ICS 35.040
L80

中华人民共和国国家标准

GB/T 20279—2006

信息安全技术
网络和终端设备隔离部件安全技术要求

Information security technology
Security techniques requirements of separation components
of network and terminal equipment

2006-05-31 发布　　2006-12-01 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 V
引　言 VI
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　安全环境 2
4.1　物理方面 2
4.2　人员方面 2
4.3　连通性方面 2
5　隔离部件分级安全技术要求 2
5.1　物理断开隔离部件 2
5.1.1　基本级要求 2
5.1.1.1　访问控制 2
5.1.1.2　配置管理 3
5.1.1.3　交付与运行 3
5.1.1.4　安全功能开发过程 3
5.1.1.5　指导性文档 3
5.1.1.6　测试 4
5.1.1.7　生命周期支持 4
5.1.2　增强级要求 4
5.1.2.1　访问控制 4
5.1.2.2　不可旁路 5
5.1.2.3　客体重用 5
5.1.2.4　配置管理 5
5.1.2.5　交付与运行 5
5.1.2.6　安全功能开发过程 5
5.1.2.7　指导性文档 6
5.1.2.8　生命周期支持 6
5.1.2.9　测试 6
5.1.2.10　脆弱性评定 7
5.2　单向隔离部件 7
5.2.1　基本级要求 7
5.2.1.1　访问控制 7
5.2.1.2　配置管理 8
5.2.1.3　交付与运行 8
5.2.1.4　安全功能开发过程 8
5.2.1.5　指导性文档 8
5.2.1.6　测试 9

5.2.1.7 生命周期支持 9
5.2.2 增强级要求 9
5.2.2.1 访问控制 9
5.2.2.2 不可旁路 10
5.2.2.3 客体重用 10
5.2.2.4 配置管理 10
5.2.2.5 交付与运行 10
5.2.2.6 安全功能开发过程 10
5.2.2.7 指导性文档 11
5.2.2.8 生命周期支持 11
5.2.2.9 测试 11
5.2.2.10 脆弱性评定 12
5.3 协议隔离部件 12
5.3.1 第一级 12
5.3.1.1 访问控制 12
5.3.1.2 身份鉴别 13
5.3.1.3 数据完整性 13
5.3.1.4 配置管理 13
5.3.1.5 交付与运行 13
5.3.1.6 安全功能开发过程 13
5.3.1.7 指导性文档 13
5.3.1.8 测试 14
5.3.1.9 生命周期支持 14
5.3.2 第二级 14
5.3.2.1 访问控制 14
5.3.2.2 身份鉴别 15
5.3.2.3 客体重用 16
5.3.2.4 审计 16
5.3.2.5 数据完整性 17
5.3.2.6 配置管理 17
5.3.2.7 交付与运行 17
5.3.2.8 安全功能开发过程 17
5.3.2.9 指导性文档 18
5.3.2.10 生命周期支持 18
5.3.2.11 测试 18
5.3.2.12 脆弱性评定 19
5.3.3 第三级 19
5.3.3.1 访问控制 19
5.3.3.2 标记 20
5.3.3.3 身份鉴别 20

5.3.3.4 客体重用 21
5.3.3.5 审计 21
5.3.3.6 数据完整性 22
5.3.3.7 密码支持 22
5.3.3.8 配置管理 22
5.3.3.9 交付和运行 22
5.3.3.10 安全功能开发过程 23
5.3.3.11 指导性文档 24
5.3.3.12 生命周期支持 24
5.3.3.13 测试 25
5.3.3.14 脆弱性评定 25
5.4 网闸隔离部件 25
5.4.1 第一级 25
5.4.1.1 访问控制 25
5.4.1.2 身份鉴别 26
5.4.1.3 数据完整性 26
5.4.1.4 配置管理 26
5.4.1.5 交付与运行 26
5.4.1.6 安全功能开发过程 26
5.4.1.7 指导性文档 27
5.4.1.8 测试 27
5.4.1.9 生命周期支持 28
5.4.2 第二级 28
5.4.2.1 访问控制 28
5.4.2.2 身份鉴别 29
5.4.2.3 客体重用 29
5.4.2.4 审计 29
5.4.2.5 数据完整性 30
5.4.2.6 配置管理 30
5.4.2.7 交付与运行 30
5.4.2.8 安全功能开发过程 30
5.4.2.9 指导性文档 31
5.4.2.10 生命周期支持 32
5.4.2.11 测试 32
5.4.2.12 脆弱性评定 32
5.4.3 第三级 32
5.4.3.1 访问控制 32
5.4.3.2 标记 34
5.4.3.3 身份鉴别 34

5.4.3.4 客体重用 34
5.4.3.5 审计 34
5.4.3.6 数据完整性 35
5.4.3.7 密码支持 35
5.4.3.8 配置管理 35
5.4.3.9 交付和运行 36
5.4.3.10 安全功能开发过程 36
5.4.3.11 指导性文档 37
5.4.3.12 生命周期支持 38
5.4.3.13 测试 38
5.4.3.14 脆弱性评定 39
参考文献 40

