ICS 35.040
A 90

GA

中华人民共和国公共安全行业标准

GA/T 672—2006

信息安全技术
终端计算机系统安全等级评估准则

**Information security technology—
Evaluation criteria for terminal computer system
of security classified protection**

2006-12-28 发布　　2007-02-01 实施

中华人民共和国公安部　发布

目　　次

前　言

本标准由公安部信息系统安全标准化技术委员会提出。

本标准由全国信息安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心。

本标准主要起草人：邱梓华、顾健、景乾元、李毅、沈亮、张奕、邹春明、马海燕、俞优。

引　言

本标准用以指导评估者如何评估各安全等级的终端计算机系统。

终端计算机系统在计算机信息系统中，承担着大量数据存储、处理、传输的工作，与用户有着最紧密的联系。终端计算机系统的安全，对整个信息系统的安全，起着至关重要的作用。在各个安全等级的信息系统中，终端计算机系统也应该达到相应的安全等级。

本标准依据《信息安全技术　终端计算机系统安全等级技术要求》的相关要求，对第一、第二和第三级的终端计算机系统提出了具体的评估方法，能够对终端计算机系统的测试、开发提供指导。

信息安全技术
终端计算机系统安全等级评估准则

1 范围

本标准规定了终端计算机系统的评估方法。

本标准适用于按照GA/T 671—2006《信息安全技术 终端计算机系统安全等级技术要求》所开发的终端计算机系统的评估。

2 规范性引用文件

下列文件中的条款通过在本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 20272—2006 信息安全技术 操作系统安全技术要求

GA/T 671—2006 信息安全技术 终端计算机系统安全等级技术要求

3 术语、定义和缩略语

3.1 术语和定义

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

3.1.1

终端计算机系统 terminal computer system

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

3.1.2

可信 trusted

一种特性，具有该特性的实体总是以预期的行为和方式达到既定目的。

3.1.3

完整性度量(简称度量) measurement of integrity

一种使用密码学杂凑算法对实体计算其杂凑值的过程。

3.1.4

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

实体在可信状态下度量得到的杂凑值，可用来作为完整性校验基准。

3.1.5

度量根 root of trust for measurement

一个可信的实体，是终端计算机系统内进行可信度量的基点。

3.1.6

动态度量根　dynamic root of trust for measurement

度量根的一种，支持终端计算机系统对动态启动的程序模块进行实时可信度量。

3.1.7

存储根　root of trust for storage

一个可信的实体，是终端计算机系统内进行可信存储的基点。

3.1.8

报告根　root of trust for reporting

一个可信的实体，是终端计算机系统内进行可信报告的基点。

3.1.9

可信根　trusted root

度量根、存储根和报告根的集合，是保证终端计算机系统可信的基础。

3.1.10

可信硬件模块　trusted hardware module

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

3.1.11

信任链　trusted chains

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

3.1.12

可信计算平台　trusted computing platform

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

3.1.13

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

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

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

3.1.14

SSOTCS 安全功能　SSOTCS security function

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

3.1.15

SSOTCS 安全控制范围　SSOTCS scope of control

SSOTCS 的操作所涉及的主体和客体。

3.1.16

SSOTCS 安全策略　SSOTCS security policy

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

3.2　缩略语

下列缩略语适用于本标准：

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

4　信息安全技术　终端计算机系统安全等级评估准则

4.1　第一级：用户自主保护级

4.1.1　安全功能要求

4.1.1.1　物理系统

4.1.1.1.1　设备安全可用

评估内容：

见 GA/T 671—2006 中 5.1.1.1.1 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机系统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。

评估方法：

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系统的基本运行；

b）　按照开发者提供的文档，模拟出现一些故障事件（如：调电、硬件故障等），验证终端计算机系统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评估方法要求作出判断。

4.1.1.1.2　设备防盗防毁

评估内容：

见 GA/T 671—2006 中 5.1.1.1.2 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机系统的设备具有哪些无法除去的标记。

评估方法：

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评估方法要求作出判断。

4.1.1.2　可信计算平台

4.1.1.2.1　密码支持

评估内容：

见 GA/T 671—2006 中 5.1.1.3.1 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。

评估方法：

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；

b）　检测公钥密码算法、对称密码算法、杂凑算法和随机数生成器算法，是采用软件实现，还是采用硬件实现。如果硬件支持插拔，将硬件拔出，检测能否进行相关密码操作；

c）　按照开发者提供的文档，检测所有密钥是否受存储根保护。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.1.1.2.2 信任链

评估内容：

见 GA/T 671—2006 中 5.1.1.3.2 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机系统如何在系统启动过程中，对 BIOS、MBR、OS 等部件进行完整性度量，并说明完整性度量值是否存储在一个受保护的区域中。

评估方法：

a) 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；

b) 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；

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

d) 使用各种方法和工具，对存储的完整性度量值进行篡改和破坏，检测系统能否保护完整性度量值。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.1.1.2.3 运行时防护

评估内容：

见 GA/T 671—2006 中 5.1.1.3.3 的内容。

评估方法：

a) 在系统中植入一个测试用的恶意代码，并运行恶意代码；

b) 对文件系统和内存进行扫描，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评估方法要求作出判断。

4.1.1.2.4 系统安全性检测分析

评估内容：

见 GA/T 671—2006 中 5.1.1.3.4 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机是否经过操作系统安全性检测分析，并且提供相应的检测分析报告。

评估方法：

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；

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。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.1.1.2.5 备份与故障恢复

评估内容：

见 GA/T 671—2006 中 5.1.1.3.5 的内容。

评估方法：

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) 对系统定时进行增量备份，对系统数据进行修改，然后进行恢复，检测能否有效恢复。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.1.1.2.6 I/O 接口配置

