求，实现终端计算机第四级的文档要求；**

e) **生存周期支持：应按 GB/T 20271—2006 中 6.4.5.5 的要求，实现终端计算机第四级的生存周期支持；**

f) **测试：应按 GB/T 20271—2006 中 6.4.5.6 的要求，实现终端计算机第四级的测试；**

g) **脆弱性评定：应按 GB/T 20271—2006 中 6.4.5.7 的要求，实现网络第四级的脆弱性评定。**

4.4.4 SSOTC 管理

应按 GB/T 20271—2006 中 6.4.6 的要求，从以下方面实现终端计算机**第四级**的 SSOTC 安全管理：

a) 对相应的 SSOTC 的访问控制、鉴别控制、审计等相关的安全功能，以及与一般的安装、配置和维护有关的功能，制定相应的操作、运行规程和行为规章制度；

b) 根据本级中安全功能技术要求和安全保证技术要求所涉及的安全属性，设计 SSOTC 安全属性管理；

c) 根据本级中安全功能技术要求和安全保证技术要求所涉及的安全数据，设计 SSOTC 安全数据管理；

d) 应将系统管理员、安全员和审计员等重要安全角色分别设置专人担任，并按“职能分离原则”分别授予他们各自为完成自身任务所需的权限，并形成相互制约的关系；

e) **支持集中安全管理。**

4.5 第五级

4.5.1 安全功能要求

4.5.1.1 硬件系统

4.5.1.1.1 设备安全可用

应按 GB/T 20271—2006 中 6.5.1.2 的要求，从以下方面设计和实现终端计算机的设备安全可用功能：

a) 基本运行支持：终端计算机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) **设备安全可用：终端计算机的设备应满足安全可用的要求，包括主机、外部设备、网络连接部件及其他辅助部件等均应安全可用。**

4.5.1.1.2 设备防盗

应按 GB/T 20271—2006 中 6.5.1.2 的要求，从以下方面设计和实现终端计算机的设备防盗功能：

a) 设备标记要求：终端计算机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：终端计算机的主机应有机箱封装保护，防止部件损害或被盗；
c) 设备防盗要求：终端计算机的设备应提供拥有者可控的防盗报警功能。

4.5.1.1.3 设备高可靠

应按以下要求，设计和实现终端计算机设备高可靠功能：

a) 防水要求：终端计算机应具有高密封性，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：终端计算机应能抵御电磁干扰和电磁辐射对系统的安全威胁。

4.5.1.2 操作系统

应按 GB/T 20272—2006 中 4.5.1 的要求，从身份鉴别、自主访问控制、标记、强制访问控制、安全审计、用户数据保密性、用户数据完整性、可信路径 8 个方面，来设计、实现或选购第五级终端计算机所需要的操作系统。

4.5.1.3 安全支撑系统

4.5.1.3.1 密码支持

应按以下要求，设计与实现第五级终端计算机密码支持功能：

a) 密码算法：应使用国家密码管理部门批准的密码算法，并应采用密码硬件实现密码算法；
b) 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。其中密钥生成、数字签名生成和验证等关键密码操作应基于可信密码模块或其他硬件密码模块支持。
c) 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 GB/T 17901.1—1999 的相关要求。所有密钥应受可信存储根保护，可信存储根本身应由可信密码模块保护。

4.5.1.3.2 信任链

应通过在终端计算机启动过程中提供的信任链支持，确保终端计算机的运行处于真实可信状态。并按以下要求，设计和实现终端计算机第五级的信任链功能：

a) 静态信任链建立：基于可信密码模块，利用终端计算机上的可信度量根，在系统启动过程中对 BIOS、MBR、OS 部件模块进行完整性度量，度量值应存储于可信密码模块中。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的完整性度量基准接受国家主管机构管理，支持离线校验；完整性度量基准应存储在受可信存储根保护的区域中，若度量值与完整性度量基准不一致，应停止操作系统启动。
c) 动态信任链的建立：基于可信密码模块，利用终端计算机上的动态可信度量根，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) 动态信任链中关键应用程序的完整性度量基准应由国家主管机构管理，支持在线离线校验，完整性度量基准应存储在受可信存储根保护的区域中，若度量值与完整性度量基准不一致，应立即停止应用程序运行。

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。

4.5.1.3.3 运行时防护

应按 GB/T 20271—2006 中 6.5.2.5 和 6.5.2.7 的要求，从以下方面设计和实现第五级终端计算机的运行时防护功能：

a) 恶意代码防护：
   ——特征码扫描：对文件系统、内存和使用时的外来介质采用特征码扫描，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。
   ——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。
   ——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。
   ——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。
b) 网络攻击防护：终端计算机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：
   ——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；
   ——内容过滤：应能对网页内容进行基于关键字匹配的过滤；
   ——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；
   ——实现注册表监控、文件监控、事件监测、实时流量分析、实时阻断的入侵检测功能。
c) 网络接入控制：终端计算机应能对所接入网络进行可信度评价（包含以下方面：网络提供者是否可信、网络状态和接入条件是否符合设定策略、网络提供的服务是否符合需求，等等），并根据不同可信度评价等级采取不同的安全接入策略。

4.5.1.3.4 系统安全性检测分析

应按 GB/T 20271—2006 中 6.5.2.2 的要求，设计和实现终端计算机**第五级**的系统安全性检测分析功能：

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) 电磁泄漏发射检测分析：应对运行中的终端计算机环境进行电磁泄漏发射检测，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的安全性所造成的威胁，并提出补救措施。

4.5.1.3.5 信任服务

终端计算机建立静态信任链后，可以对完整性度量值由可信报告根进行数字签名后，对系统用户或

系统外部实体实现信任报告。

应根据以下要求，设计与实现终端计算机的**第五级**信任服务功能：

a） 应在可信密码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，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，所有度量值存取访问应受权限控制；

b） 应设置一个由可信密码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） 必要时应向国家主管机构报告操作系统和**应用程序**完整性度量值。

4.5.1.3.6 系统身份标识与鉴别

a） 系统身份标识：

应对终端计算机进行身份标识，确保其身份唯一性和真实性。

——唯一性标识：应通过唯一绑定的可信密码模块产生的密钥来标识系统身份。

——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。

——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。

——标识信息管理：应对终端计算机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。

b） 系统身份标识应由国家权威管理机构进行管理。

c） 系统身份鉴别：在进行终端计算机身份鉴别时，请求方应提供系统的身份证书和/或证书信任链验证路径，并通过一定的认证协议完成身份鉴别过程。

4.5.1.3.7 数据保密性保护

应按 GB/T 20271—2006 中 6.5.3.8 的数据保密性要求，从以下方面设计和实现安全支撑系统的数据保密性功能：

a） 数据存储保密性：

应对存储在终端计算机内的重要用户数据进行保密性保护，

——例如数据加密：应确保加密后的数据由密钥的合法持有者解密，除合法持有密钥者外，其余任何用户不应获得该数据；

——数据绑定：如果基于可信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中解密；

——数据密封：如果基于可信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的特定状态下解密；

b） 数据传输保密性：

按所配置的密码，对在不同 SSF 之间传输的数据，设计和实现数据传输保密性保护功能，确保数据在传输过程中不被泄漏和窃取；

c） 客体安全重用：

在安全支撑系统进行动态资源管理过程中，客体资源中的剩余信息不应引起信息的泄漏。根据本安全等级要求，应实现安全支撑系统如下客体安全重用功能：

——子集信息保护：由安全支撑系统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；

——完全信息保护：由安全支撑系统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；

——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。

4.5.1.3.8 数据完整性保护

应按以下要求，实现安全支撑系统内部存储、处理和传输的数据的**完整性**保护功能。

a) 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：

——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；

——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；

b) 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：

——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；

——数据交换恢复：由接收者借助于源可信信息系统提供的信息，或由接收者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；

c) 处理数据的完整性：

回退：对终端计算机中处理中的数据，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。

4.5.1.3.9 安全审计

应按 GB/T 20271—2006 中 6.5.2.4 的要求，从以下方面设计和实现安全支撑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、系统身份标识与鉴别、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：

——支持安全审计响应

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；当检测到可能有安全侵害事件时，生成实时报警信息；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；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；

——可为以下安全事件产生审计记录：

内置于终端计算机的可信密码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，能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；

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；

——支持安全审计分析

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；

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；

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；

——支持审计查阅

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；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；

——提供审计事件选择

应根据以下属性选择终端计算机的可审计事件：客体身份、用户身份、主体身份、主机身份、事件类型；作为审计选择性依据的附加属性；

——提供审计事件存储

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；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；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；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；

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。

4.5.1.3.10 备份与故障修复

为实现确定的恢复功能，应在终端计算机正常运行时定期地或按某种条件实施备份。应根据以下要求，实现备份与故障恢复功能：

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) 系统备份与恢复：应提供定期对终端计算机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发生故障时，应提供用户按系统备份所保留的现场信息进行系统恢复的功能；

c) 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。

4.5.1.3.11 I/O 接口配置

应配置终端计算机的串口、并口、USB、网卡、硬盘等各类 I/O 接口和设备的启用/禁用等状态，并按以下要求，设计和实现终端计算机的 I/O 接口配置功能：

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。

4.5.1.3.12 可信时间戳

终端计算机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 中 5.1.2.7 的

要求提供可信时间戳服务。

4.5.2 SSOTC 自身安全保护

4.5.2.1 安全支撑系统的自身安全保护

a) 可信存储根安全保护：应按以下要求实现终端计算机的可信存储根：
——可信存储根应设置在可信密码模块内；
——可信密码模块应由国家主管机构研制；
b) 可信报告根安全保护：应按以下要求实现终端计算机的可信报告根：
——可信报告根应设置在可信密码模块内；
——可信报告根对应的公钥证书应有国家专门权威机构发行和管理；
c) 可信度量根安全保护：应按以下要求实现终端计算机的可信度量根：
——可信度量根应设置在终端计算机启动的固件模块内；
——应对可信度量根采取物理保护措施；
d) 动态可信度量根安全保护：应按以下要求实现终端计算机的动态可信度量根：
——动态可信度量根应设置在终端计算机的自主虚拟机监控器；
——应对动态可信度量根采取安全保护措施；
e) 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密码模块的直接通信；
——应有物理开关控制是否启用键盘输入与可信密码模块的通信路径；
f) 用户使用可信密码模块之前需进行身份鉴别。

4.5.2.2 操作系统的自身安全保护

应按 GB/T 20272—2006 中 4.5.2 的要求，设计和实现操作系统的自身安全保护。

4.5.3 SSOTC 设计和实现

SSOTC 的设计和实现要求如下：

a) 配置管理：应按 GB/T 20271—2006 中 6.5.5.1 的要求，实现终端计算机第五级的配置管理；
b) 分发和操作：应按 GB/T 20271—2006 中 6.5.5.2 的要求，实现终端计算机第五级的分发和操作；
c) 开发：应按 GB/T 20271—2006 中 6.5.5.3 的要求，实现终端计算机第五级的开发；
d) 文档要求：应按 GB/T 20271—2006 中 6.5.5.4 的要求，实现终端计算机第五级的文档要求；
e) 生存周期支持：应按 GB/T 20271—2006 中 6.5.5.5 的要求，实现终端计算机第五级的生存周期支持；
f) 测试：应按 GB/T 20271—2006 中 6.5.5.6 的要求，实现终端计算机第五级的测试；
g) 脆弱性评定：应按 GB/T 20271—2006 中 6.5.5.7 的要求，实现网络第五级的脆弱性评定。

4.5.4 SSOTC 管理

应按 GB/T 20271—2006 中 6.5.6 的要求，从以下方面实现终端计算机**第五级**的 SSOTC 安全管理：

a) 对相应的 SSOTC 的访问控制、鉴别控制、审计等相关的安全功能，以及与一般的安装、配置和维护有关的功能，制定相应的操作、运行规程和行为规章制度；
b) 根据本级中安全功能技术要求和安全保证技术要求所涉及的安全属性，设计 SSOTC 安全属

性管理；

c) 根据本级中安全功能技术要求和安全保证技术要求所涉及的安全数据，设计 SSOTC 安全数据管理；

d) 应将系统管理员、安全员和审计员等重要安全角色分别设置专人担任，并按“职能分离原则”分别授予他们各自为完成自身任务所需的权限，并形成相互制约的关系；

e) 支持集中安全管理。

5 测试评价方法

5.1 测试环境

终端计算机的典型测试环境如图 1 所示：

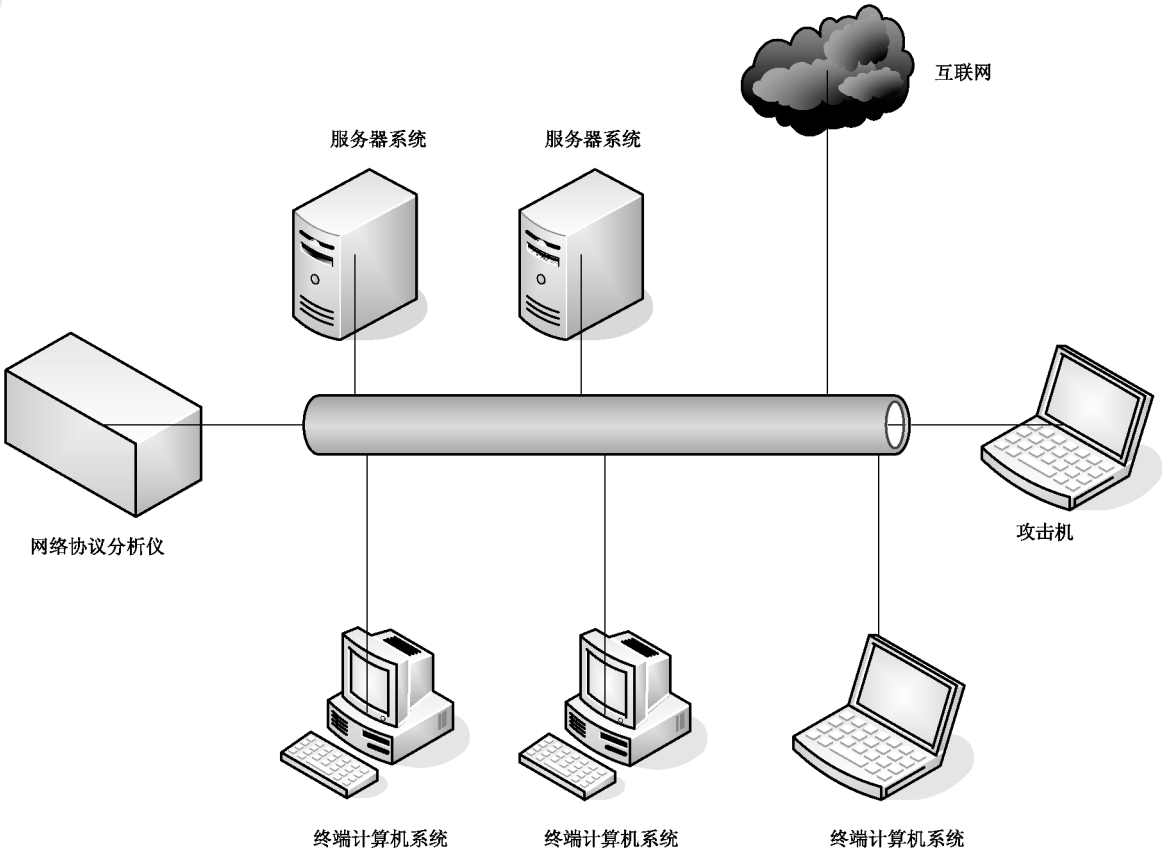

图 1 终端计算机典型测试环境

测试环境中包含 3 台被测的终端计算机，2 台终端计算机访问的服务器系统，一台攻击机能够对终端计算机发起各类攻击，一台网络协议分析仪能够对终端计算机的网络数据进行分析。

5.2 第一级

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

——测试评价内容：

见 4.1.1.1.1 的内容。

——对开发者的要求：

开发者应提供文档，说明终端计算机的设备提供哪些基本的运行支持措施，提供哪些必要的容错和故障恢复能力。

——测试评价方法：

a) 按照开发者提供的文档，逐项验证所提供的运行支持措施是否有效，能否支持终端计算机的基本运行；

b) 按照开发者提供的文档，模拟出现一些故障事件（如：掉电、硬件故障等），验证终端计算机的容错和故障恢复能力是否有效。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.1.1.2 设备防盗

——测试评价内容：

见 4.1.1.1.2 的内容。

——对开发者的要求：

开发者应提供文档，说明终端计算机的设备具有哪些无法除去的标记。

——测试评价方法：

a) 按照开发者提供的文档，尝试使用各种方式除去设备中的标记，检测能否除去。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.1.2 操作系统

——测试评价内容：

见 4.1.1.2 的内容。

——对开发者的要求：

开发者应提供第三方权威机构对该操作系统的检测报告，或者提供文档对 GB/T 20272—2006 中 4.1.1 的各个项目进行说明。

——测试评价方法：

a) 如果提供了第三方权威机构对该操作系统的检测报告，则查验报告，查看报告中对应项目检测结果是否符合；

b) 如果未能提供第三方权威机构对该操作系统的检测报告，则按照 GB/T 20272—2006 中4.1.1 的要求对操作系统的相关项目进行检测。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.1.3 安全支撑系统

5.2.1.3.1 运行时防护

——测试评价内容：

见 4.1.1.3.1 的内容。

——测试评价方法：

a) 在系统和外来介质中植入一个测试用的恶意代码，并运行恶意代码；

b) 对文件系统、内存和使用时的外来介质进行扫描，检测系统能否清除或隔离恶意代码；

c) 检测系统能否对恶意代码特征库进行及时更新。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.1.3.2 备份与故障恢复

——测试评价内容：

见 4.1.1.3.2 的内容。

——测试评价方法：

a) 以授权用户身份有选择地备份重要数据，对系统中已备份的用户数据进行修改，然后进行恢复，检测能否按照备份信息有效恢复。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.2 SSOTC 自身安全保护