评估内容：

见 GA/T 671—2006 中 5.1.1.3.6 的内容。

评估方法：

a) 以用户身份，在 BIOS 和操作系统中，分别启用串口、并口、PCI、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，分别禁用串口、并口、PCI、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评估方法要求作出判断。

4.1.2 SSOTCS 自身安全保护

4.1.2.1 可信根安全保护

评估内容：

见 GA/T 671—2006 中 5.1.2.1 a)的内容。

对开发者的要求：

开发者应提供文档，说明采取哪些保护措施，以防止存储根和报告根的泄漏和窜改，说明是否对度量根采取物理保护措施。

评估方法：

a) 以各种方法和工具，尝试读取、修改存储根和报告根，检测能否尝试成功；

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

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.1.3 SSOTCS 设计和实现

4.1.3.1 配置管理

评估内容：

见 GB/T 20271—2006 中 6.1.5.1 的内容。

评估方法：

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：

开发者所使用的版本号与所应表示的终端计算机系统样本应完全对应，没有歧义。

记录审查结果并对该结果是否完全符合上述评估方法要求作出判断。

4.1.3.2 分发和操作

4.1.3.2.1 分发

评估内容：

见 GB/T 20271—2006 中 6.1.5.2 a)的内容。

评估方法：

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系统时，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评估方法要求作出判断。

4.1.3.2.2 操作

评估内容：

见 GB/T 20271—2006 中 6.1.5.2 b)的内容。

评估方法：

a) 评估者应审查操作文档，是否说明了终端计算机系统的安装、生成、启动和使用的过程；

b) 用户应能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评估方法要求作出判断。

4.1.3.3 开发

4.1.3.3.1 功能设计

评估内容：

见 GB/T 20271—2006 中 6.1.5.3 a)的内容。

评估方法：

评估者应审查开发者所提供的信息是否满足如下要求：

a) 功能设计应使用非形式化风格来描述终端计算机系统安全功能与其外部接口；

b) 功能设计应是内在一致的；

c) 功能设计应描述使用所有外部终端计算机系统安全功能接口的目的与方法，适当的时候，应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评估方法要求作出判断。

4.1.3.3.2 高层设计

评估内容：

见 GB/T 20271—2006 中 6.1.5.3 b)的内容。

评估方法：

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系统的体系结构；

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；

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评估方法要求作出判断。

4.1.3.3.3 低层设计

评估内容：

见 GB/T 20271—2006 中 6.1.5.3 c)的内容。

评估方法：

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) 标识终端计算机系统安全功能模块的所有接口，标识终端计算机系统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系统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系统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评估方法要求作出判断。

4.1.3.3.4 内部结构设计

评估内容：

见 GB/T 20271—2006 中 6.1.5.3 d)的内容。

评估方法：

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系统安全功能，并避免设计模块之间出现不必要的交互；

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

c) 描述终端计算机系统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评估方法要求作出判断。

4.1.3.3.5 实现表示设计

评估内容：

见 GB/T 20271—2006 中 6.1.5.3 e)的内容。

评估方法：

评估者应审查开发者所提供的信息是否满足如下要求：

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

记录审查结果并对该结果是否完全符合上述评估方法要求作出判断。

4.1.3.3.6 对应性设计

评估内容：

见 GB/T 20271—2006 中 6.1.5.3 f)的内容。

评估方法：

评估者应审查开发者所提供的信息是否满足如下要求：

应在所提供的终端计算机系统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，应阐明较为抽象的终端计算机系统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系统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评估方法要求作出判断。

4.1.3.4 文档要求

4.1.3.4.1 管理员指南

评估内容：

见 GB/T 20271—2006 中 6.1.5.4 的内容。

评估方法：

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) 终端计算机系统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系统；

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系统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评估方法要求作出判断。

4.1.3.4.2 用户指南

评估内容：

见 GB/T 20271—2006 中 6.1.5.4 的内容。

评估方法：

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) 终端计算机系统的非管理用户可使用的安全功能和接口；

b) 终端计算机系统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) 终端计算机系统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评估方法要求作出判断。

4.1.3.5 生存周期支持

评估内容：

见 GB/T 20271—2006 中 6.1.5.5 的内容。

评估方法：

评估者应审查开发者所提供的信息是否满足如下要求：

开发者应建立用于开发和维护终端计算机系统的生存周期模型，对终端计算机系统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系统的模型。

记录审查结果并对该结果是否完全符合上述评估方法要求作出判断。

4.1.3.6 测试

4.1.3.6.1 功能测试

评估内容：

见 GB/T 20271—2006 中 6.1.5.6 a)的内容。

评估方法：

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评估方法要求作出判断。

4.1.3.6.2 独立性测试

评估内容：

见 GB/T 20271—2006 中 6.1.5.6 b)的内容。

评估方法：

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系统。

记录审查结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2 第二级：系统审计保护级

4.2.1 安全功能要求

4.2.1.1 物理系统

4.2.1.1.1 设备安全可用

评估内容：

见 GA/T 671—2006 中 5.2.1.1.1 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机系统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。

评估方法：

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系统的基本运行；

b) 按照开发者提供的文档，模拟出现一些故障事件（如：调电、硬件故障等），验证终端计算机系统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评估方法要求作出判断。

4.2.1.1.2 设备防盗防毁

评估内容：

见 GA/T 671—2006 中 5.2.1.1.2 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机系统的设备具有哪些无法除去的标记。

评估方法：

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) 检测终端计算机系统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评估方法要求作出判断。

4.2.1.2 可信计算平台

4.2.1.2.1 密码支持

评估内容：

见 GA/T 671—2006 中 5.2.1.3.1 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。

评估方法：

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；

b) 检测公钥密码算法、对称密码算法、杂凑算法和随机数生成器算法，是采用软件实现，还是采用硬件实现。如果硬件支持插拔，将硬件拔出，检测能否进行相关密码操作；

c) 按照开发者提供的文档，检测所有密钥是否受存储根保护。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.1.2.2 信任链

评估内容：

见 GA/T 671—2006 中 5.2.1.3.2 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机系统如何在系统启动过程中，对 BIOS、MBR、OS 等部件进行完整性度量，并说明完整性度量值是否存储在一个受保护的区域中。

评估方法：

a) 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；

b) 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；

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

d) 使用各种方法和工具，对存储的完整性度量值进行篡改和破坏，检测系统能否保护完整性度量值。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.1.2.3 运行时防护

评估内容：

见 GA/T 671—2006 中 5.2.1.3.3 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机系统具有哪些运行时防护功能。

评估方法：

a) 在系统中植入一个测试用的恶意代码，并运行恶意代码；

b) 对文件系统和内存进行扫描，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) 网络协议分析：根据网络协议类型（协议类型如：HTTP、FTP、SMTP、POP3、TELNET、NNTP 等），制定拒绝通过的过滤规则，模拟访问相应的应用协议，检测能否拒绝访问；制定允许某些协议的过滤规则，模拟访问相应的应用协议，检测能否正常访问；

f) 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；

g) 内容过滤：对某些关键词设置相应的过滤规则，访问包含所设置关键词的网页，检测能否正常过滤。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.1.2.4 系统安全性检测分析

评估内容：

见 GA/T 671—2006 中 5.2.1.3.4 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，并且提供相应的检测分析报告。

评估方法：

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；

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。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.1.2.5 信任服务

评估内容：

见 GA/T 671—2006 中 5.2.1.3.5 的内容。

对开发者的要求：

开发者应提供文档，说明如何在可信硬件模块中，专门设置受保护区域来存储所有完整性度量值。

评估方法：

a) 按照开发者提供的文档，检测系统是否在可信硬件模块中，专门设置受保护区域存储所有完整性度量值；

b) 尝试以各种方法篡改完整性度量值，检测能否防止篡改。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.1.2.6 用户身份标识与鉴别

评估内容：

见 GA/T 671—2006 中 5.2.1.3.6 的内容。

评估方法：

a) 在安全功能实施所要求的动作之前，检测系统能否先对提出该动作要求的用户进行标识，并进行鉴别，只有鉴别成功后才运行进行相关操作；

b) 创建一个用户，并赋予其一些权限，然后删除此用户，再创建一个新的同名用户，检测新的用户是否具有老用户的权限；

c) 查看审计记录，检测审计信息中是否记录了用户的唯一性标识；

d) 尝试以各种非授权方式访问、修改或删除身份标识信息，检测能否防止不被非授权地访问、修改或删除；

e) 检测系统能否支持以数字证书形式提供鉴别信息，如果支持，使用用户数字证书登录系统，检测能否登录成功；

f) 用户以伪造的鉴别数据进行鉴别，检测系统能否检测出并拒绝用户鉴别；

g) 用户以从其他用户处复制的鉴别数据进行鉴别，检测系统能否检测出并拒绝用户鉴别；

h) 以错误的用户名-口令登录，在一定次数的鉴别失败后，测试系统是否终止了进行登录尝试主机建立会话的过程。分别以授权管理员和普通用户的身份登录，测试系统是否提供最多失败次数的设定功能，且最多失败次数仅由授权管理员设定；

i) 以用户身份登录系统，要求安全功能完成某个任务，从而激活另一个主体(如进程)，检测系统是否将该用户与该主体相关联，查看相应的审计记录，检测审计信息中是否记录了用户的身份。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.1.2.7 自主访问控制

评估内容：

见 GA/T 671—2006 中 5.2.1.3.7 的内容。

对开发者的要求：

开发者应提供文档，明确指出终端计算机系统自主访问控制的客体和主体，并说明自主访问控制的范围、策略和粒度。

评估方法：

a) 根据开发者提供的文档，以主体身份对客体添加一条自主访问控制策略，策略为拒绝其他主体的访问；以其他主体身份访问客体，检测能否访问成功；

b) 以主体身份对客体添加一条自主访问控制策略，策略为允许指定主体的访问；以授权主体身份访问客体，检测能否访问成功；以非授权主体身份访问客体，检测能否访问成功。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.1.2.8 数据保密性保护

4.2.1.2.8.1 数据存储保密性

评估内容：

见 GA/T 671—2006 中 5.2.1.3.8 a)的内容。

对开发者的要求：

开发者应提供文档，说明如何基于存储根实现对数据的保密存储，描述是否支持在特定终端计算机系统的特定状态下解密。

评估方法：

a) 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) 尝试以其他用户身份对数据进行解密，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评估方法要求作出判断。

4.2.1.2.8.2 数据传输保密性

评估内容：

见 GA/T 671—2006 中 5.2.1.3.8 b)的内容。

对开发者的要求：

开发者应提供文档，说明如何对传输的用户数据，进行保密性保护。

评估方法：

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评估方法要求作出判断。

4.2.1.2.9 数据完整性保护

4.2.1.2.9.1 存储数据的完整性

评估内容：

见 GA/T 671—2006 中 5.2.1.3.9 的内容。

对开发者的要求：

开发者应提供文档，说明对可信计算平台内部存储的数据，采取了哪些数据完整性保护措施。

评估方法：

a) 使用各种方法和工具，对可信计算平台内部存储的数据，进行修改，检测系统能否检测出完整性错误，能否采取恢复措施；

b) 对照原始数据和恢复后的数据，检测能否完全恢复全部数据。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.1.2.9.2 传输数据的完整性