5.2.2.1 操作系统的自身安全保护

——测试评价内容：

见 4.1.2.1 的内容。

——对开发者的要求：

开发者应提供第三方权威机构对该操作系统的检测报告，或者提供文档对 GB/T 20272—2006 中4.1.2的各个项目进行说明。

——测试评价方法：

a) 如果提供了第三方权威机构对该操作系统的检测报告，则查验报告，查看报告中对应项目检测结果是否符合；

b) 如果未能提供第三方权威机构对该操作系统的检测报告，则按照 GB/T 20272—2006 中4.1.2的要求对操作系统的相关项目进行检测。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3 SSOTC 设计和实现

5.2.3.1 配置管理

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.1 的要求，实现终端计算机第一级的配置管理。

——测试评价方法：

评估者应审查开发者提供的配置管理支持文档是否完全符合以下要求：

a) 开发者所使用的版本号与所应表示的终端计算机样本应完全对应，没有歧义。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3.2 分发和操作

5.2.3.2.1 分发

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.2 a) 的要求，实现终端计算机第一级的分发。

——测试评价方法：

a) 评估者应审查开发者是否按分发过程的要求，编制分发文档；

b) 评估者应审查分发文档，是否描述给用户分发终端计算机时，用以维护安全所必须的所有过程；

c) 评估者应审查是否按该过程进行分发。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3.2.2 操作

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.2 b）的要求，实现终端计算机第一级的操作。

——测试评价方法：

a） 评估者应审查操作文档，是否说明了终端计算机的安装、生成、启动和使用的过程。用户能够通过此文档了解安装、生成、启动和使用过程。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3.3 开发

5.2.3.3.1 功能设计

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.3 a）的要求，实现终端计算机第一级的功能设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a） 功能设计应当使用非形式化风格来描述终端计算机安全功能与其外部接口；

b） 功能设计应当是内在一致的；

c） 功能设计应当描述使用所有外部终端计算机安全功能接口的目的与方法，适当的时候，要提供结果影响例外情况和错误信息的细节。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3.3.2 高层设计

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.3 b）的要求，实现终端计算机第一级的高层设计。

——测试评价方法：

评估者应审查开发者所提供的高层设计文档是否满足如下要求：

a） 以子系统的观点、以非形式化的方法来一致性地描述终端计算机的体系结构；

b） 描述每一个子系统所提供的安全功能及其相互关系；

c） 标识安全功能要求的任何基础性的硬件、固件和/或软件，并且通过这些硬件、固件和/或软件所实现的保护机制，来提供安全功能功能；

d） 标识安全功能子系统的所有接口，并标明安全功能子系统的哪些接口是外部可见的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3.3.3 低层设计

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.3 c）的要求，实现终端计算机第一级的低层设计。

——测试评价方法：

评估者应审查开发者所提供的低层设计文档是否满足如下要求：

a） 低层设计的表示应是非形式化的，内在一致的，并以模块术语描述；

b） 描述每一个模块的目的；

c） 以所提供的安全功能和对其他模块的依赖性术语定义模块间的相互关系；

d) 描述如何提供每一个安全策略功能的实施；

e) 标识终端计算机安全功能模块的所有接口，标识终端计算机安全功能模块的哪些接口是外部可见的，以及描述终端计算机安全功能模块所有接口的目的与方法，必要时，应提供影响、例外情况和错误信息的细节；

f) 描述如何将终端计算机分离成安全策略实施模块和其他模块。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3.3.4 内部结构设计

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.3 d) 的要求，实现终端计算机第一级的内部结构设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 应以模块化方法设计和构建终端计算机安全功能，并避免设计模块之间出现不必要的交互；

b) 标识终端计算机安全功能模块，并应描述每一个终端计算机安全功能模块的目的、接口、参数和影响；

c) 描述终端计算机安全功能设计是如何使独立的模块间避免不必要的交互作用。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3.3.5 实现表示设计

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.3 e) 的要求，实现终端计算机第一级的实现表示设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 应无歧义地为选定的终端计算机安全功能子集定义一个详细级别的终端计算机安全功能实现表示，并且实现表示应当是内在一致的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3.3.6 对应性设计

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.3 f) 的要求，实现终端计算机第一级的对应性设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 应在所提供的终端计算机安全功能表示的所有相邻对之间提供其对应性分析，对每个相邻对，应当阐明较为抽象的终端计算机安全功能表示的所有相关安全功能在较不抽象的终端计算机安全功能表示中得到正确而完备地细化。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3.4 文档要求

5.2.3.4.1 管理员指南

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.4 的要求，实现终端计算机第一级的管理员指南。

——测试评价方法：

评估者应审查开发者是否提供了供系统管理员使用的管理员指南，并且此管理员指南是否包括如下内容：

a） 终端计算机可以使用的管理功能和接口；

b） 怎样安全地管理终端计算机；

c） 在安全处理环境中应进行控制的功能和权限；

d） 所有对与终端计算机的安全操作有关的用户行为的假设；

e） 所有受管理员控制的安全参数，如果可能，应指明安全值；

f） 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g） 所有与系统管理员有关的 IT 环境的安全要求。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3.4.2 用户指南

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.4 的要求，实现终端计算机第一级的用户指南。

——测试评价方法：

评估者应审查开发者是否提供了供系统用户使用的用户指南，并且此用户指南是否包括如下内容：

a） 终端计算机的非管理用户可使用的安全功能和接口；

b） 终端计算机提供给用户的安全功能和接口的用法；

c） 用户可获取但应受安全处理环境控制的所有功能和权限；

d） 终端计算机安全操作中用户所应承担的职责；

e） 与用户有关的 IT 环境的所有安全要求。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3.5 生存周期支持

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.5 的要求，实现终端计算机第一级的生存周期支持。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a） 开发者应建立用于开发和维护终端计算机的生存周期模型，对终端计算机开发和维护提供必要的控制，并以文档形式描述用于开发和维护终端计算机的模型。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3.6 测试

5.2.3.6.1 功能测试

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.6 a） 的要求，实现终端计算机第一级的功能测试。

——测试评价方法：

a） 评价开发者提供的测试文档，是否包括测试计划、测试规程、预期的测试结果和实际测试结果；

b） 评价测试计划是否标识了要测试的安全功能，是否描述了测试的目标；

c） 评价测试规程是否标识了要执行的测试，是否描述了每个安全功能的测试概况（这些概况包括对其他测试结果的顺序依赖性）；

d) 评价期望的测试结果是否表明测试成功后的预期输出；

e) 评价实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.2.3.6.2 独立性测试

——测试评价内容：

按 GB/T 20271—2006 中 6.1.5.6 b) 的要求，实现终端计算机第一级的独立性测试。

——测试评价方法：

a) 开发者提供的测试文档，应表明安全功能是按规定运作的；

b) 开发者应提供与测试相适应的终端计算机。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3 第二级

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

——测试评价内容：

见 4.2.1.1.1 的内容。

——对开发者的要求：

开发者应提供文档，说明终端计算机的设备提供哪些基本的运行支持措施，提供哪些必要的容错和故障恢复能力。

——测试评价方法：

a) 按照开发者提供的文档，逐项验证所提供的运行支持措施是否有效，能否支持终端计算机的基本运行；

b) 按照开发者提供的文档，模拟出现一些故障事件(如：掉电、硬件故障等)，验证终端计算机的容错和故障恢复能力是否有效。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.1.1.2 设备防盗

——测试评价内容：

见 4.2.1.1.2 的内容。

——对开发者的要求：

开发者应提供文档，说明终端计算机的设备具有哪些无法除去的标记。

——测试评价方法：

a) 按照开发者提供的文档，尝试使用各种方式除去设备中的标记，检测能否除去；

b) 检测终端计算机的主机是否具有机箱封装保护，能否防止部件损害或被盗。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.1.2 操作系统

——测试评价内容：

见 4.2.1.2 的内容。

——对开发者的要求：

开发者应提供第三方权威机构对该操作系统的检测报告，或者提供文档对 GB/T 20272—2006 中4.2.1 的各个项目进行说明。

——测试评价方法：

a) 如果提供了第三方权威机构对该操作系统的检测报告，则查验报告，查看报告中对应项目检测结果是否符合；

b) 如果未能提供第三方权威机构对该操作系统的检测报告，则按照 GB/T 20272—2006 中4.2.1 的要求对操作系统的相关项目进行检测。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.1.3 安全支撑系统

5.3.1.3.1 密码支持

——测试评价内容：

见 4.2.1.3.1 的内容。

——对开发者的要求：

开发者应提供文档和相关证书，说明所使用的密码算法、相关的密码操作以及相关的密钥管理措施，并证明所使用的密码算法已经通过国家密码管理部门的批准。

——测试评价方法：

a) 按照开发者提供的文档和相关证书，检测所使用的密码算法是否由硬件或者软件支撑实现，是否已经通过国家密码管理部门的批准；

b) 根据开发者提供的文档，检验系统是否建立可信存储根密钥；

c) 按照开发者提供的文档，检测所有密钥是否受可信存储根保护；

d) 按照开发者提供的文档，检测可信存储根本身是否由硬件密码模块保护。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.1.3.2 运行时防护

——测试评价内容：

见 4.2.1.3.2 的内容。

——对开发者的要求：

开发者应提供文档，说明终端计算机具有哪些运行时防护功能。

——测试评价方法：

a) 在系统和外来介质中植入一个测试用的恶意代码，并运行恶意代码；

b) 对文件系统、内存和使用时的外来介质进行扫描，检测系统能否清除或隔离恶意代码；

c) 检测系统能否对恶意代码特征库进行及时更新；

d) IP 过滤：根据源地址、目的地址设置多条允许通过的过滤规则，模拟相应的网络通讯，检测能否正常通讯；根据源地址、目的地址设置多条拒绝通过的过滤规则，模拟相应的网络通讯，检测能否拒绝相应的网络数据包。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.1.3.3 系统身份标识与鉴别

——测试评价内容：

见 4.2.1.3.3 的内容。

——对开发者的要求：

开发者应提供文档，详细说明系统标识产生的过程以及终端计算机身份的鉴别过程。

——测试评价方法：

a) 根据开发者提供的文档，验证系统身份的标识的产生过程，检验系统身份标识是否是由唯一绑定的硬件密码模块或受保护的软件模块产生的密钥；

b) 根据开发者提供的文档模拟终端计算机的身份鉴别过程，验证请求方是否通过一定的认证协议完成身份鉴别过程。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.1.3.4 数据保密性保护

5.3.1.3.4.1 数据存储保密性

——测试评价内容：

见 4.2.1.3.4 a）的内容。

——对开发者的要求：

开发者应提供文档，说明如何对存储在终端计算机内的重要用户数据进行保密性保护。

——测试评价方法：

a) 根据开发者提供的文档，对测试数据进行加密，并以密钥的合法持有者身份进行解密，检测能否解密成功；

b) 以其余任何用户身份登录，检测是否无法获得该数据。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.1.3.4.2 数据传输保密性

——测试评价内容：

见 4.2.1.3.4 b）的内容。

——对开发者的要求：

开发者应提供文档，说明如何对在不同 SSF 之间基于网络传输的重要数据，进行保密性保护。

——测试评价方法：

a) 利用协议分析仪截取网络传输的用户数据，检测基于网络传输的重要数据是否按照开发者的设计进行保密性保护。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.1.3.5 安全审计

——测试评价内容：

见 4.2.1.3.5 的内容。

——对开发者的要求：

开发者应提供文档，说明安全支撑系统对哪些操作生成审计记录。

——测试评价方法：

a) 查看系统的审计记录信息，检测是否有密码支持、系统身份标识与鉴别、数据保密性保护等安全功能相关操作的审计记录；

b) 检测审计功能是否支持审计日志；

c) 对于绑定于终端计算机的硬件密码模块，检测是否提供给上层应用软件查询审计情况的接口；

d) 检测审计记录是否包括：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；

e) 检测审计功能是否为授权用户提供基本审计查阅；以未授权用户身份，尝试查阅审计信息，检测系统是否拒绝未授权访问；

f) 检测审计功能是否支持根据客体身份、用户身份、主体身份、主机身份、事件类型等属性进行审计事件选择。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.1.3.6 备份与故障恢复

——测试评价内容：

见 4.2.1.3.6 的内容。

——对开发者的要求：

开发者应提供文档，说明备份与故障恢复的方法。

——测试评价方法：

a) 以授权用户身份有选择地备份重要数据，对系统中已备份的用户数据进行修改，然后进行恢复，检测能否按照备份信息有效恢复；

b) 设置对系统数据进行定时备份，对已备份的系统数据进行修改，然后进行恢复，检测能否按照备份信息有效恢复。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.2 SSOTC 自身安全保护

5.3.2.1 安全支撑系统的自身安全保护

——测试评价内容：

见 4.2.2.1 的内容。

——对开发者的要求：

开发者应提供文档，说明可信存储根是否设置在硬件密码模块内，所采用的硬件密码模块和软件密码模块是否符合国家相关密码管理要求，如果是，则提供相应的认证证书；说明采取何种方式对安全支撑系统的使用用户进行鉴别。

——测试评价方法：

a) 按照开发者提供的文档，检测可信存储根是否设置在硬件密码模块内；

b) 按照开发者提供的文档和相关证书，检测所使用的硬件密码模块和软件密码模块是否符合国家相关密码管理要求；

c) 以各种方法和工具，尝试读取、修改可信存储根，检测能否尝试成功；

d) 尝试以授权用户和非授权用户去使用硬件密码模块，检验是否需要进行身份鉴别。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.2.2 操作系统的自身安全保护

——测试评价内容：

见 4.2.2.2 的内容。

——测试评价方法：

a) 如果提供了第三方权威机构对该操作系统的检测报告，则查验报告，查看报告中对应项目检测结果是否符合；

b) 如果未能提供第三方权威机构对该操作系统的检测报告，则按照 GB/T 20272—2006 中4.2.2 的要求对操作系统的相关项目进行检测。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3 SSOTC 设计和实现

5.3.3.1 配置管理

5.3.3.1.1 配置管理能力

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.1 a)的要求，实现终端计算机第二级的配置管理**能力设计**。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 开发者所使用的版本号与所应表示的终端计算机样本应完全对应，没有歧义。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.1.2 配置管理范围

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.1 b)的要求，实现终端计算机第二级的配置管理范围设计。

——测试评价方法：

终端计算机配置管理范围，要求将终端计算机的实现表示、设计文档、测试文档、用户文档、安全管理员文档、配置管理文档等置于配置管理之下，从而确保它们的修改是在一个正确授权的可控方式下进行的。为此要求：

a) 开发者所提供的配置管理文档应展示配置管理系统至少能跟踪上述配置管理之下的内容；

b) 文档应描述配置管理系统是如何跟踪这些配置项的；

c) 文档还应提供足够的信息表明达到所有要求。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.2 分发和操作

5.3.3.2.1 分发

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.2 a) 的要求，实现终端计算机第二级的分发。

——测试评价方法：

a) 评估者应审查开发者是否按分发过程的要求，编制分发文档；

b) 评估者应审查分发文档，是否描述给用户分发终端计算机时，用以维护安全所必须的所有过程。

c) 评估者应审查是否按该过程进行分发。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.2.2 操作

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.2 b) 的要求，实现终端计算机第二级的操作。

——测试评价方法：

a) 评估者应审查操作文档，是否说明了终端计算机的安装、生成、启动和使用的过程。用户能够通过此文档了解安装、生成、启动和使用过程。

b） 评估者应审查操作文档，是否说明了日志生成的要求和过程。用户能够通过此文档进行生成日志。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.3 开发

5.3.3.3.1 功能设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.3 a）的要求，实现终端计算机第二级的功能设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a） 功能设计应当使用非形式化风格来描述终端计算机安全功能与其外部接口；

b） 功能设计应当是内在一致的；

c） 功能设计应当描述使用所有外部终端计算机安全功能接口的目的与方法，适当的时候，要提供结果影响例外情况和错误信息的细节；

d） 开发者应完备地表示终端计算机安全功能的基本原理。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.3.2 安全策略模型

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.3 b）的要求，实现终端计算机第二级的安全策略模型设计。

——测试评价方法：

评估者应审查开发者所提供的文档中，安全策略模型的相关内容，是否满足如下要求：

a） SSP 模型应是非形式化的，并描述所有可以模型化的 SSP 策略的规则与特征；

b） SSP 模型应包括一个基本原理，阐明该模型与所有可模型化的 SSP 策略是一致的、完备的；

c） SSP 模型和功能设计之间的对应性阐明应说明功能设计中的安全功能与 SSP 模型是一致的、完备的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.3.3 高层设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.3 c）的要求，实现终端计算机第二级的高层设计。

——测试评价方法：

评估者应审查开发者所提供的高层设计文档是否满足如下要求：

a） 以子系统的观点、以非形式化的方法来一致性地描述终端计算机的体系结构；

b） 描述每一个子系统所提供的安全功能及其相互关系；

c） 标识安全功能要求的任何基础性的硬件、固件和/或软件，并且通过这些硬件、固件和/或软件所实现的保护机制，来提供安全功能功能；

d） 标识安全功能子系统的所有接口，并标明安全功能子系统的哪些接口是外部可见的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.3.4 低层设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.3 d) 的要求，实现终端计算机第二级的低层设计。