评估内容：

见 GA/T 671—2006 中 5.2.1.3.9 的内容。

对开发者的要求：

开发者应提供文档，说明对可信信息系统间传输的用户数据，采取了哪些数据完整性保护措施，选择哪种恢复措施：

——由接收者 SSOTCS 借助于源可信信息系统提供的信息；

——由接收者 SSOTCS 自己无须来自源可信信息系统的任何帮助，来恢复被破坏的数据为原始的用户数据。

评估方法：

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

b) 按照开发者提供的文档，检测能否对检测出的完整性错误进行恢复，并检测恢复措施的有效性。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.1.2.9.3 处理数据的完整性

评估内容：

见 GA/T 671—2006 中 5.2.1.3.9 的内容。

对开发者的要求：

开发者应提供文档，说明具体的回退措施。

评估方法：

a) 记录当前系统的各种状态；

b) 进行一些操作，然后对这些操作进行回退，检测系统能否回退到以前的状态。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.1.2.10 安全审计

评估内容：

见 GA/T 671—2006 中 5.2.1.3.10 的内容。

评估方法：

a) 查看系统的审计记录信息，检测是否有密码支持、身份标识与鉴别、自主访问控制、数据保密性保护、用户数据完整性保护、信任服务等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、实时报警生成和违例进程终止；

c) 检测审计功能是否支持潜在侵害分析和基于异常检测；

d) 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；

e) 检测审计信息是否受到安全保护，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评估方法要求作出判断。

4.2.1.2.11 备份与故障恢复

评估内容：

见 GA/T 671—2006 中 5.2.1.3.11 的内容。

对开发者的要求：

开发者应提供文档，说明对用户数据和局部系统，如何在备份、存储和恢复过程中进行安全保护。

评估方法：

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) 对系统定时进行增量备份，对系统数据进行修改，然后进行恢复，检测能否有效恢复；

c) 对局部系统进行定期备份，对系统数据进行修改，然后进行恢复，检测能否有效恢复。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.1.2.12 I/O 接口配置

评估内容：

见 GA/T 671—2006 中 5.2.1.3.12 的内容。

评估方法：

a) 以用户身份，在 BIOS 和操作系统中，分别启用串口、并口、PCI、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，分别禁用串口、并口、PCI、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评估方法要求作出判断。

4.2.2 SSOTCS 自身安全保护

4.2.2.1 可信根安全保护

评估内容：

见 GA/T 671—2006 中 5.2.2.1 a)的内容。

对开发者的要求：

开发者应提供文档，说明存储根和报告根，是否设置在可信硬件模块内，是否对度量根采取物理保护措施。

评估方法：

a) 按照开发者提供的文档，检测存储根和报告根是否设置在可信硬件模块内；

b) 以各种方法和工具，尝试读取、修改存储根和报告根，检测能否尝试成功；

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

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.2.2 安全功能运行安全保护

评估内容：

见 GA/T 671—2006 中 5.2.2.1 c)的内容。

评估方法：

a) 使终端计算机系统进入休眠状态，然后使系统退出休眠状态，检测系统能否恢复到退出工作状态前的配置，并且检测信任链系统能否正常工作；

b) 使终端计算机系统进入待机状态，然后使系统退出待机状态，检测系统能否恢复到退出工作状态前的配置，并且检测信任链系统能否正常工作。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.3 SSOTCS 设计和实现

4.2.3.1 配置管理

4.2.3.1.1 配置管理能力

评估内容：

见 GB/T 20271—2006 中 6.2.5.1 a)的内容。

评估方法：

评估者应审查开发者所提供的信息是否满足如下要求：

开发者所使用的版本号与所应表示的终端计算机系统样本应完全对应，没有歧义。

记录审查结果并对该结果是否完全符合上述评估方法要求作出判断。

4.2.3.1.2 配置管理范围

评估内容：

见 GB/T 20271—2006 中 6.2.5.1 b)的内容。

评估方法：

终端计算机系统配置管理范围，要求将终端计算机系统的实现表示、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评估方法要求作出判断。

4.2.3.2 分发和操作

4.2.3.2.1 分发

评估内容：

见 GB/T 20271—2006 中 6.2.5.2 a)的内容。

评估方法：

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系统时，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评估方法要求作出判断。

4.2.3.2.2 操作

评估内容：

见 GB/T 20271—2006 中 6.2.5.2 b)的内容。

评估方法：

a) 评估者应审查操作文档，是否说明了终端计算机系统的安装、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评估方法要求作出判断。

4.2.3.3 开发

4.2.3.3.1 功能设计

评估内容：

见 GB/T 20271—2006 中 6.2.5.3 a)的内容。

评估方法：

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系统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系统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系统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评估方法要求作出判断。

4.2.3.3.2 安全策略模型

评估内容：

见 GB/T 20271—2006 中 6.2.5.3 b)的内容。

评估方法：

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评估方法要求作出判断。

4.2.3.3.3 高层设计

评估内容：

见 GB/T 20271—2006 中 6.2.5.3 c)的内容。

评估方法：

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系统的体系结构；

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评估方法要求作出判断。

4.2.3.3.4 低层设计

评估内容：

见 GB/T 20271—2006 中 6.2.5.3 d)的内容。

评估方法：

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) 标识终端计算机系统安全功能 模块的所有接口，标识终端计算机系统安全功能 模块的哪些接口是外部可见的，以及描述终端计算机系统安全功能 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系统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评估方法要求作出判断。

4.2.3.3.5 内部结构设计

评估内容：

见 GB/T 20271—2006 中 6.2.5.3 e)的内容。

评估方法：

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系统安全功能，并避免设计模块之间出现不必要的交互；

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

c) 描述终端计算机系统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评估方法要求作出判断。

4.2.3.3.6 实现表示

评估内容：

见 GB/T 20271—2006 中 6.2.5.3 f)的内容。

评估方法：

评估者应审查开发者所提供的信息是否满足如下要求：

应无歧义地为选定的终端计算机系统安全功能子集定义一个详细级别的终端计算机系统安全功能实现表示，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评估方法要求作出判断。