——测试评价方法：

评估者应审查开发者所提供的低层设计文档是否满足如下要求：

a) 低层设计的表示应是非形式化的，内在一致的，并以模块术语描述；

b) 描述每一个模块的目的；

c) 以所提供的安全功能和对其他模块的依赖性术语定义模块间的相互关系；

d) 描述如何提供每一个安全策略功能的实施；

e) 标识终端计算机安全功能模块的所有接口，标识终端计算机安全功能模块的哪些接口是外部可见的，以及描述终端计算机安全功能模块所有接口的目的与方法，必要时，应提供影响、例外情况和错误信息的细节；

f) 描述如何将终端计算机分离成安全策略实施模块和其他模块。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.3.5 内部结构设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.3 e) 的要求，实现终端计算机第二级的内部结构设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 应以模块化方法设计和构建终端计算机安全功能，并避免设计模块之间出现不必要的交互；

b) 标识终端计算机安全功能模块，并应描述每一个终端计算机安全功能模块的目的、接口、参数和影响；

c) 描述终端计算机安全功能设计是如何使独立的模块间避免不必要的交互作用；

d) 在设计和构建安全功能时，应使安全功能局部的复杂度最小化，以加强访问控制策略；

e) 标识安全功能模块，并应指明安全功能的哪些部分是加强安全策略的；

f) 描述分层结构，并说明如何使交互作用最小化；

g) 描述加安全策略的安全功能部分是如何被构建的，从而使其复杂性降低。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.3.6 实现表示

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.3 f) 的要求，实现终端计算机第二级的实现表示设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 应无歧义地为选定的终端计算机安全功能子集定义一个详细级别的终端计算机安全功能实现表示，并且实现表示应当是内在一致的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.3.7 对应性设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.3 g) 的要求，实现终端计算机第二级的对应性设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 应在所提供的终端计算机安全功能表示的所有相邻对之间提供其对应性分析，对每个相邻对，

应当阐明较为抽象的终端计算机安全功能表示的所有相关安全功能在较不抽象的终端计算机安全功能表示中得到正确而完备地细化。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.4 文档要求

5.3.3.4.1 管理员指南

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.4 的要求，实现终端计算机第二级的管理员文档。

——测试评价方法：

评估者应审查开发者是否提供了供系统管理员使用的管理员指南，并且此管理员指南是否包括如下内容：

a) 终端计算机可以使用的管理功能和接口；

b) 怎样安全地管理终端计算机；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与终端计算机的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，应指明安全值；

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g) 所有与系统管理员有关的 IT 环境的安全要求。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.4.2 用户指南

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.4 的要求，实现终端计算机第二级的用户指南。

——测试评价方法：

评估者应审查开发者是否提供了供系统用户使用的用户指南，并且此用户指南是否包括如下内容：

a) 终端计算机的非管理用户可使用的安全功能和接口；

b) 终端计算机提供给用户的安全功能和接口的用法；

c) 用户可获取但应受安全处理环境控制的所有功能和权限；

d) 终端计算机安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.5 生存周期支持

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.5 的要求，实现终端计算机第二级的生存周期支持。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 开发人员的安全管理：开发人员的安全规章制度，开发人员的安全教育培训制度和记录；

b) 开发环境的安全管理：开发地点的出入口控制制度和记录，开发环境的温湿度要求和记录，开发环境的防火防盗措施和国家有关部门的许可文件，开发环境中所使用安全产品应采用符合国家有关规定的产品并提供相应证明材料；

c) 开发设备的安全管理：开发设备的安全管理制度，包括开发主机使用管理和记录，设备的购置、修理、处置的制度和记录，上网管理，计算机病毒管理和记录等；

d) 开发过程和成果的安全管理：对产品代码、文档、样机进行受控管理的制度和记录，若代码和文档进行加密保护应采用符合国家有关规定的产品并提供相应证明材料；

e) 开发安全文件中所提供的安全措施的证据，应能证明安全措施对维护终端计算机的安全性提供了充分的保护；

f) 开发者应建立用于开发和维护终端计算机的生存周期模型，对终端计算机开发和维护提供必要的控制，并以文档形式描述用于开发和维护终端计算机的模型；

g) 开发者应标识用于开发终端计算机的工具，并且所有用于实现的开发工具都应有明确定义。开发者应文档化已选择的依赖实现的开发工具的选项，开发工具文档应明确定义实现中每个语句的含义，以及明确定义所有基于实现的选项的含义。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.6 测试

5.3.3.6.1 测试范围

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.6 a)的要求，确定终端计算机第二级的测试范围。

——测试评价方法：

a) 评估者应审查开发者提供的测试覆盖分析结果，是否表明了测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的；

b) 评价测试文档中已标识的测试是否包括了安全功能设计描述中所有安全功能的测试，是否都经过了完整性测试；

c) 评估者应审查测试文档，是否覆盖了在功能设计描述中的所有安全功能；

d) 开发者所提供的范围分析应表明测试文档所标识的测试与功能设计所描述的安全功能之间的对应性；

e) 测试范围的分析应阐明功能设计所描述的安全功能和测试文档所标识的测试之间的对应性是完备的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.6.2 测试深度

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.6 b)的要求，确定终端计算机第二级的测试深度。

——测试评价方法：

a) 评价开发者提供的测试深度分析，是否说明了测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计是一致的。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.6.3 功能测试

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.6 c)的要求，实现终端计算机第二级的功能测试。

——测试评价方法：

a) 评价开发者提供的测试文档，是否包括测试计划、测试规程、预期的测试结果和实际测试结果；

b) 评价测试计划是否标识了要测试的安全功能，是否描述了测试的目标；

c) 评价测试规程是否标识了要执行的测试，是否描述了每个安全功能的测试概况(这些概况包括对其他测试结果的顺序依赖性)；

d) 评价期望的测试结果是否表明测试成功后的预期输出；

e) 评价实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.3.6.4 独立性测试

——测试评价内容：

应按 GB/T 20271—2006 中 6.2.5.6 d)的要求，实现终端计算机第二级的独立性测试。

——测试评价方法：

a) 开发者提供的测试文档，应表明安全功能是按规定运作的；

b) 开发者应提供与测试相适应的终端计算机。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4 第三级

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

——测试评价内容：

见 4.3.1.1.1 的内容。

——对开发者的要求：

开发者应提供文档，说明终端计算机的设备提供哪些基本的运行支持措施，提供哪些必要的容错和故障恢复能力，能否满足基本安全可用的要求。

——测试评价方法：

a) 按照开发者提供的文档，逐项验证所提供的运行支持措施是否有效，能否支持终端计算机的基本运行；

b) 按照开发者提供的文档，模拟出现一些故障事件(如：掉电、硬件故障等)，验证终端计算机的容错和故障恢复能力是否有效；

c) 检测主机、外部设备、网络连接部件及其他辅助部件，能否满足基本安全可用的要求。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.1.1.2 设备防盗

——测试评价内容：

见 4.3.1.1.2 的内容。

——对开发者的要求：

开发者应提供文档，说明终端计算机的设备具有哪些无法除去的标记。

——测试评价方法：

a) 按照开发者提供的文档，尝试使用各种方式除去设备中的标记，检测能否除去；

b) 检测终端计算机的主机是否具有机箱封装保护，能否防止部件损害或被盗。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.1.2 操作系统

——测试评价内容：

见 4.3.1.2 的内容。

——对开发者的要求：

开发者应提供第三方权威机构对该操作系统的检测报告，或者提供文档对 GB/T 20272—2006 中4.3.1的各个项目进行说明。

——测试评价方法：

a) 如果提供了第三方权威机构对该操作系统的检测报告，则查验报告，查看报告中对应项目检测结果是否符合；

b) 如果未能提供第三方权威机构对该操作系统的检测报告，则按照 GB/T 20272—2006 中4.3.1的要求对操作系统的相关项目进行检测。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.1.3 安全支撑系统

5.4.1.3.1 密码支持

——测试评价内容：

见 4.3.1.3.1 的内容。

——对开发者的要求：

开发者应提供文档和相关证书，说明所使用的密码算法、相关的密码操作以及相关的密钥管理措施，并证明所使用的密码算法已经通过国家密码管理部门的批准。

——测试评价方法：

a) 按照开发者提供的文档和相关证书，检测所使用的密码算法，是否已经通过国家密码管理部门的批准并由密码硬件实现；

b) 按照开发者提供的文档，检验系统是否建立可信存储根密钥；

c) 按照开发者提供的文档，检测所有密钥是否受可信存储根保护；

d) 按照开发者提供的文档，检测所有密钥是否受可信存储根保护，可信存储根本身是否由可信密码模块(TCM)保护；

e) 按照密码算法要求进行密码操作，包括：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；

f) 拔除密码硬件，进行密钥生成、数字签名与验证等关键密码操作，检验以上操作是否基于密码硬件支持。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.1.3.2 运行时防护

——测试评价内容：

见 4.3.1.3.2 的内容。

——对开发者的要求：

开发者应提供文档，说明终端计算机具有哪些运行时防护功能。

——测试评价方法：

a) 在系统和外来介质中植入一个测试用的恶意代码，并运行恶意代码；

b) 对文件系统、内存和使用时的外来介质进行扫描，检测系统能否清除或隔离恶意代码；

c) 检测系统能否对恶意代码特征库进行及时更新；

d) IP过滤：根据源地址、目的地址设置多条允许通过的过滤规则，模拟相应的网络通讯，检测能否正常通讯；根据源地址、目的地址设置多条拒绝通过的过滤规则，模拟相应的网络通讯，检测能否拒绝相应的网络数据包；

e) 应用程序监控：对某个应用程序设置允许访问网络规则，使用这个应用程序访问网络，检测能否正常访问；对某个应用程序设置拒绝访问网络规则，使用这个应用程序访问网络，检测能否拒绝访问。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.1.3.3 系统安全性检测分析

——测试评价内容：

见4.3.1.3.3的内容。

——对开发者的要求：

开发者应提供文档，按GB/T 20271—2006中6.4.2.2的要求，说明终端计算机是否经过操作系统安全性检测分析和硬件系统安全性检测分析，以设计和实现终端计算机第四级的系统安全性检测分析功能，并且提供相应的检测分析报告。

——测试评价方法：

a) 按照开发者提供的文档，检测终端计算机是否经过操作系统安全性检测分析和硬件系统安全性检测分析；

b) 根据相关的检测报告，判断检测方法是否科学，检测结果是否可信；

c) 对存在的问题，检测改进措施是否有效。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.1.3.4 系统身份标识与鉴别

——测试评价内容：

见4.3.1.3.4的内容。

——对开发者的要求：

开发者应提供文档，详细说明系统标识产生的过程以及终端计算机身份的鉴别过程。

——测试评价方法：

a) 根据开发者提供的文档，验证系统身份的标识的产生过程，检验系统身份标识是否是由唯一绑定的可信密码模块(TCM)产生的密钥，该身份密钥即为可信报告根；

b) 根据开发者提供的文档，验证身份标识的可信性是否通过国家批准的权威机构颁发证书来实现；

c) 根据开发者提供的文档，验证系统身份标识的隐秘性；

d) 尝试对终端计算机身份标识信息进行操作，检验身份标识是否能够进行管理和维护；

e) 分别使用经过授权和未经授权的管理员对系统身份标识进行操作，检验系统身份标识是否能够确保其不被非授权地访问、修改或删除；

f) 根据开发者提供的文档模拟终端计算机的身份鉴别过程，验证请求方是否提供系统的身份证书和/或证书信任链验证路径，并通过一定的认证协议完成身份鉴别过程。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.1.3.5 数据保密性保护

5.3.1.3.5.1 数据存储保密性

——测试评价内容：

见 4.3.1.3.5 a）的内容。

——对开发者的要求：

开发者应提供文档，说明如何对存储在终端计算机内的重要用户数据进行保密性保护，描述数据加密和数据绑定的方法和步骤。

——测试评价方法：

a） 根据开发者提供的文档，对测试数据进行加密，并以密钥的合法持有者身份进行解密，检测能否解密成功；

b） 以其余任何用户身份登录，检测是否无法获得该数据；

c） 根据开发者提供的文档，在特定终端计算机中基于可信存储根对测试数据进行加密，并且由密钥的合法持有者在特定终端计算机中解密，检测能否解密成功；

d） 由密钥的合法持有者在其他终端计算机中解密，检测能否解密成功；

e） 以其余任何用户身份登录特定终端计算机，解密测试数据，检测是否无法获得该数据。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.3.1.3.5.2 数据传输保密性

——测试评价内容：

见 4.3.1.3.5 b）的内容。

——对开发者的要求：

开发者应提供文档，说明如何对在不同 SSF 之间基于网络传输的重要数据，进行保密性保护。

——测试评价方法：

a） 利用协议分析仪截取网络传输的用户数据，检测基于网络传输的重要数据是否按照开发者的设计进行保密性保护。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.1.3.6 安全审计

——测试评价内容：

见 4.3.1.3.6 的内容。

——对开发者的要求：

开发者应提供文档，说明安全支撑系统中生成、维护及保护审计数据过程，以及具备哪些保护措施。

——测试评价方法：

a） 查看系统的审计记录信息，检测是否有密码支持、系统身份标识与鉴别、数据保密性保护等安全功能相关操作的审计记录；

b） 检测审计功能是否支持审计日志；

c） 对于内置于终端计算机的可信密码模块，检测能否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，并查看审计记录；检测是否提供给上层应用软件查询审计情况的接口；检测能否存储审计记录；

d） 检测审计记录是否包括：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；

e) 检测审计功能是否支持潜在侵害分析;检测系统能否用一系列规则去监控审计事件,并根据这些规则指出系统的潜在侵害;

f) 检测审计功能是否为授权用户提供基本审计查阅;检测系统是否提供审计查阅工具对审计数据进行搜索、分类、排序;以未授权用户身份,尝试查阅审计信息,检测系统是否拒绝未授权访问;

g) 检测审计功能是否支持根据客体身份、用户身份、主体身份、主机身份、事件类型等属性进行审计事件选择;

h) 根据开发者提供的文档,检测审计数据是否受到安全保护,尝试以未授权用户进行访问、修改和破坏审计信息,检测系统能否拒绝未授权访问。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.1.3.7 备份与故障恢复

——测试评价内容:

见 4.3.1.3.7 的内容。

——对开发者的要求:

开发者应提供文档,说明对用户数据和系统,如何在备份、存储和恢复过程中进行安全保护,以及具备哪些备份保护措施。

——测试评价方法:

a) 以授权用户身份有选择地备份重要数据,对系统中已备份的用户数据进行修改,然后进行恢复,检测能否按照备份信息有效恢复;

b) 设置对系统数据进行定时备份,对已备份的系统数据进行修改,然后进行恢复,检测能否按照备份信息有效恢复;

c) 根据开发者提供的文档,检测数据在备份、存储和恢复过程中是否具有安全保护措施,是否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,用户操作系统是否不可访问系统备份数据。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.1.3.8 I/O 接口配置

——测试评价内容:

见 4.3.1.3.8 的内容。

——测试评价方法:

a) 以用户身份,在 BIOS 和操作系统中,分别启用 USB、网卡、硬盘,检测能否正常使用;

b) 以用户身份,在 BIOS 和操作系统中,分别禁用 USB、网卡、硬盘,检测能否使用。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.2 SSOTC 自身安全保护

5.4.2.1 安全支撑系统的自身安全保护

——测试评价内容:

见 4.3.2.1 的内容。

——对开发者的要求:

开发者应提供文档,说明可信存储根是否设置在可信密码模块内,所采用的可信密码模块是否符合国家密码管理部门的相关规范和管理要求;说明可信报告根是否设置在可信密码模块内,可信报告根所

对应的公钥证书由哪家机构发行和管理;说明采取何种方式对安全支撑系统的使用用户进行鉴别。

——测试评价方法:

a) 按照开发者提供的文档,检测可信存储根和可信报告根是否设置在可信密码模块内;

b) 按照开发者提供的文档和相关证书,检测所使用的密码模块是否符合国家密码管理部门的相关规范和管理要求;

c) 按照开发者提供的文档,并查看可信报告根的公钥证书及其发行机构的相关证书,检验是否由国家批准的权威机构发行和管理;

d) 尝试以授权用户和非授权用户去使用可信密码模块,检验是否需要进行身份鉴别。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.2.2 操作系统的自身安全保护

——测试评价内容:

见 4.3.2.2 的内容。

——对开发者的要求:

开发者应提供第三方权威机构对该操作系统的检测报告,或者提供文档对 GB/T 20272—2006 中 4.3.2 的各个项目进行说明。

——测试评价方法:

a) 如果提供了第三方权威机构对该操作系统的检测报告,则查验报告,查看报告中对应项目检测结果是否符合;

b) 如果未能提供第三方权威机构对该操作系统的检测报告,则按照 GB/T 20272—2006 中4.3.2 的要求对操作系统的相关项目进行检测。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3 SSOTC 设计和实现

5.4.3.1 配置管理

5.4.3.1.1 配置管理能力

——测试评价内容:

应按 GB/T 20271—2006 中 6.3.5.1 a) 的要求,实现终端计算机第三级的配置管理能力设计。

——测试评价方法:

评估者应审查开发者所提供的信息是否满足如下要求:

a) 开发者所使用的版本号与所应表示的终端计算机样本应完全对应,没有歧义。

b) 配置管理系统应对所有的配置项作出唯一的标识。

c) 配置管理计划中,应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。

d) 配置管理文档应提供所有的配置项得到有效地维护的证据。

e) 配置管理系统应确保对配置项只进行授权修改。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.1.2 配置管理自动化

——测试评价内容:

应按 GB/T 20271—2006 中 6.3.5.1 b) 的要求,实现终端计算机第三级的配置管理自动化设计。

——测试评价方法:

评估者应审查开发者所提供的信息是否满足如下要求：

a) 配置管理系统应通过自动方式来确保终端计算机的实现表示只能进行已授权的变化，并能提供自动方式来支持终端计算机的生成；

b) 配置管理计划应描述配置管理系统中所使用的自动工具，并说明如何使用这些工具。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.1.3 配置管理范围

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.1 c) d) 的要求，实现终端计算机第三级的配置管理范围设计。

——测试评价方法：

a) 终端计算机配置管理范围，要求将终端计算机的实现表示、设计文档、测试文档、用户文档、安全管理员文档、配置管理文档等置于配置管理之下，从而确保它们的修改是在一个正确授权的可控方式下进行的。为此要求：

1) 开发者所提供的配置管理文档应展示配置管理系统至少能跟踪上述配置管理之下的内容；

2) 文档应描述配置管理系统是如何跟踪这些配置项的；

3) 文档还应提供足够的信息表明达到所有要求。

b) 配置管理系统应对安全缺陷进行跟踪。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.2 分发和操作

5.4.3.2.1 分发

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.2 a) 的要求，实现终端计算机第三级的分发。

——测试评价方法：

a) 评估者应审查开发者是否按分发过程的要求，编制分发文档；

b) 评估者应审查分发文档，是否描述给用户分发终端计算机时，用以维护安全所必须的所有过程；

c) 评估者应审查是否按该过程进行分发；

d) 评估者应审查分发文档，是否描述检测修改的方法和技术，是否描述开发者的主拷贝与用户收到的版本之间的差异；

e) 评估者应审查分发文档，是否描述用来检测试图伪装成开发者向用户发送产品的方法。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.2.2 操作

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.2 b) 的要求，实现终端计算机第三级的操作。

——测试评价方法：

a) 评估者应审查操作文档，是否说明了终端计算机的安装、生成、启动和使用的过程。用户能够通过此文档了解安装、生成、启动和使用过程。

b) 评估者应审查操作文档，是否说明了日志生成的要求。用户能够通过此文档进行生成日志。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.3 开发

5.4.3.3.1 功能设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.3 a）的要求，实现终端计算机第三级的功能设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a） 功能设计应当使用非形式化风格来描述终端计算机安全功能与其外部接口；

b） 功能设计应当是内在一致的；

c） 功能设计应当描述使用所有外部终端计算机安全功能接口的目的与方法，适当的时候，要提供结果影响例外情况和错误信息的细节；

d） 开发者应完备地表示终端计算机安全功能的基本原理。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.3.2 安全策略模型

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.3 b）的要求，实现终端计算机第三级的安全策略模型设计。

——测试评价方法：

评估者应审查开发者所提供的文档中，安全策略模型的相关内容，是否满足如下要求：

a） SSP 模型应是非形式化的，并描述所有可以模型化的 SSP 策略的规则与特征；

b） SSP 模型应包括一个基本原理，阐明该模型与所有可模型化的 SSP 策略是一致的、完备的；

c） SSP 模型和功能设计之间的对应性阐明应说明功能设计中的安全功能与 SSP 模型是一致的、完备的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.3.3 高层设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.3 c）的要求，实现终端计算机第三级的高层设计。

——测试评价方法：

评估者应审查开发者所提供的高层设计文档是否满足如下要求：

a） 以子系统的观点、以非形式化的方法来一致性地描述终端计算机的体系结构；

b） 描述每一个子系统所提供的安全功能及其相互关系；

c） 标识安全功能要求的任何基础性的硬件、固件和/或软件，并且通过这些硬件、固件和/或软件所实现的保护机制，来提供安全功能功能；

d） 标识安全功能子系统的所有接口，并标明安全功能子系统的哪些接口是外部可见的；

e） 高层设计文档应当描述安全功能子系统所有接口的使用目的与方法，并提供例外情况和错误信息的细节；

f） 高层设计文档应当描述如何将终端计算机分离成安全策略加强单元和其他子系统。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.3.4 低层设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.3 d) 的要求，实现终端计算机第三级的低层设计。

——测试评价方法：

评估者应审查开发者所提供的低层设计文档是否满足如下要求：

a) 低层设计的表示应是非形式化的，内在一致的，并以模块术语描述；

b) 描述每一个模块的目的；

c) 以所提供的安全功能和对其他模块的依赖性术语定义模块间的相互关系；

d) 描述如何提供每一个安全策略功能的实施；

e) 标识终端计算机安全功能模块的所有接口，标识终端计算机安全功能模块的哪些接口是外部可见的，以及描述终端计算机安全功能模块所有接口的目的与方法，必要时，应提供影响、例外情况和错误信息的细节；

f) 描述如何将终端计算机分离成安全策略实施模块和其他模块。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.3.5 内部结构设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.3 e) 的要求，实现终端计算机第三级的内部结构设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 应以模块化方法设计和构建终端计算机安全功能，并避免设计模块之间出现不必要的交互；

b) 标识终端计算机安全功能模块，并应描述每一个终端计算机安全功能模块的目的、接口、参数和影响；

c) 描述终端计算机安全功能设计是如何使独立的模块间避免不必要的交互作用；

d) 在设计和构建安全功能时，应使安全功能局部的复杂度最小化，以加强访问控制策略；

e) 标识安全功能模块，并应指明安全功能的哪些部分是加强安全策略的；

f) 描述分层结构，并说明如何使交互作用最小化；

g) 描述加安全策略的安全功能部分是如何被构建的，从而使其复杂性降低。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.3.6 实现表示

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.3 f) 的要求，实现终端计算机第三级的实现表示设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 应无歧义地为全部终端计算机安全功能，定义一个详细级别的终端计算机安全功能实现表示，并且实现表示应当是内在一致的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.3.7 对应性设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.3 g) 的要求，实现终端计算机第三级的对应性设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 应在所提供的终端计算机安全功能表示的所有相邻对之间提供其对应性分析，对每个相邻对，

应当阐明较为抽象的终端计算机安全功能表示的所有相关安全功能在较不抽象的终端计算机安全功能表示中得到正确而完备地细化。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.4 文档要求

5.4.3.4.1 管理员指南

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.4 的要求，实现终端计算机第三级的管理员指南。

——测试评价方法：

评估者应审查开发者是否提供了供系统管理员使用的管理员指南，并且此管理员指南是否包括如下内容：

a) 终端计算机可以使用的管理功能和接口；
b) 怎样安全地管理终端计算机；
c) 在安全处理环境中应进行控制的功能和权限；
d) 所有对与终端计算机的安全操作有关的用户行为的假设；
e) 所有受管理员控制的安全参数，如果可能，应指明安全值；
f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；
g) 所有与系统管理员有关的 IT 环境的安全要求。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.4.2 用户指南

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.4 的要求，实现终端计算机第三级的用户指南。

——测试评价方法：

评估者应审查开发者是否提供了供系统用户使用的用户指南，并且此用户指南是否包括如下内容：

a) 终端计算机的非管理用户可使用的安全功能和接口；
b) 终端计算机提供给用户的安全功能和接口的用法；
c) 用户可获取但应受安全处理环境控制的所有功能和权限；
d) 终端计算机安全操作中用户所应承担的职责；
e) 与用户有关的 IT 环境的所有安全要求。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.5 生存周期支持

5.4.3.5.1 开发安全

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.5 a) 的要求，实现终端计算机第三级的开发安全。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 开发人员的安全管理：开发人员的安全规章制度，开发人员的安全教育培训制度和记录；
b) 开发环境的安全管理：开发地点的出入口控制制度和记录，开发环境的温室度要求和记录，开发环境的防火防盗措施和国家有关部门的许可文件，开发环境中所使用安全产品必须采用符

合国家有关规定的产品并提供相应证明材料；

c) 开发设备的安全管理：开发设备的安全管理制度，包括开发主机使用管理和记录，设备的购置、修理、处置的制度和记录，上网管理，计算机病毒管理和记录等；

d) 开发过程和成果的安全管理：对产品代码、文档、样机进行受控管理的制度和记录，若代码和文档进行加密保护必须采用符合国家有关规定的产品并提供相应证明材料。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.5.2 缺陷纠正

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.5 b) 的要求，实现终端计算机第三级的缺陷纠正。

——测试评价方法：

评估者应审查开发者所提供的生存周期定义文档中是否完全符合以下要求：

a) 描述用以跟踪所有终端计算机版本里已被报告的安全缺陷的过程；

b) 描述所提供的每个安全缺陷的性质和效果，以及缺陷纠正的情况；

c) 标识每个安全缺陷所采取的纠正措施；

d) 描述为终端计算机用户的纠正行为所提供的信息，纠正和指导的方法。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.5.3 生存周期定义

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.5 c) 的要求，实现终端计算机第三级的生存周期定义。

——测试评价方法：

评估者应审查开发者所提供的生存周期定义文档中是否完全符合以下要求：

a) 开发者应建立标准化的、用于开发和维护终端计算机的生存周期模型；

b) 标准化的生存周期模型应是为某些专家组(例如学科专家、标准化实体等)所认可的模型；

c) 该模型应对终端计算机开发和维护提供必要的控制；

d) 开发者所提供的生存周期定义文档应描述用于开发和维护终端计算机的模型，解释选择该模型的原因，解释如何用该模型来开发和维护终端计算机，以及阐明与标准化的生存周期模型的相符性。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.5.4 工具和技术

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.5 d) 的要求，确定终端计算机第三级的工具和技术。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 开发者应标识用于开发终端计算机的工具，并且所有用于实现的开发工具都应有明确定义；

b) 开发者应文档化已选择的依赖实现的开发工具的选项，开发工具文档应明确定义实现中每个语句的含义，以及明确定义所有基于实现的选项的含义。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.6 测试

5.4.3.6.1 测试范围

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.6 a）的要求，确定终端计算机第三级的测试范围。

——测试评价方法：

a） 评估者应审查开发者提供的测试覆盖分析结果，是否表明了测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的；

b） 评价测试文档中已标识的测试是否包括了安全功能设计描述中所有安全功能的测试，是否都经过了完整性测试；

c） 评估者应审查测试文档，是否覆盖了在功能设计描述中的所有安全功能；

d） 开发者所提供的范围分析应表明测试文档所标识的测试与功能设计所描述的安全功能之间的对应性；

e） 测试范围的分析应阐明功能设计所描述的安全功能和测试文档所标识的测试之间的对应性是完备的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.6.2 测试深度

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.6 b）的要求，确定终端计算机第三级的测试深度。

——测试评价方法：

a） 评价开发者提供的测试深度分析，是否说明了测试文档中所标识的对安全功能的测试，足以表明该安全功能与高层设计和低层设计是一致的。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.6.3 功能测试

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.6 c）的要求，实现终端计算机第三级的功能测试。

——测试评价方法：

a） 评价开发者提供的测试文档，是否包含测试计划、测试规程、预期的测试结果和实际测试结果；

b） 评价测试计划是否标识了要测试的安全功能，是否描述了测试的目标；

c） 评价测试规程是否标识了要执行的测试，是否描述了每个安全功能的测试概况（这些概况包括对其他测试结果的顺序依赖性）；

d） 评价期望的测试结果是否表明测试成功后的预期输出；

e） 评价实际测试结果是否表明每个被测试的安全功能能按照规定进行运作；

f） 评价测试文档是否包含测试过程中对顺序依赖性的分析。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.6.4 独立性测试

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.6 d）的要求，实现终端计算机第三级的独立性测试。

——测试评价方法：

a) 开发者提供的测试文档，应表明安全功能是按规定运作的；
b) 开发者应提供与测试相适应的终端计算机；
c) 通过抽样，重复进行测试，检查测试文档的正确性和完备性。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.7 脆弱性评定

5.4.3.7.1 防止误用

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.7 a) 的要求，实现第三级的防止误用设计。

——测试评价方法：

评估者应审查开发者提供的文档，是否满足了以下要求：

a) 评价指南性文档，是否确定了对终端计算机的所有可能的操作方式(包括失败和操作失误后的操作)，是否确定了它们的后果，以及是否确定了对于保持安全操作的意义；
b) 评价指南性文档，是否列出了所有目标环境的假设以及所有外部安全措施(包括外部程序的、物理的或人员的控制)的要求；
c) 评价指南性文档是否完整、清晰、一致、合理；
d) 评价开发者提供的分析文档，是否阐明指南性文档是完整的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.7.2 安全功能强度评估

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.7 b) 的要求，实现第三级的安全功能强度评估设计。

——测试评价方法：

评估者应审查开发者提供的文档，是否满足了以下要求：

a) 通过对安全机制的安全行为的合格性或统计结果的分析，以及对克服脆弱性所付出努力的分析，得到终端计算机安全功能强度的说明；
b) 对安全目标中标识的每个具有安全功能强度声明的安全机制，进行安全功能强度的分析，证明该机制达到或超过安全目标要求所定义的最低强度，并证明该机制达到或超过安全目标要求所定义的特定功能强度。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.4.3.7.3 脆弱性分析

——测试评价内容：

应按 GB/T 20271—2006 中 6.3.5.7c) 的要求，实现第三级的脆弱性分析设计。

——测试评价方法：

a) 评价开发者提供的脆弱性分析文档，是否从用户可能破坏安全策略的明显途径出发，对终端计算机的各种功能进行了分析；
b) 对被确定的脆弱性，评价开发者是否明确记录了采取的措施；
c) 对每一条脆弱性，评价是否有证据显示在使用终端计算机的环境中该脆弱性不能被利用；
d) 评价所提供的文档，是否表明经过标识脆弱性的终端计算机可以抵御明显的穿透性攻击；
e) 实施独立的穿透性测试，检测终端计算机能否抵御低攻击能力攻击者发起的攻击。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5 第四级

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

——测试评价内容：

见 4.4.1.1.1 的内容。

——对开发者的要求：

开发者应提供文档，说明终端计算机的设备提供哪些基本的运行支持措施，提供哪些必要的容错和故障恢复能力，能否满足基本安全可用的要求。

——测试评价方法：

a) 按照开发者提供的文档，逐项验证所提供的运行支持措施是否有效，能否支持终端计算机的基本运行；

b) 按照开发者提供的文档，模拟出现一些故障事件（如：掉电、硬件故障等），验证终端计算机的容错和故障恢复能力是否有效；

c) 检测主机、外部设备、网络连接部件及其他辅助部件，能否满足设备安全可用的要求。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.1.2 设备防盗

——测试评价内容：

见 4.4.1.1.2 的内容。

——测试评价方法：

a) 按照开发者提供的文档，尝试使用各种方式除去设备中的标记，检测能否除去；

b) 检测终端计算机的主机是否具有机箱封装保护，能否防止部件损害或被盗；

c) 对终端计算机设置防盗报警功能，尝试进行相关偷盗操作，检测能否正常报警。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.2 操作系统

——测试评价内容：

见 4.4.1.2 的内容。

——对开发者的要求：

开发者应提供第三方权威机构对该操作系统的检测报告，或者提供文档对 GB/T 20272—2006 中 4.4.1 的各个项目进行说明。

——测试评价方法：

a) 如果提供了第三方权威机构对该操作系统的检测报告，则查验报告，查看报告中对应项目检测结果是否符合；

b) 如果未能提供第三方权威机构对该操作系统的检测报告，则按照 GB/T 20272—2006 中4.4.1 的要求对操作系统的相关项目进行检测；

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3 安全支撑系统

5.5.1.3.1 密码支持

——测试评价内容：

见 4.4.1.3.1 的内容。

——对开发者的要求：

开发者应提供文档和相关证书，说明所使用的密码算法、相关的密码操作以及相关的密钥管理措施，并证明所使用的密码算法已经通过国家密码管理部门的批准。

——测试评价方法：

a) 按照开发者提供的文档和相关证书，检测所使用的密码算法，是否已经通过国家密码管理部门的批准并由密码硬件实现；

b) 按照开发者提供的文档，检验系统是否建立可信存储根密钥；

c) 按照开发者提供的文档，检测所有密钥是否受可信存储根保护；

d) 按照开发者提供的文档，检测可信存储根本身是否由硬件密码模块保护；

e) 按照开发者提供的文档，检测所有密钥是否受可信存储根保护，可信存储根本身是否由可信密码模块保护；

f) 按照密码算法要求进行密码操作，包括：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；

g) 拔除密码硬件，进行密钥生成、数字签名与验证等关键密码操作，检验以上操作是否基于密码硬件支持。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.2 信任链

——测试评价内容：

见 4.4.1.3.2 的内容。

——对开发者的要求：

a) 开发者应提供文档，说明终端计算机如何利用可信度量根和可信硬件模块(TCM)，在系统启动过程中对 BIOS、MBR、OS、应用程序等部件进行完整性度量；

b) 开发者应提供证明，静态信任链中操作系统的完整性度量基准由国家主管机构管理，是否支持离线或在线校验；

c) 开发者应提供文档，说明完整性度量基准是否存储在可信密码模块(TCM)中。

——测试评价方法：

a) 按照开发者提供的文档和相关证书，检测操作系统的完整性度量基准，是否已接受国家主管机构管理；

b) 以未授权用户身份篡改操作系统的完整性度量基准，检测系统检测到未经授权的篡改，并停止操作系统的运行；

c) 对静态信任链中操作系统的完整性度量基准，进行离线或在线校验，检测能否校验成功；

d) 修改操作系统的核心文件后，对操作系统进行完整性度量，检测终端计算机能否终止操作系统的启动；

e) 根据开发者提供的文档，检验是否基于可信硬件模块(TCM)实现信任链的建立，将硬件断开，检验信任链还能否正常工作；

f) 使用各种方法和工具，对 BIOS 进行修改，启动系统，检测系统能否检测出 BIOS 的完整性被破坏；

g) 使用各种方法和工具，对 MBR 进行修改，启动系统，检测系统能否检测出 MBR 的完整性被破坏；

h) 使用各种方法和工具，对保护的应用程序进行修改，启动系统，检测系统能否检测出应用程序的完整性被破坏；

i） 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（如：BIOS、MBR、OS、应用程序）进行实时修复，检测能否实时修复成功。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.3 运行时防护