4.2.3.3.7 对应性设计

评估内容：

见 GB/T 20271—2006 中 6.2.5.3 g)的内容。

评估方法：

评估者应审查开发者所提供的信息是否满足如下要求：

应在所提供的终端计算机系统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系统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系统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评估方法要求作出判断。

4.2.3.4 文档要求

4.2.3.4.1 管理员指南

评估内容：

见 GB/T 20271—2006 中 6.2.5.4 的内容。

评估方法：

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) 终端计算机系统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系统；
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系统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评估方法要求作出判断。

4.2.3.4.2 用户指南

评估内容：

见 GB/T 20271—2006 中 6.2.5.4 的内容。

评估方法：

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) 终端计算机系统的非管理用户可使用的安全功能和接口；
b) 终端计算机系统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) 终端计算机系统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评估方法要求作出判断。

4.2.3.5 生存周期支持

评估内容：

见 GB/T 20271—2006 中 6.1.5.5 的内容。

评估方法：

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系统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系统的生存周期模型，对终端计算机系统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系统的模型；

g) 开发者应标识用于开发终端计算机系统的工具，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评估方法要求作出判断。

4.2.3.6 测试

4.2.3.6.1 范围

评估内容：

见 GB/T 20271—2006 中 6.2.5.6 a)的内容。

评估方法：

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) 评价测试文档中所标识的测试，是否完整；

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评估方法要求作出判断。

4.2.3.6.2 测试深度

评估内容：

见 GB/T 20271—2006 中 6.2.5.6 b)的内容。

评估方法：

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评估方法要求作出判断。

4.2.3.6.3 功能测试

评估内容：

见 GB/T 20271—2006 中 6.2.5.6 c)的内容。

评估方法：

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评估方法要求作出判断。

4.2.3.6.4 独立性测试

评估内容：

见 GB/T 20271—2006 中 6.2.5.6 d)的内容。

评估方法：

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系统。

记录审查结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3 第三级：安全标记保护级

4.3.1 安全功能要求

4.3.1.1 物理系统

4.3.1.1.1 设备安全可用

评估内容：

见 GA/T 671—2006 中 5.3.1.1.1 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机系统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。

评估方法：

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系统的基本运行；

b) 按照开发者提供的文档，模拟出现一些故障事件（如：调电、硬件故障等），验证终端计算机系统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评估方法要求作出判断。

4.3.1.1.2 设备防盗防毁

评估内容：

见 GA/T 671—2006 中 5.3.1.1.2 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机系统的设备具有哪些无法除去的标记。

评估方法：

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) 检测终端计算机系统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评估方法要求作出判断。

4.3.1.2 可信计算平台

4.3.1.2.1 密码支持

评估内容：

见 GA/T 671—2006 中 5.3.1.3.1 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。

评估方法：

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；

b) 检测公钥密码算法、杂凑算法和随机数生成器算法，是否采用硬件实现，如果硬件支持插拔，将硬件拔出，检测能否进行相关密码操作；

c) 检测对称密码算法是由软件，还是由硬件实现，如果由硬件实现并且硬件支持插拔，将硬件拔出，检测能否进行相关密码操作；

d) 按照开发者提供的文档，检测密钥生成、数字签名与验证等关键密码操作，是否基于密码硬件支持，如果硬件支持插拔，将硬件拔出，检测能否进行相关密码操作；

e) 按照开发者提供的文档，检测所有密钥是否受存储根保护，存储根本身是否由安全硬件保护。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.2 信任链

评估内容：

见 GA/T 671—2006 中 5.3.1.3.2 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机系统如何利用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。

开发者应提供证明，静态信任链中操作系统(OS)的完整性度量基准值由国家专门机构管理，是否支持离线(或在线)校验。

开发者应提供文档，说明基准值是否存储在受存储根保护的区域中。

评估方法：

a) 按照开发者提供的文档和相关证书，检测操作系统(OS)的完整性度量基准值，是否已接受国家专门机构管理；

b) 以未授权用户身份篡改操作系统(OS)的完整性度量基准值，检测系统能否防止未经授权的篡改；

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

d) 修改操作系统(OS)的核心文件后，对操作系统进行完整性度量，检测终端计算机系统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；

i) 在被授权的情况下，对信任链建立过程中涉及的各个部件进行升级，检测能否成功；

j) 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评估方法要求作出判断。

4.3.1.2.3 运行时防护

评估内容：

见 GA/T 671—2006 中 5.3.1.3.3 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，并且提供相应的检测分析报告。

评估方法：

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。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.4 系统安全性检测分析

评估内容：

见 GA/T 671—2006 中 5.3.1.3.4 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机系统具有哪些运行时防护功能。

评估方法：

a) 在系统中植入一个测试用的恶意代码，并运行恶意代码；

b) 对文件系统和内存进行扫描，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) 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；

f) 网络协议分析：根据网络协议类型（协议类型如：HTTP、FTP、SMTP、POP3、TELNET、NNTP 等），制定拒绝通过的过滤规则，模拟访问相应的应用协议，检测能否拒绝访问；制定允许某些协议的过滤规则，模拟访问相应的应用协议，检测能否正常访问；

g) 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；

h) 内容过滤：对某些关键词设置相应的过滤规则，访问包含所设置关键词的网页，检测能否正常过滤；

i) 实现实时阻断：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；

j) 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；

k) 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。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.5 信任服务

评估内容：

见 GA/T 671—2006 中 5.3.1.3.5 的内容。

对开发者的要求：

开发者应提供文档，说明如何在可信硬件模块中，专门设置受保护区域来存储所有完整性度量值。

开发者应提供文档，说明是否提供接口向国家专门机构报告操作系统完整性度量值。

评估方法：

a) 按照开发者提供的文档，检测系统是否在可信硬件模块中，专门设置受保护区域存储所有完整性度量值；

b) 尝试以各种方法篡改完整性度量值，检测能否防止篡改；

c) 利用开发者提供的接口，检测能否将操作系统完整性度量值，发送给国家专门机构。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.6 用户身份标识与鉴别