——测试评价内容：

见 4.4.1.3.3 的内容。

——对开发者的要求：

开发者应提供文档，说明终端计算机具有哪些运行时防护功能。

——测试评价方法：

a） 在系统和外来介质中植入一个测试用的恶意代码，并运行恶意代码；

b） 对文件系统、内存和使用时的外来介质进行扫描，检测系统能否清除或隔离恶意代码；

c） 检测系统能否对恶意代码特征库进行及时更新；

d） 模拟一个利用缓冲区溢出的攻击，检测系统能否基于 CPU，阻止从受保护的内存位置执行恶意代码。

e） 检测系统是否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；

f） 检测系统是否具备以下防火墙功能：

1） IP 过滤：根据源地址、目的地址设置多条允许通过的过滤规则，模拟相应的网络通讯，检测能否正常通讯；根据源地址、目的地址设置多条拒绝通过的过滤规则，模拟相应的网络通讯，检测能否拒绝相应的网络数据包；

2） 应用程序监控：对某个应用程序设置允许访问网络规则，使用这个应用程序访问网络，检测能否正常访问；对某个应用程序设置拒绝访问网络规则，使用这个应用程序访问网络，检测能否拒绝访问；

3） 内容过滤：设置内容过滤条件，以 HTTP 协议、FTP 协议访问含有设置内容的网页或文件，检测能否拒绝访问；以 FTP 协议访问含有设置内容的文件，检测能否拒绝访问；发送和接收含有设置内容的电子邮件，检测能否拒绝访问；

g） 检测系统是否具备以下入侵检测功能：

1） 注册表监控：以未授权用户身份，访问注册表，检测系统能否拒绝访问；以授权用户身份，访问注册表，检测能否正常访问；

2） 文件监控：以未授权用户身份，访问受保护的文件，检测系统能否拒绝访问；以授权用户身份，访问受保护的文件，检测能否正常访问；

3） 事件监测：设置需要监测的异常事件，并模拟异常事件的产生，检测系统能否监测到事件的发生；

4） 实时流量分析：检测系统能否正确分析系统的发送和接收流量；

5） 实时阻断：对系统模拟进行入侵行为，检测系统能否实时阻断入侵行为；

h） 检测系统能否对所接入网络进行可信度评价（包含以下方面：网络提供者是否可信、网络状态和接入条件是否符合设定策略、网络提供的服务是否符合需求，等等），并根据不同可信度评价等级采取不同的安全接入策略，接入不同可信度的网络，检测接入策略是否正确。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.4 系统安全性检测分析

——测试评价内容：

见 4.4.1.3.4 的内容。

——对开发者的要求：

开发者应提供文档，按 GB/T 20271—2006 中 6.4.2.2 的要求，说明终端计算机是否经过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，以设计和实现终端计算机第四级的系统安全性检测分析功能，并且提供相应的检测分析报告。

——测试评价方法：

a) 按照开发者提供的文档，检测终端计算机是否经过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；

b) 根据相关的检测报告，判断检测方法是否科学，检测结果是否可信；

c) 对存在的问题，检测改进措施是否有效。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.5 信任服务

——测试评价内容：

见 4.4.1.3.5 的内容。

——测试评价方法：

a) 检测系统是否在可信密码模块（TCM）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) 检测是否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；

c) 尝试以各种不同权限的管理员访问所有度量值，检测存取访问是否受权限控制；

d) 检测在必要时是否向国家主管机构报告操作系统和关键应用程序完整性度量值。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.6 系统身份标识与鉴别

——测试评价内容：

见 4.4.1.3.6 的内容。

——测试评价方法：

a) 根据开发者提供的文档，验证系统身份的标识的产生过程，检验系统身份标识是否是由唯一绑定的可信密码模块（TCM）产生的密钥；

b) 根据开发者提供的文档，验证身份标识的可信性是否通过权威机构颁发证书来实现；

c) 根据开发者提供的文档，验证系统身份标识的隐秘性；

d) 尝试对终端计算机身份标识信息进行操作，检验身份标识是否能够进行管理和维护；

e) 分别使用经过授权和未经授权的管理员对系统身份标识进行操作，检验系统身份标识是否能够确保其不被非授权地访问、修改或删除；

f) 根据开发者提供的文档模拟终端计算机的身份鉴别过程，验证请求方是否提供系统的身份证书和/或证书信任链验证路径，并通过一定的认证协议完成身份鉴别过程。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.7 数据保密性保护

5.5.1.3.7.1 数据存储保密性

——测试评价内容：

见 4.4.1.3.7 a）的内容。

——对开发者的要求：

开发者应提供文档，说明如何对存储在终端计算机内的重要用户数据进行保密性保护，描述数据加密、数据绑定和数据密封的方法和步骤。

——测试评价方法：

a) 根据开发者提供的文档，对测试数据进行加密，并以密钥的合法持有者身份进行解密，检测能否解密成功；

b) 以其余任何用户身份登录，检测是否无法获得该数据；

c) 根据开发者提供的文档，在特定终端计算机中基于可信存储根对测试数据进行加密，并且由密钥的合法持有者在特定终端计算机中的特定状态下解密，检测能否解密成功；

d) 由密钥的合法持有者在特定终端计算机中的其他状态下解密，检测能否解密成功；

e) 由密钥的合法持有者在其他终端计算机中解密，检测能否解密成功；

f) 以其余任何用户身份登录特定终端计算机，在特定状态下解密测试数据，检测是否无法获得该数据；

g) 以其余任何用户身份登录特定终端计算机，在其他状态下解密测试数据，检测是否无法获得该数据。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.7.2 数据传输保密性

——测试评价内容：

见 4.4.1.3.7 b）的内容。

——对开发者的要求：

开发者应提供文档，说明如何对在不同 SSF 之间基于网络传输的重要数据，进行保密性保护。

——测试评价方法：

a) 利用协议分析仪截取网络传输的用户数据，检测基于网络传输的重要数据是否按照开发者的设计进行保密性保护。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.7.3 客体安全重用

——测试评价内容：

见 4.4.1.3.7 c）的内容。

——对开发者的要求：

开发者应提供文档，说明对安全支撑系统进行动态资源管理过程中，如何保证客体资源（包括子集信息和完全信息）中的剩余信息不应引起信息的泄漏。

——测试评价方法：

a) 检测系统对安全支撑系统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，是否会清除该客体中的原有信息；

b) 检测系统对安全支撑系统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，是否会清除该客体中的原有信息。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.8 数据完整性保护

5.5.1.3.8.1 存储数据的完整性

——测试评价内容：

见 4.4.1.3.8 a）的内容。

——对开发者的要求：

开发者应提供文档，说明系统对基于用户属性的所有客体，如何对存储在 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，系统采取何种恢复措施。

——测试评价方法：

a） 使用各种方法和工具，对安全支撑系统内部存储的数据，进行修改，检测系统能否检测出完整性错误；

b） 检测系统能否采取恢复措施，使数据恢复到修改前的状态。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.8.2 传输数据的完整性

——测试评价内容：

见 4.4.1.3.8 b）的内容。

——对开发者的要求：

开发者应提供文档，说明在 SSF 和其他可信信息系统间传输用户数据时，提供了哪些数据完整性检测的功能；并说明接收者如何恢复被破坏的数据为原始的用户数据。

——测试评价方法：

a） 使用各种方法和工具，对在 SSF 和其他可信信息系统间传输的用户数据，进行篡改、删除、插入等操作，检测系统能否检测出完整性错误；

b） 接收者尝试对被破坏的数据进行恢复，检测是否能够恢复为原始的用户数据。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.8.3 处理数据的完整性

——测试评价内容：

见 4.4.1.3.8 c）的内容。

——对开发者的要求：

开发者应提供文档，说明对终端计算机中处理中的数据采用何种方式保证处理数据的完整性。

——测试评价方法：

a） 根据开发者提供的文档，定制相关的 SSF 访问控制策略；

b） 选定一个终端计算机中处理中的数据为测试数据，对其进行一系列操作，检测系统能否对所进行的操作序列进行回退，并恢复数据为操作前的状态。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.9 安全审计

——测试评价内容：

见 4.4.1.3.9 的内容。

——对开发者的要求：

开发者应提供文档，说明安全支撑系统中生成、维护及保护审计数据过程，以及具备哪些保护措施。

——测试评价方法：

a） 查看系统的审计记录信息，检测是否有密码支持、系统身份标识与鉴别、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相关操作的审计记录；

b） 检测审计功能是否支持审计日志；

c） 对于内置于终端计算机的可信密码模块，检测能否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，并查看审计记录；检测是否提供给上层应用软件查询审计情况的接口；检测能否存储审计记录；

d) 检测审计记录是否包括：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；

e) 检测审计功能是否支持潜在侵害分析；检测系统能否用一系列规则去监控审计事件，并根据这些规则指出系统的潜在侵害；

f) 检测系统能否确立用户或进程的质疑度（或信誉度）；当用户或进程的质疑等级超过门限条件时，检测系统能否发现并指出将要发生对安全性的威胁；

g) 检测系统是否提供系统行为记录与侵害的签名事件匹配的功能，检测系统能否通过对一个或多个事件的对比分析或综合分析，预测攻击出现的时间或方式；

h) 检测审计功能是否为授权用户提供基本审计查阅；检测系统是否提供审计查阅工具对审计数据进行搜索、分类、排序；以未授权用户身份，尝试查阅审计信息，检测系统是否拒绝未授权访问；

i) 检测审计功能是否支持根据客体身份、用户身份、主体身份、主机身份、事件类型等属性进行审计事件选择；

j) 在意外情况出现时，检测审计功能是否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，检测审计功能是否能够采取相应的保护措施，确保有实效性的审计记录不被破坏；

k) 根据开发者提供的文档，检测审计数据是否受到安全保护，尝试以未授权用户进行访问、修改和破坏审计信息，检测系统能否拒绝未授权访问；

l) 检测系统能否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。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.10 备份与故障恢复

——测试评价内容：

见 4.4.1.3.10 的内容。

——对开发者的要求：

开发者应提供文档，说明对用户数据和系统，如何在备份、存储和恢复过程中进行安全保护，以及具备哪些备份保护措施。

——测试评价方法：

a) 以授权用户身份有选择地备份重要数据的功能，对数据进行修改，然后进行恢复，检测能否有效恢复；

b) 对系统的运行现场进行定期备份，对系统数据进行修改，然后进行恢复，检测能否有效恢复；

c) 根据开发者提供的文档，检测数据在备份、存储和恢复过程中是否具有安全保护措施，是否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，用户操作系统是否不可访问系统备份数据。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.11 I/O 接口配置

——测试评价内容：

见 4.4.1.3.11 的内容。

——测试评价方法：

a) 以授权用户身份，在 BIOS 和操作系统中，分别启用串口、并口、USB、网卡、硬盘，检测能否正常使用；

b) 以授权用户身份，在 BIOS 和操作系统中，分别禁用串口、并口、USB、网卡、硬盘，检测能否使用；

c) 检测系统能否接受所接入网络的接口集中配置管理，尝试以未授权用户进行配置管理，检测系统能否拒绝未授权访问。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.1.3.12 可信时间戳

——测试评价内容：

见 4.4.1.3.12 的内容。

——对开发者的要求：

开发者应提供文档，说明系统如何提供可信的时间戳。

——测试评价方法：

a) 根据开发者提供的文档，检测系统是否提供可靠的时钟和时钟同步系统。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.2 SSOTC 自身安全保护

5.5.2.1 安全支撑系统的自身安全保护

——测试评价内容：

见 4.4.2.1 的内容。

——对开发者的要求：

开发者应提供文档，说明可信存储根是否设置在可信密码模块内，所采用的可信密码模块是否由国家主管机构研制，并提供该机构相应的资质证书；说明可信报告根是否设置在可信密码模块内，可信报告根所对应的公钥证书由哪家机构发行和管理，并提供该机构相应的资质证书；说明可信度量根是否设置在固件模块内，该模块的物理位置，以及计算机的启动过程，是否包含了该模块；提供物理结构图，包括键盘输入信号路径，可信密码模块、物理开关位置等详细信息；说明采取何种方式对安全支撑系统的使用用户进行鉴别。

——测试评价方法：

a) 按照开发者提供的文档，检测可信存储根和可信报告根是否设置在可信密码模块内；

b) 按照开发者提供的文档和相关证书，检测所使用的密码模块是否通过国家主管机构测评认证；

c) 按照开发者提供的文档，并查看可信报告根的公钥证书及其发行机构相关证书，检验是否由国家专门权威机构发行和管理；

d) 查验文档是否符合要求，通过加载/卸载可信度量根，和其所在的固件模块，检验终端计算机启动是否依赖该固件和可信度量根；

e) 按照开发者提供的文档，检测是否对可信度量根采取物理保护措施，并且检测保护措施的有效性；

f) 查验开发者提供的物理结构图，检查是否有物理路径支持键盘输入与可信密码模块的直接通信，是否具有物理开关控制；

g) 打开机箱检验物理线路是否与图纸一致，分别打开、关闭控制开关，检验其是否有效；

h) 尝试以授权用户和非授权用户去使用可信密码模块，检验是否需要进行身份鉴别。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.2.2 操作系统的自身安全保护

——测试评价内容：

见 4.4.2.2 的内容。

——对开发者的要求：

开发者应提供第三方权威机构对该操作系统的检测报告，或者提供文档对 GB/T 20272—2006 中 4.4.2 的各个项目进行说明。

——测试评价方法：

a) 如果提供了第三方权威机构对该操作系统的检测报告，则查验报告，查看报告中对应项目检测结果是否符合；

b) 如果未能提供第三方权威机构对该操作系统的检测报告，则按照 GB/T 20272—2006 中4.4.2 的要求对操作系统的相关项目进行检测。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3 SSOTC 设计和实现

5.5.3.1 配置管理

5.5.3.1.1 配置管理能力

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.1 a) 的要求，实现终端计算机第四级的配置管理能力设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 开发者所使用的版本号与所应表示的终端计算机样本应完全对应，没有歧义。

b) 配置管理系统应对所有的配置项作出唯一的标识。

c) 配置管理计划中，应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。

d) 配置管理文档应提供所有的配置项得到有效地维护的证据。

e) 配置管理系统应确保对配置项只进行授权修改。

f) 配置管理系统应支持终端计算机的生成。

g) 验收计划应描述用来验收修改过的或新建的配置项的过程，将其作为终端计算机的一部分，并确认对配置项的任何生成和修改都是由授权者进行的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.1.2 配置管理自动化

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.1 b) 的要求，实现终端计算机第四级的配置管理自动化设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 配置管理系统应通过自动方式来确保终端计算机的实现表示只能进行已授权的变化，并能提供自动方式来支持终端计算机的生成；

b) 配置管理计划应描述配置管理系统中所使用的自动工具，并说明如何使用这些工具。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.1.3 配置管理范围

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.1 c)、6.4.5.1 d) 的要求，实现终端计算机第四级的配置管理范围设计。

——测试评价方法：

a) 终端计算机配置管理范围，要求将终端计算机的实现表示、设计文档、测试文档、用户文档、安全管理员文档、配置管理文档等置于配置管理之下，从而确保它们的修改是在一个正确授权的可控方式下进行的。为此要求：
   1) 开发者所提供的配置管理文档应展示配置管理系统至少能跟踪上述配置管理之下的内容；
   2) 文档应描述配置管理系统是如何跟踪这些配置项的；
   3) 文档还应提供足够的信息表明达到所有要求；
b) 配置管理系统应对安全缺陷进行跟踪；
c) 配置管理系统应对开发工具和相关信息进行跟踪。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.2 分发和操作

5.5.3.2.1 分发

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.2 a) 的要求，实现终端计算机第四级的分发。

——测试评价方法：

a) 评估者应审查开发者是否按分发过程的要求，编制分发文档；
b) 评估者应审查分发文档，是否描述给用户分发终端计算机时，用以维护安全所必须的所有过程；
c) 评估者应审查是否按该过程进行分发；
d) 评估者应审查分发文档，是否描述检测修改的方法和技术，是否描述开发者的主拷贝与用户收到的版本之间的差异；
e) 评估者应审查分发文档，是否描述用来检测试图伪装成开发者向用户发送产品的方法；
f) 评估者应审查分发文档，是否在修改检测的基础上，还描述了如何防止修改的方法和技术。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.2.2 操作

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.2 b) 的要求，实现终端计算机第四级的操作。

——测试评价方法：

a) 评估者应审查操作文档，是否说明了终端计算机在开发者所期望的安全方式下进行安装、生成和启动的过程。用户能够通过此文档了解安装、生成和启动过程；
b) 评估者应审查操作文档，是否说明了将处于配置控制下的终端计算机的实现安全地转换为用户环境下的初始操作，并最终生成了安全的配置。用户能够通过此文档了解安装、生成、启动完成后，终端计算机在用户环境下生成的相应的安全配置情况；
c) 评估者应审查操作文档，是否说明了日志生成的要求(包括日志生成选项、生成时间及生成方

法等)和过程。用户能够通过此文档进行建立日志的过程。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.3 开发

5.5.3.3.1 功能设计

——测试评价内容:

应按 GB/T 20271—2006 中 6.4.5.3 a) 的要求,实现终端计算机第四级的功能设计。

——测试评价方法:

评估者应审查开发者所提供的信息是否满足如下要求:

a) 功能设计应当使用半形式化风格来描述终端计算机安全功能与其外部接口,必要时可由非形式化、解释性的文字来支持;

b) 功能设计应当是内在一致的;

c) 功能设计应当描述使用所有外部终端计算机安全功能接口的目的与方法,适当的时候,要提供结果影响例外情况和错误信息的细节;

d) 开发者应完备地表示终端计算机安全功能的基本原理。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.3.2 安全策略模型

——测试评价内容:

应按 GB/T 20271—2006 中 6.4.5.3 b) 的要求,实现终端计算机第四级的安全策略模型设计。

——测试评价方法:

评估者应审查开发者所提供的文档中,安全策略模型的相关内容,是否满足如下要求:

a) SSP 模型应是半形式化的,并描述所有可以模型化的 SSP 策略的规则与特征;

b) SSP 模型应包括一个基本原理,阐明该模型与所有可模型化的 SSP 策略是一致的、完备的;

c) SSP 模型和功能设计之间的对应性阐明应说明功能设计中的安全功能与 SSP 模型是一致的、完备的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.3.3 高层设计

——测试评价内容:

应按 GB/T 20271—2006 中 6.4.5.3 c) 的要求,实现终端计算机第四级的高层设计。

——测试评价方法:

评估者应审查开发者所提供的高层设计文档是否满足如下要求:

a) 以子系统的观点、以半形式化的方法来一致性地描述终端计算机的体系结构;

b) 描述每一个子系统所提供的安全功能及其相互关系;

c) 标识安全功能要求的任何基础性的硬件、固件和/或软件,并且通过这些硬件、固件和/或软件所实现的保护机制,来提供安全功能功能;

d) 标识安全功能子系统的所有接口,并标明安全功能子系统的哪些接口是外部可见的;

e) 高层设计文档应当描述安全功能子系统所有接口的使用目的与方法,并提供例外情况和错误信息的细节;

f) 高层设计文档应当描述如何将终端计算机分离成安全策略加强单元和其他子系统;

g) 高层设计文档应当描述所提供的 SSP 模型是否是半形式化的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.3.4 低层设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.3 d) 的要求，实现终端计算机第四级的低层设计。

——测试评价方法：

评估者应审查开发者所提供的低层设计文档是否满足如下要求：

a) 低层设计的表示应是半形式化的，内在一致的，并以模块术语描述，必要时提供所有结果的完备细节、例外情况和错误信息；

b) 描述每一个模块的目的；

c) 以所提供的安全功能和对其他模块的依赖性术语定义模块间的相互关系；

d) 描述如何提供每一个安全策略功能的实施；

e) 标识终端计算机安全功能模块的所有接口，标识终端计算机安全功能模块的哪些接口是外部可见的，以及描述终端计算机安全功能模块所有接口的目的与方法，必要时，应提供影响、例外情况和错误信息的细节；

f) 描述如何将终端计算机分离成安全策略实施模块和其他模块。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.3.5 内部结构设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.3 e) 的要求，实现终端计算机第四级的内部结构设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 应以模块化方法设计和构建终端计算机安全功能，并避免设计模块之间出现不必要的交互；

b) 标识终端计算机安全功能模块，并应描述每一个终端计算机安全功能模块的目的、接口、参数和影响；

c) 描述终端计算机安全功能设计是如何使独立的模块间避免不必要的交互作用；

d) 在设计和构建安全功能时，应使安全功能局部的复杂度最小化，以加强访问控制策略；

e) 标识安全功能模块，并应指明安全功能的哪些部分是加强安全策略的；

f) 描述分层结构，并说明如何使交互作用最小化；

g) 描述加安全策略的安全功能部分是如何被构建的，从而使其复杂性降低；

h) 描述在设计和构建 SSF 时，如何保证实施任何安全策略的 SSF 部分简单且易分析；

i) 描述那些与 SSF 无关的功能是否已从 SSF 中排斥出去。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.3.6 实现表示

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.3 f) 的要求，实现终端计算机第四级的实现表示设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 应无歧义地为全部终端计算机安全功能，定义一个详细级别的终端计算机安全功能实现表示，并且实现表示应当是内在一致的；

b) 所定义的实现表示应是结构精简的，且易于理解。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.3.7 对应性设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.3 g）的要求，实现终端计算机第四级的对应性设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a） 应在所提供的终端计算机安全功能表示的所有相邻对之间提供其对应性分析，对每个相邻对，应当阐明较为抽象的终端计算机安全功能表示的所有相关安全功能在较不抽象的终端计算机安全功能表示中得到正确而完备地细化；

b） 当 SSF 表示的两个相邻对的各部分至少都是以半形式化来描述时，其对应性说明是否也是半形式化的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.4 文档要求

5.5.3.4.1 管理员指南

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.4 的要求，实现终端计算机第四级的管理员指南。

——测试评价方法：

评估者应审查开发者是否提供了供系统管理员使用的管理员指南，并且此管理员指南是否包括如下内容：

a） 终端计算机可以使用的管理功能和接口；

b） 怎样安全地管理终端计算机；

c） 在安全处理环境中应进行控制的功能和权限；

d） 所有对与终端计算机的安全操作有关的用户行为的假设；

e） 所有受管理员控制的安全参数，如果可能，应指明安全值；

f） 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g） 所有与系统管理员有关的 IT 环境的安全要求。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.4.2 用户指南

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.4 的要求，实现终端计算机第四级的用户指南。

——测试评价方法：

评估者应审查开发者是否提供了供系统用户使用的用户指南，并且此用户指南是否包括如下内容：

a） 终端计算机的非管理用户可使用的安全功能和接口；

b） 终端计算机提供给用户的安全功能和接口的用法；

c） 用户可获取但应受安全处理环境控制的所有功能和权限；

d） 终端计算机安全操作中用户所应承担的职责；

e） 与用户有关的 IT 环境的所有安全要求。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.5 生存周期支持

5.5.3.5.1 开发安全

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.5 a) 的要求，实现终端计算机第四级的开发安全。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 开发人员的安全管理：开发人员的安全规章制度，开发人员的安全教育培训制度和记录；

b) 开发环境的安全管理：开发地点的出入口控制制度和记录，开发环境的温室度要求和记录，开发环境的防火防盗措施和国家有关部门的许可文件，开发环境中所使用安全产品必须采用符合国家有关规定的产品并提供相应证明材料；

c) 开发设备的安全管理：开发设备的安全管理制度，包括开发主机使用管理和记录，设备的购置、修理、处置的制度和记录，上网管理，计算机病毒管理和记录等；

d) 开发过程和成果的安全管理：对产品代码、文档、样机进行受控管理的制度和记录，若代码和文档进行加密保护必须采用符合国家有关规定的产品并提供相应证明材料；

e) 开发安全文件中所提供的安全措施的证据应能证明安全措施对维护终端计算机的安全性提供了必要的保护。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.5.2 缺陷纠正

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.5 b) 的要求，实现终端计算机第四级的缺陷纠正。

——测试评价方法：

评估者应审查开发者所提供的生存周期定义文档中是否完全符合以下要求：

a) 描述用以跟踪所有终端计算机版本里已被报告的安全缺陷的过程；

b) 描述所提供的每个安全缺陷的性质和效果，以及缺陷纠正的情况；

c) 标识每个安全缺陷所采取的纠正措施；

d) 描述为终端计算机用户的纠正行为所提供的信息，纠正和指导的方法。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.5.3 生存周期定义

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.5 c) 的要求，实现终端计算机第四级的生存周期定义。

——测试评价方法：

评估者应审查开发者所提供的生存周期定义文档中是否完全符合以下要求：

a) 开发者应建立标准化的、用于开发和维护终端计算机的生存周期模型；

b) 标准化的生存周期模型应是为某些专家组(例如学科专家、标准化实体等)所认可的模型；

c) 该模型应对终端计算机开发和维护提供必要的控制；

d) 开发者所提供的生存周期定义文档应描述用于开发和维护终端计算机的模型，解释选择该模型的原因，解释如何用该模型来开发和维护终端计算机，以及阐明与标准化的生存周期模型的相符性。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.5.4 工具和技术

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.5 d）的要求，确定终端计算机第四级的工具和技术。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a） 开发者应标识用于开发终端计算机的工具，并且所有用于实现的开发工具都应有明确定义。开发者应文档化已选择的依赖实现的开发工具的选项，开发工具文档应明确定义实现中每个语句的含义，以及明确定义所有基于实现的选项的含义。

b） 开发者应对终端计算机所应用部分的实现标准进行描述。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.6 测试

5.5.3.6.1 测试范围

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.6 a）的要求，确定终端计算机第四级的测试范围。

——测试评价方法：

a） 评估者应审查开发者提供的测试覆盖分析结果，是否表明了测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的；

b） 评价测试文档中已标识的测试是否包括了安全功能设计描述中所有安全功能的测试，是否都经过了完整性测试；

c） 评估者应审查测试文档，是否覆盖了在功能设计描述中的所有安全功能；

d） 开发者所提供的范围分析应表明测试文档所标识的测试与功能设计所描述的安全功能之间的对应性；

e） 测试范围的分析应阐明功能设计所描述的安全功能和测试文档所标识的测试之间的对应性是完备的；

f） 测试范围的分析应严格地阐明功能设计所标识的安全功能的所有外部接口已经被完备测试过了。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.6.2 测试深度

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.6 b）的要求，确定终端计算机第四级的测试深度。

——测试评价方法：

a） 评价开发者提供的测试深度分析，是否说明了测试文档中所标识的对安全功能的测试，足以表明该安全功能与高层设计和低层设计是一致的；

b） 开发者所提供的测试深度分析应阐明测试文档中所标识的测试足以表明该安全功能是根据高层设计、低层设计和实现表示而运作的。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.6.3 功能测试

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.6 c) 的要求，实现终端计算机第四级的功能测试。

——测试评价方法：

a) 评价开发者提供的测试文档，是否包含测试计划、测试规程、预期的测试结果和实际测试结果；

b) 评价测试计划是否标识了要测试的安全功能，是否描述了测试的目标；

c) 评价测试规程是否标识了要执行的测试，是否描述了每个安全功能的测试概况(这些概况包括对其他测试结果的顺序依赖性)；

d) 评价期望的测试结果是否表明测试成功后的预期输出；

e) 评价实际测试结果是否表明每个被测试的安全功能能按照规定进行运作；

f) 评价测试文档是否包含测试过程中对顺序依赖性的分析。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.6.4 独立性测试

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.6 d) 的要求，实现终端计算机第四级的独立性测试。

——测试评价方法：

a) 开发者提供的测试文档，应表明安全功能是按规定运作的；

b) 开发者应提供与测试相适应的终端计算机；

c) 通过抽样，重复进行测试，检查测试文档的正确性和完备性。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.7 脆弱性评定

5.5.3.7.1 隐蔽信道分析

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.7 a) 的要求，实现网络第四级的隐蔽信道分析设计。

——测试评价方法：

评估者应审查开发者提供的文档中，隐蔽信道分析的相关内容，是否满足了以下要求：

a) 描述如何通过对隐蔽存储信道的非形式化搜索，标识出可识别的隐蔽存储信道，并估算它们的带宽；

b) 描述用于确定隐蔽存储信道存在的过程，以及进行隐蔽存储信道分析所需要的信息；

c) 描述隐蔽存储信道分析期间所作的全部假设；

d) 描述最坏情况下对隐蔽存储信道带宽进行估算的方法；

e) 描述每个可标识的隐蔽存储信道的最大可利用情形；

f) 描述用封锁和/或限制带宽和/或审计等，对所标识的隐蔽存储信道进行处理的措施。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.7.2 防止误用

——测试评价内容：

应按 GB/T 20271—2006 中 6.4.5.7 b) 的要求，实现网络第四级的防止误用设计。

——测试评价方法：

评估者应审查开发者提供的文档，是否满足了以下要求：

a) 评价指南性文档，是否确定了对终端计算机的所有可能的操作方式(包括失败和操作失误后的操作)，是否确定了它们的后果，以及是否确定了对于保持安全操作的意义；

b) 评价指南性文档,是否列出了所有目标环境的假设以及所有外部安全措施(包括外部程序的、物理的或人员的控制)的要求;
c) 评价指南性文档是否完整、清晰、一致、合理;
d) 评价开发者提供的分析文档,是否阐明指南性文档是完整的;
e) 评估者应进行独立验证,以确定安全管理员或用户在正确理解文档的情况下能基本判断 SSOTC 是否在不安全状态下配置或运行。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.7.3 安全功能强度评估

——测试评价内容:

应按 GB/T 20271—2006 中 6.4.5.7 c) 的要求,实现网络第四级的安全功能强度评估设计。

——测试评价方法:

评估者应审查开发者提供的文档,是否满足了以下要求:

a) 通过对安全机制的安全行为的合格性或统计结果的分析,以及对克服脆弱性所付出努力的分析,得到终端计算机安全功能强度的说明;
b) 对安全目标中标识的每个具有安全功能强度声明的安全机制,进行安全功能强度的分析,证明该机制达到或超过安全目标要求所定义的最低强度,并证明该机制达到或超过安全目标要求所定义的特定功能强度。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.5.3.7.4 脆弱性分析

——测试评价内容:

应按 GB/T 20271—2006 中 6.4.5.7 d) 的要求,实现网络第四级的脆弱性分析设计。

——测试评价方法:

a) 评价开发者提供的脆弱性分析文档,是否从用户可能破坏安全策略的明显途径出发,对终端计算机的各种功能进行了分析;
b) 对被确定的脆弱性,评价开发者是否明确记录了采取的措施;
c) 对每一条脆弱性,评价是否有证据显示在使用终端计算机的环境中该脆弱性不能被利用;
d) 评价所提供的文档,是否表明经过标识脆弱性的终端计算机可以抵御明显的穿透性攻击;
e) 实施独立的穿透性测试,检测终端计算机能否抵御低攻击能力攻击者发起的攻击;
f) 评价开发者提供的分析文档,是否表明对脆弱性的搜索是系统化的,并确定终端计算机能否抵御中攻击能力的攻击者发起的对 SSOTC 的穿透性攻击。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6 第五级

5.6.1 安全功能要求

5.6.1.1 物理系统

5.6.1.1.1 设备安全可用

——测试评价内容:

见 4.5.1.1.1 的内容。

——对开发者的要求:

开发者应提供文档，说明终端计算机的设备提供哪些基本的运行支持措施，提供哪些必要的容错和故障恢复能力，能否满足基本安全可用的要求。

——测试评价方法：

a) 按照开发者提供的文档，逐项验证所提供的运行支持措施是否有效，能否支持终端计算机的基本运行；

b) 按照开发者提供的文档，模拟出现一些故障事件（如：掉电、硬件故障等），验证终端计算机的容错和故障恢复能力是否有效；

c) 检测主机、外部设备、网络连接部件及其他辅助部件，能否满足基本安全可用的要求；

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.1.2 设备防盗

——测试评价内容：

见 4.5.1.1.2 的内容。

——测试评价方法：

a) 按照开发者提供的文档，尝试使用各种方式除去设备中的标记，检测能否除去；

b) 检测终端计算机的主机是否具有机箱封装保护，能否防止部件损害或被盗；

c) 对终端计算机设置防盗报警功能，尝试进行相关偷盗操作，检测能否正常报警。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.1.3 设备高可靠

——测试评价内容：

见 4.5.1.1.3 的内容。

——测试评价方法：

根据特殊环境应用要求，终端计算机设备高可靠分为：

a) 检测系统是否具有防水要求；

b) 检测系统是否具有防跌落和防震功能；

c) 检测系统能否抗高低温与高低气压；

d) 检测系统能否抗电磁辐射与干扰。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.2 操作系统

——测试评价内容：

见 4.5.1.2 的内容。

——对开发者的要求：

开发者应提供第三方权威机构对该操作系统的检测报告，或者提供文档对 GB/T 20272—2006 中 4.5.1 的各个项目进行说明。

——测试评价方法：

a) 如果提供了第三方权威机构对该操作系统的检测报告，则查验报告，查看报告中对应项目检测结果是否符合；

b) 如果未能提供第三方权威机构对该操作系统的检测报告，则按照 GB/T 20272—2006 中4.5.1 的要求对操作系统的相关项目进行检测。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3 安全支撑系统

5.6.1.3.1 密码支持

——测试评价内容：

见 4.5.1.3.1 的内容。

——对开发者的要求：

开发者应提供文档和相关证书，说明所使用的密码算法、相关的密码操作以及相关的密钥管理措施，并证明所使用的密码算法已经通过国家密码管理部门的批准。

——测试评价方法：

a) 按照开发者提供的文档和相关证书，检测所使用的密码算法，是否已经通过国家密码管理部门的批准并由密码硬件实现；

b) 按照开发者提供的文档，检测所有密钥是否受可信存储根保护；

c) 按照开发者提供的文档，检测可信存储根本身是否由硬件密码模块保护；

d) 按照开发者提供的文档，检测所有密钥是否受可信存储根保护，可信存储根本身是否由可信密码模块保护；

e) 按照密码算法要求进行密码操作，包括：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；

f) 拔除密码硬件，进行密钥生成、数字签名与验证等关键密码操作，检验以上操作是否基于密码硬件支持。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.2 信任链

——测试评价内容：

见 4.5.1.3.2 的内容。

——对开发者的要求：

a) 开发者应提供文档，说明终端计算机如何利用可信度量根和可信硬件模块，在系统启动过程中对 BIOS、MBR、OS、应用程序等部件进行完整性度量；

b) 开发者应提供证明，静态信任链中操作系统的完整性度量基准由国家主管机构管理，是否支持离线或在线校验；

c) 开发者应提供文档，分别说明静态完整性度量基准和动态完整性度量基准是否存储在可信密码模块中。

——测试评价方法：

a) 按照开发者提供的文档和相关证书，检测操作系统的完整性度量基准，是否已接受国家主管机构管理；

b) 以未授权用户身份篡改操作系统的完整性度量基准，检测系统检测到未经授权的篡改，并停止操作系统的运行；

c) 对静态信任链中操作系统的完整性度量基准，进行离线和在线校验，检测能否校验成功；

d) 修改操作系统的核心文件后，对操作系统进行完整性度量，检测终端计算机能否终止操作系统的启动；

e) 根据开发者提供的文档，检验是否基于可信硬件模块实现信任链的建立，将硬件断开，检验信任链还能否正常工作；

f) 使用各种方法和工具，对 BIOS 进行修改，启动系统，检测系统能否检测出 BIOS 的完整性被

破坏；

g） 使用各种方法和工具，对 MBR 进行修改，启动系统，检测系统能否检测出 MBR 的完整性被破坏；

h） 使用各种方法和工具，对保护的应用程序进行修改，启动系统，检测系统能否检测出应用程序的完整性被破坏，并停止应用程序的运行；

i） 检测应用程序的完整性度量基准，是否接受国家主管机构管理，是否支持在线或离线校验；使用各种方法和工具，对应用程序的完整性进行破坏，检验动态信任链是否能够检测出完整性被破坏；检测应用程序的动态完整性度量基准是否存储在可信密码模块中；

j） 检查动态信任链中关键应用程序的完整性度量基准是否由国家主管机构管理，是否支持在线离线校验；

k） 破坏应用程序的完整性后，检测应用程序是否能立即停止运行；

l） 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（如：BIOS、MBR、OS、应用程序）进行实时修复，检测能否实时修复成功。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.3 运行时防护