4.3.1.2.6.1 系统身份标识与鉴别

评估内容：

见 GA/T 671—2006 中 5.3.1.3.6.1 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机系统的设备是否具有唯一性标识，是否提供对请求访问的终端计算机系统进行身份鉴别。

评估方法：

a) 按照开发者提供的文档，检测是否通过唯一绑定的可信硬件模块产生的密钥来标识系统身份；

b) 查看审计记录，检测审计中是否记录了系统的唯一性标识，并且检测系统的唯一性标识是否正确；

c) 检测身份标识是否生成证书，检测证书的颁发机构是否满足国家的相关要求；

d) 检测证书是否具有隐秘性；

e) 尝试以各种非授权方式访问、修改或删除身份标识信息，检测能否防止不被非授权地访问、修改或删除；

f) 按照开发者提供的文档，在终端计算机系统上进行访问请求，检测是否进行身份鉴别，并且鉴别时是否提供系统完整性度量值报告。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.6.2 用户身份标识与鉴别

评估内容：

见 GA/T 671—2006 中 5.3.1.3.6.2 的内容。

评估方法：

a) 在安全功能实施所要求的动作之前，检测系统能否先对提出该动作要求的用户进行标识，并进行鉴别，只有鉴别成功后才运行进行相关操作；

b) 创建一个用户，并赋予其一些权限，然后删除此用户，再创建一个新的同名用户，检测新的用户是否具有老用户的权限；

c) 查看审计记录，检测审计信息中是否记录了用户的唯一性标识；
d) 尝试以各种非授权方式访问、修改或删除身份标识信息，检测能否防止不被非授权地访问、修改或删除；
e) 用户以伪造的鉴别数据进行鉴别，检测系统能否检测出并拒绝用户鉴别；
f) 用户以从其他用户处复制的鉴别数据进行鉴别，检测系统能否检测出并拒绝用户鉴别；
g) 检测安全功能能否防止与已标识过的鉴别机制有关的鉴别数据的重用；
h) 以错误的用户名-口令登录，在一定次数的鉴别失败后，测试系统是否终止了进行登录尝试主机建立会话的过程。分别以授权管理员和普通用户的身份登录，测试系统是否提供最多失败次数的设定功能，且最多失败次数仅由授权管理员设定；
i) 以用户身份登录系统，要求安全功能完成某个任务，从而激活另一个主体(如进程)，检测系统是否将该用户与该主体相关联，查看相应的审计记录，检测审计信息中是否记录了用户的身份；
j) 检测系统能否支持以数字证书形式提供鉴别信息，如果支持，使用用户数字证书登录系统，检测能否登录成功；
k) 检测系统能否支持以指纹形式提供鉴别信息，如果支持，使用指纹登录系统，检测能否登录成功；
l) 检测系统能否支持以 USBKey 形式提供鉴别信息，如果支持，使用 USBKey 登录系统，检测能否登录成功。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.7 自主访问控制

评估内容：

见 GA/T 671—2006 中 5.3.1.3.7 的内容。

对开发者的要求：

开发者应提供文档，明确指出终端计算机系统自主访问控制的客体和主体，并说明自主访问控制的范围、策略和粒度。

评估方法：

a) 根据开发者提供的文档，以主体身份对客体添加一条自主访问控制策略，策略为拒绝其他主体的访问；以其他主体身份访问客体，检测能否访问成功；
b) 以主体身份对客体添加一条自主访问控制策略，策略为允许指定主体的访问；以授权主体身份访问客体，检测能否访问成功；以非授权主体身份访问客体，检测能否访问成功。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.8 标记

评估内容：

见 GA/T 671—2006 中 5.3.1.3.8 的内容。

对开发者的要求：

开发者应提供文档，明确指出终端计算机系统能够标记的客体和主体。

评估方法：

a) 对各种主体设置标记，包括等级分类和非等级类别，检测能否设置成功；
b) 对各种客体设置标记，包括等级分类和非等级类别，检测能否设置成功。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.9 强制访问控制

评估内容：

见 GA/T 671—2006 中 5.3.1.3.9 的内容。

对开发者的要求：

开发者应提供文档，明确指出终端计算机系统强制访问控制的客体和主体，并说明强制访问控制的范围、策略和粒度。

评估方法：

a) 根据强制访问控制的拒绝访问策略，对多个主体和多个客体添加不同的标记，并以主体身份访问客体，检测能否访问成功；

b) 根据强制访问控制的允许访问策略，对多个主体和多个客体添加不同的标记，并以主体身份访问客体，检测能否访问成功。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.10 数据保密性保护

4.3.1.2.10.1 数据存储保密性

评估内容：

见 GA/T 671—2006 中 5.3.1.3.10 a)的内容。

对开发者的要求：

开发者应提供文档，说明如何基于存储根实现对数据的保密存储，描述是否支持在特定终端计算机系统的特定状态下解密。

评估方法：

a) 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) 尝试以其他用户身份对数据进行解密，检测能否解密成功；

c) 根据开发者提供的文档，检测系统能否基于存储根实现对数据的保密存储；

d) 在特定终端计算机系统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系统中解密，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系统中解密，检测能否解密成功；

f) 在特定终端计算机系统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系统的特定状态下解密，检测能否解密成功；

g) 由密钥的合法持有者在其他终端计算机系统中解密，检测能否解密成功；

h) 由密钥的合法持有者在特定终端计算机系统的其他状态下解密，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评估方法要求作出判断。

4.3.1.2.10.2 数据传输保密性

评估内容：

见 GA/T 671—2006 中 5.3.1.3.10 b)的内容。

对开发者的要求：

开发者应提供文档，说明如何对传输的用户数据，进行保密性保护。

评估方法：

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评估方法要求作出判断。

4.3.1.2.10.3 客体安全重用

评估内容：

见 GA/T 671—2006 中 5.3.1.3.10 c)的内容。

对开发者的要求：

开发者应提供文档，说明如何设计和实现系统的客体安全重用功能。

评估方法：

a) 以主体身份，申请全部剩余的客体资源，并全部填充一个特殊的值，然后释放此资源；

b) 以另一主体身份，申请全部剩余的客体资源，查看客体资源中，是否存在特殊的值。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.11 数据完整性保护

4.3.1.2.11.1 存储数据的完整性

评估内容：

见 GA/T 671—2006 中 5.3.1.3.11 的内容。

对开发者的要求：

开发者应提供文档，说明对可信计算平台内部存储的数据，采取了哪些数据完整性保护措施。

评估方法：

a) 使用各种方法和工具，对可信计算平台内部存储的数据，进行修改，检测系统能否检测出完整性错误，能否采取恢复措施；

b) 对照原始数据和恢复后的数据，检测能否完全恢复全部数据。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.11.2 传输数据的完整性

评估内容：

见 GA/T 671—2006 中 5.3.1.3.11 的内容。

对开发者的要求：

开发者应提供文档，说明对可信信息系统间传输的用户数据，采取了哪些数据完整性保护措施，选择哪种恢复措施：

——由接收者 SSOTCS 借助于源可信信息系统提供的信息；

——由接收者 SSOTCS 自己无须来自源可信信息系统的任何帮助，来恢复被破坏的数据为原始的用户数据。

评估方法：

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

b) 按照开发者提供的文档，检测能否对检测出的完整性错误进行恢复，并检测恢复措施的有效性。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.11.3 处理数据的完整性

评估内容：

见 GA/T 671—2006 中 5.3.1.3.11 的内容。

对开发者的要求：

开发者应提供文档，说明具体的回退措施。

评估方法：

a) 记录当前系统的各种状态；

b) 进行一些操作，然后对这些操作进行回退，检测系统能否回退到以前的状态。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.12 安全审计

评估内容：

见 GA/T 671—2006 中 5.3.1.3.12 的内容。

评估方法：

a) 查看系统的审计记录信息，检测是否有密码支持、身份标识与鉴别、自主访问控制、数据保密性保护、用户数据完整性保护、信任服务、标记、强制访问控制等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、实时报警生成和违例进程终止；

c) 检测审计功能是否支持潜在侵害分析和基于异常检测；

d) 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；

e) 检测审计信息是否受到安全保护，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；

f) 对于内置可信硬件模块的终端计算机系统，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，检测是否具有相关审计信息；检测是否提供给上层应用软件查询审计情况的接口；检测是否存储审计记录。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.13 备份与故障恢复

评估内容：

见 GA/T 671—2006 中 5.3.1.3.13 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。

评估方法：

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) 对系统定时进行增量备份，对系统数据进行修改，然后进行恢复，检测能否有效恢复；

c) 对局部系统进行定期备份，对系统数据进行修改，然后进行恢复，检测能否有效恢复；

d) 对全系统进行定期备份，对系统数据进行修改，然后进行恢复，检测能否有效恢复。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.1.2.14 I/O 接口配置

评估内容：

见 GA/T 671—2006 中 5.3.1.3.14 的内容。

评估方法：

a) 以用户身份，在 BIOS 和操作系统中，分别启用串口、并口、PCI、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，分别禁用串口、并口、PCI、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评估方法要求作出判断。

4.3.1.2.15 可信时间戳

评估内容：

见 GA/T 671—2006 中 5.3.1.3.15 的内容。

对开发者的要求：

开发者应提供文档，说明终端计算机系统是否提供可信时间戳功能。

评估方法：

a) 修改系统的时钟，然后对系统进行时间同步，检测时间能否调整正确；

b) 按照开发者提供的文档，检测系统的时间戳功能是否可信。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.2 SSOTCS 自身安全保护

4.3.2.1 可信根安全保护

评估内容：

见 GA/T 671—2006 中 5.3.2.1 a)的内容。

对开发者的要求：

开发者应提供文档，说明是否对度量根采取物理保护措施。

评估方法：

a) 按照开发者提供的文档，检测存储根和报告根是否设置在可信硬件模块内；

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

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.2.2 安全功能物理安全保护

评估内容：

见 GA/T 671—2006 中 5.3.2.1 b)的内容。

评估方法：

尝试对密码运算模块进行能量攻击，检测能否攻击成功。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.2.3 安全功能运行安全保护

评估内容：

见 GA/T 671—2006 中 5.3.2.1 c)的内容。

评估方法：

a) 使终端计算机系统进入休眠状态，然后使系统退出休眠状态，检测系统能否恢复到退出工作状态前的配置，并且检测信任链系统能否正常工作；

b) 使终端计算机系统进入待机状态，然后使系统退出待机状态，检测系统能否恢复到退出工作状态前的配置，并且检测信任链系统能否正常工作。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.3 SSOTCS 设计和实现

4.3.3.1 配置管理

4.3.3.1.1 配置管理能力

评估内容：

见 GB/T 20271—2006 中 6.3.5.1 a)的内容。

评估方法：

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系统样本应完全对应，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评估方法要求作出判断。

4.3.3.1.2 配置管理自动化

评估内容：

见 GB/T 20271—2006 中 6.3.5.1 b)的内容。

评估方法：

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系统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系统的生成；

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评估方法要求作出判断。

4.3.3.1.3 配置管理范围

评估内容：

见 GB/T 20271—2006 中 6.3.5.1 c)、6.3.5.1 d)的内容。

评估方法：

a) 终端计算机系统配置管理范围，要求将终端计算机系统的实现表示、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评估方法要求作出判断。