——测试评价内容：

见 4.5.1.3.3 的内容。

——对开发者的要求：

开发者应提供文档，说明终端计算机具有哪些运行时防护功能。

——测试评价方法：

a） 在系统和外来介质中植入一个测试用的恶意代码，并运行恶意代码；

b） 对文件系统、内存和使用时的外来介质进行扫描，检测系统能否清除或隔离恶意代码；

c） 检测系统能否对恶意代码特征库进行及时更新；

d） 模拟一个利用缓冲区溢出的攻击，检测系统能否基于 CPU，阻止从受保护的内存位置执行恶意代码；

e） 检测系统是否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；

f） 检测系统能否基于专家系统，对进程行为的危险程度进行等级评估，并根据评估结果，采取相应防护措施；

g） 检测系统是否具备以下防火墙功能：

1） IP 过滤：根据源地址、目的地址设置多条允许通过的过滤规则，模拟相应的网络通讯，检测能否正常通讯；根据源地址、目的地址设置多条拒绝通过的过滤规则，模拟相应的网络通讯，检测能否拒绝相应的网络数据包；

2） 应用程序监控：对某个应用程序设置允许访问网络规则，使用这个应用程序访问网络，检测能否正常访问；对某个应用程序设置拒绝访问网络规则，使用这个应用程序访问网络，检测能否拒绝访问；

3） 内容过滤：设置内容过滤条件，以 HTTP 协议、FTP 协议访问含有设置内容的网页或文件，检测能否拒绝访问；以 FTP 协议访问含有设置内容的文件，检测能否拒绝访问；发送和接收含有设置内容的电子邮件，检测能否拒绝访问；

h） 检测系统是否具备以下入侵检测功能：

1） 注册表监控：以未授权用户身份，访问注册表，检测系统能否拒绝访问；以授权用户身份，访问注册表，检测能否正常访问；

2） 文件监控：以未授权用户身份，访问受保护的文件，检测系统能否拒绝访问；以授权用户

身份，访问受保护的文件，检测能否正常访问；

3） 事件监测：设置需要监测的异常事件，并模拟异常事件的产生，检测系统能否监测到事件的发生；

4） 实时流量分析：检测系统能否正确分析系统的发送和接收流量；

5） 实时阻断：对系统模拟进行入侵行为，检测系统能否实时阻断入侵行为；

i） 检测系统能否对所接入网络进行可信度评价（包含以下方面：网络提供者是否可信、网络状态和接入条件是否符合设定策略、网络提供的服务是否符合需求等），并根据不同可信度评价等级采取不同的安全接入策略，接入不同可信度的网络，检测接入策略是否正确。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.4 系统安全性检测分析

——测试评价内容：

见 4.5.1.3.4 的内容。

——对开发者的要求：

开发者应提供文档，按 GB/T 20271—2006 中 6.4.2.2 的要求，说明终端计算机是否经过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，以设计和实现终端计算机访问验证级的系统安全性检测分析功能，并且提供相应的检测分析报告。

——测试评价方法：

a） 按照开发者提供的文档，检测终端计算机是否经过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；

b） 根据相关的检测报告，判断检测方法是否科学，检测结果是否可信；

c） 对存在的问题，检测改进措施是否有效。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.5 信任服务

——测试评价内容：

见 4.5.1.3.5 的内容。

——对开发者的要求：

开发者应提供文档，说明在可信密码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。

——测试评价方法：

a） 检测系统是否在可信密码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） 检测系统是否设置一个由可信密码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） 检测系统在必要时是否向国家主管机构报告操作系统和应用程序完整性度量值。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.6 系统身份标识与鉴别

——测试评价内容：

见 4.5.1.3.6 的内容。

——对开发者的要求：

开发者应提供文档，详细说明系统标识产生的过程以及终端计算机身份的鉴别过程。

——测试评价方法：

a） 根据开发者提供的文档，验证系统身份的标识的产生过程，检验系统身份标识是否是由唯一绑

定的可信密码模块(TCM)产生的密钥；

b) 根据开发者提供的文档，验证身份标识的可信性是否通过权威机构颁发证书来实现；

c) 根据开发者提供的文档，验证系统身份标识的隐秘性；

d) 尝试对终端计算机身份标识信息进行操作，检验身份标识是否能够进行管理和维护；

e) 分别使用经过授权和未经授权的管理员对系统身份标识进行操作，检验系统身份标识是否能够确保其不被非授权地访问、修改或删除；

f) 根据开发者提供的文档模拟终端计算机的身份鉴别过程，验证请求方是否提供系统的身份证书和/或证书信任链验证路径，并通过一定的认证协议完成身份鉴别过程；

g) 检测系统身份标识是否由国家权威管理机构进行管理。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.7 数据保密性保护

5.6.1.3.7.1 数据存储保密性

——测试评价内容：

见 4.5.1.3.7 a) 的内容。

——对开发者的要求：

开发者应提供文档，说明如何对存储在终端计算机内的重要用户数据进行保密性保护，描述数据加密、数据绑定和数据密封的方法和步骤。

——测试评价方法：

a) 根据开发者提供的文档，对测试数据进行加密，并以密钥的合法持有者身份进行解密，检测能否解密成功；

b) 以其余任何用户身份登录，检测是否无法获得该数据；

c) 根据开发者提供的文档，检测系统能否基于可信存储根实现对数据的保密存储；

d) 在特定终端计算机中对测试数据进行加密，并且由密钥的合法持有者在特定终端计算机中的特定状态下解密，检测能否解密成功；

e) 由密钥的合法持有者在特定终端计算机中的其他状态下解密，检测能否解密成功；

f) 由密钥的合法持有者在其他终端计算机中解密，检测能否解密成功。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.7.2 数据传输保密性

——测试评价内容：

见 4.5.1.3.7 b) 的内容。

——对开发者的要求：

开发者应提供文档，说明如何对在不同 SSF 之间传输的数据，进行保密性保护。

——测试评价方法：

a) 利用协议分析仪截取网络传输的用户数据，检测传输的用户数据是否按照开发者的设计进行保密性保护。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.7.3 客体安全重用

——测试评价内容：

见 4.5.1.3.7 c) 的内容。

——对开发者的要求：

开发者应提供文档，说明对安全支撑系统进行动态资源管理过程中，如何保证客体资源（包括子集信息、完全信息和特殊信息）中的剩余信息不应引起信息的泄漏。

——测试评价方法：

a） 检测系统对安全支撑系统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，是否会清除该客体中的原有信息；

b） 检测系统对安全支撑系统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，是否会清除该客体中的原有信息；

c） 在完全信息保护的基础上，对于某些需要特别保护的信息，检测系统是否能够采用专门的方法对客体资源中的残留信息做彻底清除。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.8 数据完整性保护

5.6.1.3.8.1 存储数据的完整性

——测试评价内容：

见 4.5.1.3.8 a）的内容。

——对开发者的要求：

开发者应提供文档，说明系统对基于用户属性的所有客体，如何对存储在 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，系统采取何种必要的恢复措施。

——测试评价方法：

a） 使用各种方法和工具，对安全支撑系统内部存储的数据，进行修改，检测系统能否检测出完整性错误；

b） 检测系统能否采取恢复措施，使数据恢复到修改前的状态。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.8.2 传输数据的完整性

——测试评价内容：

见 4.5.1.3.8 b）的内容。

——对开发者的要求：

开发者应提供文档，说明在 SSF 和其他可信信息系统间传输用户数据时，提供了哪些数据完整性检测的功能；并说明接收者如何恢复被破坏的数据为原始的用户数据。

——测试评价方法：

a） 使用各种方法和工具，对在 SSF 和其他可信信息系统间传输的用户数据，进行篡改、删除、插入等操作，检测系统能否检测出完整性错误；

b） 接收者尝试对被破坏的数据进行恢复，检测是否能够恢复为原始的用户数据。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.8.3 处理数据的完整性

——测试评价内容：

见 4.5.1.3.8 c）的内容。

——对开发者的要求：

开发者应提供文档，说明对终端计算机中处理中的数据采用何种方式保证处理数据的完整性。

——测试评价方法：

a) 根据开发者提供的文档,定制相关的 SSF 访问控制策略;

b) 选定一个终端计算机中处理中的数据为测试数据,对其进行一系列操作,检测系统能否对所进行的操作序列进行回退,并恢复数据为操作前的状态。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.9 安全审计

——测试评价内容:

见 4.5.1.3.9 的内容。

——对开发者的要求:

开发者应提供文档,说明安全支撑系统中生成、维护及保护审计数据过程,以及具备哪些保护措施。

——测试评价方法:

a) 查看系统的审计记录信息,检测是否有密码支持、系统身份标识与鉴别、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相关操作的审计记录;

b) 检测审计功能是否支持审计日志;

c) 当有安全侵害事件时,检测系统能否将审计数据记入审计日志;

d) 当有安全侵害事件时,检测系统能否生成实时报警信息;

e) 当有安全侵害事件时,检测系统能否将违例进程终止,违例进程可以包括但不限于服务进程、驱动、用户进程;

f) 当有安全侵害事件时,检测系统能否将当前的用户账号断开,并使其失效;

g) 对于内置于终端计算机的可信密码模块,检测能否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,并查看审计记录;检测是否提供给上层应用软件查询审计情况的接口;检测能否存储审计记录;

h) 检测审计记录是否包括: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;

i) 检测审计功能是否支持潜在侵害分析;检测系统能否用一系列规则去监控审计事件,并根据这些规则指出系统的潜在侵害;

j) 检测系统能否确立用户或进程的质疑度(或信誉度);当用户或进程的质疑等级超过门限条件时,检测系统能否发现并指出将要发生对安全性的威胁;

k) 检测系统是否提供系统行为记录与侵害的签名事件匹配的功能,检测系统能否通过对一个或多个事件的对比分析或综合分析,预测攻击出现的时间或方式;

l) 检测审计功能是否为授权用户提供基本审计查阅;检测系统是否提供审计查阅工具对审计数据进行搜索、分类、排序;以未授权用户身份,尝试查阅审计信息,检测系统是否拒绝未授权访问;

m) 检测审计功能是否支持根据客体身份、用户身份、主体身份、主机身份、事件类型等属性进行审计事件选择;

n) 在意外情况出现时,检测审计功能是否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,检测审计功能是否能够采取相应的保护措施,确保有实效性的审计记录不被破坏;

o) 根据开发者提供的文档,检测审计数据是否受到安全保护,尝试以未授权用户进行访问、修改和破坏审计信息,检测系统能否拒绝未授权访问;

p) 检测系统能否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。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.10 备份与故障恢复

——测试评价内容：

见 4.5.1.3.10 的内容。

——对开发者的要求：

开发者应提供文档，说明对用户数据和系统，如何在备份、存储和恢复过程中进行安全保护，以及具备哪些备份保护措施。

——测试评价方法：

a) 以用户身份有选择地备份重要数据的功能，对数据进行修改，然后进行恢复，检测能否有效恢复；

b) 对系统的运行现场进行定期备份，对系统数据进行修改，然后进行恢复，检测能否有效恢复；

c) 根据开发者提供的文档，检测数据在备份、存储和恢复过程中是否具有安全保护措施，是否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，用户操作系统是否不可访问系统备份数据。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.11 I/O 接口配置

——测试评价内容：

见 4.5.1.3.11 的内容。

——测试评价方法：

a) 以授权用户身份，在 BIOS 和操作系统中，分别启用串口、并口、USB、网卡、硬盘，检测能否正常使用；

b) 以授权用户身份，在 BIOS 和操作系统中，分别禁用串口、并口、USB、网卡、硬盘，检测能否使用；

c) 检测系统能否接受所接入网络的接口进行集中配置管理，尝试以未授权用户进行配置管理，检测系统能否拒绝未授权访问；

d) 检测系统能否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。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.1.3.12 可信时间戳

——测试评价内容：

见 4.5.1.3.12 的内容。

——对开发者的要求：

开发者应提供文档，说明系统如何提供可信的时间戳。

——测试评价方法：

a) 根据开发者提供的文档，检测系统是否提供可靠的时钟和时钟同步系统。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.2 SSOTC 自身安全保护

5.6.2.1 安全支撑系统的自身安全保护

——测试评价内容：

见 4.5.2.1 的内容。

——对开发者的要求：

开发者应提供文档，说明可信存储根是否设置在可信密码模块内，所采用的可信密码模块是否由国家主管机构研制，并提供该机构相应的资质证书；说明可信报告根是否设置在可信密码模块内，可信报告根所对应的公钥证书由哪家机构发行和管理，并提供该机构相应的资质证书；说明可信度量根是否设置在固件模块内，该模块的物理位置，以及计算机的启动过程，是否包含了该模块；说明动态可信度量根是否设置在自主虚拟机监控器内，以及对动态可信度量根采取了哪些保护措施；提供物理结构图，包括键盘输入信号路径，可信密码模块、物理开关位置等详细信息；说明采取何种方式对安全支撑系统的使用用户进行鉴别。

——测试评价方法：

a) 按照开发者提供的文档，检测可信存储根和可信报告根是否设置在可信密码模块内；

b) 按照开发者提供的文档和相关证书，检测所使用的密码模块是否通过国家主管机构测评认证；

c) 按照开发者提供的文档，并查看可信报告根的公钥证书及其发行机构相关证书，检验是否由国家专门权威机构发行和管理；

d) 查验文档是否符合要求，通过加载/卸载可信度量根，和其所在的固件模块，检验终端计算机启动是否依赖该固件和可信度量根；

e) 按照开发者提供的文档，检测是否对可信度量根采取物理保护措施，并且检测保护措施的有效性；

f) 按照开发者提供的文档，检测动态可信度量根是否设置在自主虚拟机监控器内；

g) 按照开发者提供的文档，检测是否对动态可信度量根采取物理保护措施，并且检测保护措施的有效性；

h) 查验开发者提供的物理结构图，检查是否有物理路径支持键盘输入与可信密码模块的直接通信，是否具有物理开关控制；

i) 打开机箱检验物理线路是否与图纸一致，分别打开、关闭控制开关，检验其是否有效；

j) 尝试以授权用户和非授权用户去使用可信密码模块，检验是否需要进行身份鉴别。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.2.2 操作系统的自身安全保护

——测试评价内容：

见 4.5.2.2 的内容。

——对开发者的要求：

开发者应提供第三方权威机构对该操作系统的检测报告，或者提供文档对 GB/T 20272—2006 中 4.5.2 的各个项目进行说明。

——测试评价方法：

a) 如果提供了第三方权威机构对该操作系统的检测报告，则查验报告，查看报告中对应项目检测结果是否符合；

b) 如果未能提供第三方权威机构对该操作系统的检测报告，则按照 GB/T 20272—2006 中4.5.2 的要求对操作系统的相关项目进行检测。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3 SSOTC 设计和实现

5.6.3.1 配置管理

5.6.3.1.1 配置管理能力

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.1 a）的要求，实现终端计算机第五级的配置管理能力设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a） 开发者所使用的版本号与所应表示的终端计算机样本应完全对应，没有歧义；

b） 配置管理系统应对所有的配置项作出唯一的标识；

c） 配置管理计划中，应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致；

d） 配置管理文档应提供所有的配置项得到有效地维护的证据；

e） 配置管理系统应确保对配置项只进行授权修改；

f） 配置管理系统应支持终端计算机的生成；

g） 验收计划应描述用来验收修改过的或新建的配置项的过程，将其作为终端计算机的一部分，并确认对配置项的任何生成和修改都是由授权者进行的；

h） 配置管理文档除应包括配置清单、配置管理计划外，还应包括一个验收计划和集成过程，集成过程应描述在终端计算机制作过程中如何使用配置管理系统；

i） 配置管理系统应要求将一个配置项接收到配置管理中的不是该配置项的开发者；

j） 配置管理系统应明确标识组成终端计算机安全功能的配置项；

k） 配置管理系统应支持所有对终端计算机修改的审计，至少应包括操纵者、日期、时间等信息；

l） 配置管理系统应有能力标明用于生成终端计算机主拷贝的所有材料；

m） 配置管理文档应阐明配置管理系统与开发安全方法相联系的使用，并只允许对终端计算机作授权的修改；

n） 配置管理文档应阐明集成过程的使用能够确保终端计算机的生成是以授权的方式正确进行的；

o） 配置管理文档应阐明配置管理系统足以确保负责将某配置项接收到配置管理中的不是该配置项的开发者；

p） 配置管理文档应能证明接收过程对所有配置项的修改都提供了充分而适当的复查。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.1.2 配置管理自动化

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.1 b）的要求，实现终端计算机第五级的配置管理自动化设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a） 配置管理系统应通过自动方式来确保终端计算机的实现表示只能进行已授权的变化，并能提供自动方式来支持终端计算机的生成；

b） 配置管理计划应描述配置管理系统中所使用的自动工具，并说明如何使用这些工具；

c） 配置管理系统应能自动确定终端计算机版本间的变化，并标识出哪个配置项会因其余配置项的修改而受到影响。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.1.3 配置管理范围

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.1 c) d) 的要求，实现终端计算机第五级的配置管理范围设计。