4.3.3.2 分发和操作

4.3.3.2.1 分发

评估内容：

见 GB/T 20271—2006 中 6.3.5.2 的内容。

评估方法：

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系统时，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评估方法要求作出判断。

4.3.3.2.2 操作

评估内容：

见 GB/T 20271—2006 中 6.3.5.2 的内容。

评估方法：

a) 评估者应审查操作文档，是否说明了终端计算机系统的安装、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评估方法要求作出判断。

4.3.3.3 开发

4.3.3.3.1 功能设计

评估内容：

见 GB/T 20271—2006 中 6.3.5.3 a)的内容。

评估方法：

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系统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系统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系统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评估方法要求作出判断。

4.3.3.3.2 安全策略模型

评估内容：

见 GB/T 20271—2006 中 6.3.5.3 b)的内容。

评估方法：

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评估方法要求作出判断。

4.3.3.3.3 高层设计

评估内容：

见 GB/T 20271—2006 中 6.3.5.3 c)的内容。

评估方法：

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系统的体系结构；

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系统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评估方法要求作出判断。

4.3.3.3.4 低层设计

评估内容：

见 GB/T 20271—2006 中 6.3.5.3 d)的内容。

评估方法：

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) 标识终端计算机系统安全功能模块的所有接口，标识终端计算机系统安全功能模块的哪

些接口是外部可见的，以及描述终端计算机系统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系统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评估方法要求作出判断。

4.3.3.3.5 内部结构设计

评估内容：

见 GB/T 20271—2006 中 6.3.5.3 e)的内容。

评估方法：

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系统安全功能，并避免设计模块之间出现不必要的交互；

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

c) 描述终端计算机系统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评估方法要求作出判断。

4.3.3.3.6 实现表示

评估内容：

见 GB/T 20271—2006 中 6.3.5.3 f)的内容。

评估方法：

评估者应审查开发者所提供的信息是否满足如下要求：

应无歧义地为全部终端计算机系统安全功能，定义一个详细级别的终端计算机系统安全功能实现表示，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评估方法要求作出判断。

4.3.3.3.7 对应性设计

评估内容：

见 GB/T 20271—2006 中 6.3.5.3 g)的内容。

评估方法：

评估者应审查开发者所提供的信息是否满足如下要求：

应在所提供的终端计算机系统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系统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系统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评估方法要求作出判断。

4.3.3.4 文档要求

4.3.3.4.1 管理员指南

评估内容：

见 GB/T 20271—2006 中 6.3.5.4 的内容。

评估方法：

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) 终端计算机系统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系统；
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系统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评估方法要求作出判断。

4.3.3.4.2 用户指南

评估内容：

见 GB/T 20271—2006 中 6.3.5.4 的内容。

评估方法：

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) 终端计算机系统的非管理用户可使用的安全功能和接口；
b) 终端计算机系统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) 终端计算机系统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评估方法要求作出判断。

4.3.3.5 生存周期支持

4.3.3.5.1 开发安全

评估内容：

见 GB/T 20271—2006 中 6.3.5.5 a)的内容。

评估方法：

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。

记录审查结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.3.5.2 缺陷纠正

评估内容：

见 GB/T 20271—2006 中 6.3.5.5 b)的内容。

评估方法：

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系统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) 描述为终端计算机系统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评估方法要求作出判断。

4.3.3.5.3 生存周期定义

评估内容：

见 GB/T 20271—2006 中 6.3.5.5 c)的内容。

评估方法：

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系统的生存周期模型；

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系统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系统的模型，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系统，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评估方法要求作出判断。

4.3.3.5.4 工具和技术

评估内容：

见 GB/T 20271—2006 中 6.3.5.5 d)的内容。

评估方法：

评估者应审查开发者所提供的信息是否满足如下要求：

开发者应标识用于开发终端计算机系统的工具，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评估方法要求作出判断。

4.3.3.6 测试

4.3.3.6.1 范围

评估内容：

见 GB/T 20271—2006 中 6.3.5.6.1 的内容。

评估方法：

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) 评价安全功能设计中所描述的安全功能，是否都经过了完整性测试。

记录审查结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.3.6.2 测试深度

评估内容：

见 GB/T 20271—2006 中 6.3.5.6.2 的内容。

评估方法：

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评估方法要求作出判断。

4.3.3.6.3 功能测试

评估内容：

见 GB/T 20271—2006 中 6.3.5.6.3 的内容。

评估方法：

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。

记录测试结果并对该结果是否完全符合上述评估方法要求作出判断。

4.3.3.6.4 独立性测试

评估内容：

见 GB/T 20271—2006 中 6.3.5.6.4 的内容。

评估方法：

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系统；

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评估方法要求作出判断。

4.3.3.7 脆弱性评定

4.3.3.7.1 防止误用

评估内容：

见 GB/T 20271—2006 中 6.3.5.7 a)的内容。

评估方法：

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系统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评估方法要求作出判断。

4.3.3.7.2 安全功能强度评估

评估内容：

见 GB/T 20271—2006 中 6.3.5.7 b)的内容。

评估方法：

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，得到终端计算机系统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评估方法要求作出判断。

4.3.3.7.3 脆弱性分析

评估内容：

见 GB/T 20271—2006 中 6.3.5.7 c)的内容。

评估方法：

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，对终端计算机系统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系统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系统可以抵御明显的穿透性攻击；

e） 实施独立的穿透性测试，检测终端计算机系统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评估方法要求作出判断。

参 考 文 献

[1] GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般模型

[2] GB/T 18336.2—2001 信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能要求

[3] GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分:安全保证要求

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

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

中华人民共和国公共安全
行业标准
信息安全技术
终端计算机系统安全等级评估准则
GA/T 672—2006
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.5 字数 70 千字
2007年3月第一版 2007年3月第一次印刷
*
书号:155066·2-17471

GA/T 672-2006