——测试评价方法：

a) 终端计算机配置管理范围，要求将终端计算机的实现表示、设计文档、测试文档、用户文档、安全管理员文档、配置管理文档等置于配置管理之下，从而确保它们的修改是在一个正确授权的可控方式下进行的。为此要求：
   1) 开发者所提供的配置管理文档应展示配置管理系统至少能跟踪上述配置管理之下的内容；
   2) 文档应描述配置管理系统是如何跟踪这些配置项的；
   3) 文档还应提供足够的信息表明达到所有要求；
b) 配置管理系统应对安全缺陷进行跟踪；
c) 配置管理系统应对开发工具和相关信息进行跟踪。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.2 分发和操作

5.6.3.2.1 分发

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.2 a) 的要求，实现终端计算机第五级的分发。

——测试评价方法：

a) 评估者应审查开发者是否按分发过程的要求，编制分发文档；
b) 评估者应审查分发文档，是否描述给用户分发终端计算机时，用以维护安全所必须的所有过程；
c) 评估者应审查是否按该过程进行分发；
d) 评估者应审查分发文档，是否描述检测修改的方法和技术，是否描述开发者的主拷贝与用户收到的版本之间的差异；
e) 评估者应审查分发文档，是否描述用来检测试图伪装成开发者向用户发送产品的方法；
f) 评估者应审查分发文档，是否在修改检测的基础上，还描述了如何防止修改的方法和技术。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.2.2 操作

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.2 b) 的要求，实现终端计算机第五级的操作。

——测试评价方法：

a) 评估者应审查操作文档，是否说明了终端计算机在开发者所期望的安全方式下进行安装、生成和启动的过程。用户能够通过此文档了解安装、生成和启动过程；
b) 评估者应审查操作文档，是否说明了将处于配置控制下的终端计算机的实现安全地转换为用户环境下的初始操作，并最终生成了安全的配置。用户能够通过此文档了解安装、生成、启动完成后，终端计算机在用户环境下生成的相应的安全配置情况；
c) 评估者应审查操作文档，是否说明了日志生成的要求(包括日志生成选项、生成时间及生成方

法等)和过程。用户能够通过此文档进行建立日志的过程。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.3 开发

5.6.3.3.1 功能设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.3 a) 的要求，实现终端计算机第五级的功能设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 功能设计应当使用形式化风格来描述终端计算机安全功能与其外部接口，必要时由非形式化、解释性的文字来支持；

b) 功能设计应当是内在一致的；

c) 功能设计应当描述使用所有外部终端计算机安全功能接口的目的与方法，适当的时候，要提供结果影响例外情况和错误信息的细节；

d) 开发者应完备地表示终端计算机安全功能的基本原理。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.3.2 安全策略模型

——测试评价内容：

应按 GB/T20271—2006 中 6.5.5.3 b) 的要求，实现终端计算机第五级的安全策略模型设计。

——测试评价方法：

评估者应审查开发者所提供的文档中，安全策略模型的相关内容，是否满足如下要求：

a) SSP 模型应是形式化的，并描述所有可以模型化的 SSP 策略的规则与特征；

b) SSP 模型应包括一个基本原理，阐明该模型与所有可模型化的 SSP 策略是一致的、完备的；

c) SSP 模型和功能设计之间的对应性阐明应说明功能设计中的安全功能与 SSP 模型是一致的、完备的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.3.3 高层设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.3 c) 的要求，实现终端计算机第五级的高层设计。

——测试评价方法：

评估者应审查开发者所提供的高层设计文档是否满足如下要求：

a) 以子系统的观点、以半形式化的方法来一致性地描述终端计算机的体系结构；

b) 描述每一个子系统所提供的安全功能及其相互关系；

c) 标识安全功能要求的任何基础性的硬件、固件和/或软件，并且通过这些硬件、固件和/或软件所实现的保护机制，来提供安全功能功能；

d) 标识安全功能子系统的所有接口，并标明安全功能子系统的哪些接口是外部可见的；

e) 高层设计文档应当描述安全功能子系统所有接口的使用目的与方法，并提供例外情况和错误信息的细节；

f) 高层设计文档应当描述如何将终端计算机分离成安全策略加强单元和其他子系统；

g) 高层设计文档应当描述所提供的 SSP 模型是否是形式化的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.3.4 低层设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.3 d) 的要求，实现终端计算机第五级的低层设计。

——测试评价方法：

评估者应审查开发者所提供的低层设计文档是否满足如下要求：

a) 低层设计的表示应是形式化的，内在一致的，并以模块术语描述，必要时提供所有结果的完备细节、例外情况和错误信息；

b) 描述每一个模块的目的；

c) 以所提供的安全功能和对其他模块的依赖性术语定义模块间的相互关系；

d) 描述如何提供每一个安全策略功能的实施；

e) 标识终端计算机安全功能模块的所有接口，标识终端计算机安全功能模块的哪些接口是外部可见的，以及描述终端计算机安全功能模块所有接口的目的与方法，必要时，应提供影响、例外情况和错误信息的细节；

f) 描述如何将终端计算机分离成安全策略实施模块和其他模块。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.3.5 内部结构设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.3 e) 的要求，实现终端计算机第五级的内部结构设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 应以模块化方法设计和构建终端计算机安全功能，并避免设计模块之间出现不必要的交互；

b) 标识终端计算机安全功能模块，并应描述每一个终端计算机安全功能模块的目的、接口、参数和影响；

c) 描述终端计算机安全功能设计是如何使独立的模块间避免不必要的交互作用；

d) 在设计和构建安全功能时，应使安全功能局部的复杂度最小化，以加强访问控制策略；

e) 标识安全功能模块，并应指明安全功能的哪些部分是加强安全策略的；

f) 描述分层结构，并说明如何使交互作用最小化；

g) 描述加安全策略的安全功能部分是如何被构建的，从而使其复杂性降低；

h) 描述在设计和构建 SSF 时，如何保证实施任何安全策略的 SSF 部分简单且易分析；

i) 描述那些与 SSF 无关的功能是否已从 SSF 中排斥出去。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.3.6 实现表示

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.3 f) 的要求，实现终端计算机第五级的实现表示设计。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 应无歧义地为全部终端计算机安全功能，定义一个详细级别的终端计算机安全功能实现表示，并且实现表示应当是内在一致的；

b) 所定义的实现表示应是结构精简的，且易于理解。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.3.7 对应性设计

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.3 g）的要求，实现终端计算机第五级的对应性设计。

——测试评价方法：

评估者应审查开发者所提供的文档信息中，对应性设计的相关内容，是否满足如下要求：

a） 应在所提供的终端计算机安全功能表示的所有相邻对之间提供其对应性分析，对每个相邻对，应当阐明较为抽象的终端计算机安全功能表示的所有相关安全功能在较不抽象的终端计算机安全功能表示中得到正确而完备地细化；

b） 对那些形式化规定的表示的相应部分，应给出其对应性证明；

c） 对所提供的 SSF 表示的每个相邻对，当其中一个表示是半形式化规定，而另一个表示至少是半形式化规定时，应当阐明表示部分之间的对应性说明是否也是半形式化的；

d） 对于所提供的 SSF 表示的每个相邻对，如果两者的各部分都是形式化规定的，应当阐明表示部分之间的对应性的说明是否也是形式化的。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.4 文档要求

5.6.3.4.1 管理员指南

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.4 的要求，实现终端计算机第五级的管理员指南。

——测试评价方法：

评估者应审查开发者是否提供了供系统管理员使用的管理员指南，并且此管理员指南是否包括如下内容：

a） 终端计算机可以使用的管理功能和接口；

b） 怎样安全地管理终端计算机；

c） 在安全处理环境中应进行控制的功能和权限；

d） 所有对与终端计算机的安全操作有关的用户行为的假设；

e） 所有受管理员控制的安全参数，如果可能，应指明安全值；

f） 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g） 所有与系统管理员有关的 IT 环境的安全要求。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.4.2 用户指南

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.4 的要求，实现终端计算机第五级的用户指南。

——测试评价方法：

评估者应审查开发者是否提供了供系统用户使用的用户指南，并且此用户指南是否包括如下内容：

a） 终端计算机的非管理用户可使用的安全功能和接口；

b） 终端计算机提供给用户的安全功能和接口的用法；

c） 用户可获取但应受安全处理环境控制的所有功能和权限；

d) 终端计算机安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.5 生存周期支持

5.6.3.5.1 开发安全

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.5 a) 的要求，实现终端计算机第五级的开发安全。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 开发人员的安全管理：开发人员的安全规章制度，开发人员的安全教育培训制度和记录；

b) 开发环境的安全管理：开发地点的出入口控制制度和记录，开发环境的温室度要求和记录，开发环境的防火防盗措施和国家有关部门的许可文件，开发环境中所使用安全产品必须采用符合国家有关规定的产品并提供相应证明材料；

c) 开发设备的安全管理：开发设备的安全管理制度，包括开发主机使用管理和记录，设备的购置、修理、处置的制度和记录，上网管理，计算机病毒管理和记录等；

d) 开发过程和成果的安全管理：对产品代码、文档、样机进行受控管理的制度和记录，若代码和文档进行加密保护必须采用符合国家有关规定的产品并提供相应证明材料；

e) 开发安全文件中所提供的安全措施的证据应能证明安全措施对维护终端计算机的安全性提供了必要的保护。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.5.2 缺陷纠正

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.5 b) 的要求，实现终端计算机第五级的缺陷纠正。

——测试评价方法：

评估者应审查开发者所提供的生存周期定义文档中是否完全符合以下要求：

a) 描述用以跟踪所有终端计算机版本里已被报告的安全缺陷的过程；

b) 描述所提供的每个安全缺陷的性质和效果，以及缺陷纠正的情况；

c) 标识每个安全缺陷所采取的纠正措施；

d) 描述为终端计算机用户的纠正行为所提供的信息，纠正和指导的方法；

e) 提供缺陷报告。缺陷报告应：

1) 记录缺陷纠正的过程，并制定用户接受安全缺陷报告和纠正这些缺陷的要求的措施；

2) 描述用以跟踪所有 SSOTC 版本里已报告的安全缺陷的过程；

3) 确保已报告的安全缺陷处理过程的所有已知缺陷都已被纠正，并将纠正办法告知用户；

4) 确保已报告的安全缺陷处理过程所提供的防范机制为纠正这些安全缺陷所引进的纠正方法不会带来新的缺陷；

f) 应为用户有关终端计算机的安全问题的报告和查询指明一个或多个特别联系点，负责及时将安全缺陷报告及其相应的纠正方法自动分发给可能受到这种安全缺陷影响的注册用户。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.5.3 生存周期定义

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.5 c) 的要求，实现终端计算机第五级的生存周期定义。

——测试评价方法：

评估者应审查开发者所提供的生存周期定义文档中是否完全符合以下要求：

a) 开发者应建立标准化的、可测量的、用于开发和维护终端计算机的生存周期模型；

b) 可测量的生存周期模型应带有算术参数和/或测量终端计算机开发特性的度量（例如源码复杂性度量）；

c) 该模型应对终端计算机开发和维护提供必要的控制；

d) 开发者所提供的生存周期定义文档应描述用于开发和维护终端计算机的模型，解释选择该模型的原因，解释如何用该模型来开发和维护终端计算机，阐明与标准化的可测量的生存周期模型的相符性，以及提供利用标准化的可测量的生存周期模型来进行终端计算机开发的测量结果。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.5.4 工具和技术

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.5 d) 的要求，确定终端计算机第五级的工具和技术。

——测试评价方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 开发者应标识用于开发终端计算机的工具，并且所有用于实现的开发工具都应有明确定义。开发者应文档化已选择的依赖实现的开发工具的选项，开发工具文档应明确定义实现中每个语句的含义，以及明确定义所有基于实现的选项的含义；

b) 开发者应对终端计算机所有部分的实现标准进行描述。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.6 测试

5.6.3.6.1 测试范围

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.6 a) 的要求，确定终端计算机第五级的测试范围。

——测试评价方法：

a) 评估者应审查开发者提供的测试覆盖分析结果，是否表明了测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的；

b) 评价测试文档中已标识的测试是否包括了安全功能设计描述中所有安全功能的测试，是否都经过了完整性测试；

c) 评估者应审查测试文档，是否覆盖了在功能设计描述中的所有安全功能；

d) 开发者所提供的范围分析应表明测试文档所标识的测试与功能设计所描述的安全功能之间的对应性；

e) 测试范围的分析应阐明功能设计所描述的安全功能和测试文档所标识的测试之间的对应性是完备的；

f) 测试范围的分析应严格地阐明功能设计所标识的安全功能的所有外部接口已经被完备测试过了。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.6.2 测试深度

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.6 b）的要求，确定终端计算机第五级的测试深度。

——测试评价方法：

a） 评价开发者提供的测试深度分析，是否说明了测试文档中所标识的对安全功能的测试，足以表明该安全功能与高层设计和低层设计是一致的；

b） 开发者所提供的测试深度分析应阐明测试文档中所标识的测试足以表明该安全功能是根据高层设计、低层设计和实现表示而运作的。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.6.3 功能测试

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.6 c）的要求，实现终端计算机第五级的功能测试。

——测试评价方法：

a） 评价开发者提供的测试文档，是否包含测试计划、测试规程、预期的测试结果和实际测试结果；

b） 评价测试计划是否标识了要测试的安全功能，是否描述了测试的目标；

c） 评价测试规程是否标识了要执行的测试，是否描述了每个安全功能的测试概况（这些概况包括对其他测试结果的顺序依赖性）；

d） 评价期望的测试结果是否表明测试成功后的预期输出；

e） 评价实际测试结果是否表明每个被测试的安全功能能按照规定进行运作；

f） 评价测试文档是否包含测试过程中对顺序依赖性的分析。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.6.4 独立性测试

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.6 d）的要求，实现终端计算机第五级的独立性测试。

——测试评价方法：

a） 开发者提供的测试文档，应表明安全功能是按规定运作的；

b） 开发者应提供与测试相适应的终端计算机；

c） 通过重复所有开发者的测试，检查测试文档的正确性和完备性。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.7 脆弱性评定

5.6.3.7.1 隐蔽信道分析

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.7 a）的要求，实现网络第五级的隐蔽信道分析设计。

评估者应审查开发者提供的文档中，隐蔽信道分析的相关内容，是否满足了以下要求：

a） 描述如何通过对隐蔽存储信道的严格搜索，以结构化、可重复的方式标识出隐蔽信道，并估算它们的带宽；

b） 描述用于确定隐蔽信道存在的过程，以及进行隐蔽信道分析所需要的信息；

c） 描述隐蔽信道分析期间所作的全部假设；

d) 描述最坏情况下对隐蔽信道带宽进行估算的方法；

e) 描述每个可标识的隐蔽信道的最大可利用情形；

f) 描述用封锁和/或限制带宽和/或审计等，对所标识的隐蔽信道进行处理的措施。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.7.2 防止误用

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.7 b) 的要求，实现网络第五级的防止误用设计。

——测试评价方法：

评估者应审查开发者提供的文档，是否满足了以下要求：

a) 评价指南性文档，是否确定了对终端计算机的所有可能的操作方式(包括失败和操作失误后的操作)，是否确定了它们的后果，以及是否确定了对于保持安全操作的意义；

b) 评价指南性文档，是否列出了所有目标环境的假设以及所有外部安全措施(包括外部程序的、物理的或人员的控制)的要求；

c) 评价指南性文档是否完整、清晰、一致、合理；

d) 评价开发者提供的分析文档，是否阐明指南性文档是完整的；

e) 评估者应进行独立验证，以确定安全管理员或用户在正确理解文档的情况下能基本判断 SSOTC 是否在不安全状态下配置或运行。

记录审查结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.7.3 安全功能强度评估

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.7 c) 的要求，实现网络第五级的安全功能强度评估设计。

——测试评价方法：

评估者应审查开发者提供的文档，是否满足了以下要求：

a) 通过对安全机制的安全行为的合格性或统计结果的分析，以及对克服脆弱性所付出努力的分析，得到终端计算机安全功能强度的说明；

b) 对安全目标中标识的每个具有安全功能强度声明的安全机制，进行安全功能强度的分析，证明该机制达到或超过安全目标要求所定义的最低强度，并证明该机制达到或超过安全目标要求所定义的特定功能强度。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

5.6.3.7.4 脆弱性分析

——测试评价内容：

应按 GB/T 20271—2006 中 6.5.5.7 d) 的要求，实现网络第五级的脆弱性分析设计。

——测试评价方法：

a) 评价开发者提供的脆弱性分析文档，是否从用户可能破坏安全策略的明显途径出发，对终端计算机的各种功能进行了分析；

b) 对被确定的脆弱性，评价开发者是否明确记录了采取的措施；

c) 对每一条脆弱性，评价是否有证据显示在使用终端计算机的环境中该脆弱性不能被利用；

d) 评价所提供的文档，是否表明经过标识脆弱性的终端计算机可以抵御明显的穿透性攻击；

e) 实施独立的穿透性测试，检测终端计算机能否抵御低攻击能力攻击者发起的攻击；

f) 评价开发者提供的分析文档，是否完备地表述了 SSOTC 的脆弱性，并确定终端计算机能否抵

御高攻击能力攻击者发起的对 SSOTC 的穿透性攻击。

记录测试结果并对该结果是否完全符合上述测试评价方法要求作出判断。

参 考 文 献

[1] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

[2] GB/T 21028—2007 信息安全技术 服务器安全技术要求

[3] GB/T 20281—2006 信息安全技术 防火墙技术要求和测试评价方法

[4] GB/T 20275—2006 信息安全技术 入侵检测系统技术要求和测试评价方法

[5] 可信计算密码支撑平台功能与接口规范.国家密码管理局 2007年12月颁布

[6] GB/T 18336.1—2008 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

[7] GB/T 18336.2—2008 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

[8] GB/T 18336.3—2008 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

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

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 终端计算机
通用安全技术要求与测试评价方法
GB/T 29240—2012
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100013)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:010-51780168
010-68522006
2013 年 5 月第一版
*
书号:155066·1-46984

GB/T 29240-2012