前　言

（略）

引　言

本标准是信息安全等级保护技术要求系列标准的重要组成部分，用以指导设计者如何设计和实现具有所需要的安全等级的隔离部件，主要从对隔离部件的安全保护等级进行划分的角度来说明其技术要求，即主要说明为实现基于 GB17859-1999 的各个保护等级的安全要求对隔离部件应采取的安全技术措施，以及各安全技术要求在不同安全级中具体实现上的差异。

本标准以 GB17859-1999 的安全等级的划分为基础，针对隔离部件的技术特点，对相应安全等级的安全功能技术要求和安全保证技术要求做了详细描述。

在本标准文本中，加粗字体表示较高等级中新出现或增强的功能要求。

信息安全技术
网络和终端设备隔离部件安全技术要求

1 范围

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

本标准适用于隔离部件的设计和实现，对隔离部件进行的测试、管理也可参照使用。

2 规范性引用文件

下列文件中的有关条款通过引用而成为本标准的条款。凡注日期或版次的引用文件，其后的任何修改单（不包括勘误的内容）或修订版本都不适用于本标准，但提倡使用本标准的各方探讨使用其最新版本的可能性。凡不注日期或版次的引用文件，其最新版本适用于本标准。

GB17859-1999 计算机信息系统安全保护等级划分准则

GB/T BBBB-XXXX 信息安全技术 计算机信息系统安全等级保护通用技术要求

3 术语和定义

GB17859-1999 和 GB/T BBBB-XXXX 中确立的以及下列术语和定义适用于本标准。

3.1

物理断开 physical disconnection

指处于不同安全域的网络之间不能以直接或间接的方式相连接。在一个物理网络环境中，实施不同安全域的网络物理断开，在技术上应确保信息在物理传导、物理存储上的断开。

3.2

协议转换 protocol conversion

在隔离部件中，协议转换的定义是协议的剥离和重建。在所属某一安全域的隔离部件一端，把基于网络的公共协议中的应用数据剥离出来，封装为系统专用协议传递至所属其他安全域的隔离部件另一端，再将专用协议剥离，并封装成需要的格式。

3.3

协议隔离 protocol separation

指处于不同安全域的网络在物理上是有连线的，通过协议转换的手段保证受保护信息在逻辑上是隔离的，只有被系统要求传输的、内容受限的信息可以通过。

3.4

信息摆渡 information ferry

信息交换的一种方式，物理传输信道只在传输进行时存在。信息传输时，信息先由信息源所在安全域一端传输至中间缓存区域，同时物理断开中间缓存区域与信息目的所在安全域的连接；随后接通中间缓存区域与信息目的所在安全域的传输信道，将信息传输至信息目的所在安全域，同时在信道上物理断开信息源所在安全域与中间缓存区域的连接。在任一时刻，中间缓存区域只与一端安全域相连。

3.5

物理断开隔离部件 physical disconnection separation components

在端上实现信息物理断开的信息安全部件，如物理隔离卡。

3.6

单向隔离部件 unilateral separation components

在端上依靠由硬件访问控制信息交换分区实现信息在不同的安全域信息单向流动的信息安全部件。

3.7

协议隔离部件 protocol separation components

位于两个不同安全域之间，实现协议隔离的信息安全部件。其信息流一般是专用应用数据。

3.8

网闸 gap

该信息安全部件位于两个不同安全域之间，通过协议转换的手段，以信息摆渡的方式实现数据交换，且只有被系统明确要求传输的信息可以通过。其信息流一般是通用应用服务。

4 安全环境

4.1 物理方面

对隔离部件资源的处理限定在一些可控制的访问设备内，防止未授权的物理访问。所有与实施隔离部件安全策略相关的硬件和软件应受到保护以免于未授权的物理修改。

4.2 人员方面

授权管理员不具敌意并遵守所有的管理员规则。

4.3 连通性方面

隔离部件是处于不同安全域网络之间的唯一连接点。对于物理断开隔离部件，不存在任何安全域网间的信息传输；对于单向隔离部件，信息可以从低级安全域向高级安全域通过断电非逸失性存储设备进行单向传输，反之则不能；对于协议隔离部件与网闸部件，所有安全域网络间的信息传输应经过隔离部件；授权管理员可以从高级安全域网络对隔离部件进行远程管理。

5 隔离部件分级安全技术要求

5.1 物理断开隔离部件

5.1.1 基本级要求

5.1.1.1 访问控制

5.1.1.1.1 安全属性定义

对于信息存储与传输部件（主要是处于不同安全域的存储设备、网络接入设备），物理断开隔离部件应为其设定唯一的、为了执行安全功能策略所必需的安全属性。

5.1.1.1.2 属性修改

物理断开隔离部件安全功能应向端设备用户提供修改与安全相关属性的参数的能力。

5.1.1.1.3 属性查询

物理断开隔离部件安全功能应向端设备用户提供安全属性查询的能力。

5.1.1.1.4 访问授权与拒绝

物理断开隔离部件的安全功能应对被隔离的计算机信息资源提供明确的访问保障能力和访问拒绝能力。在技术上确保：

a) **在信息物理传导上使内外网络隔断，确保外部网不能通过网络连接侵入内部网；同时阻止内部网信息通过网络连接泄露到外部网；**

b) 在信息物理存储上隔断两个网络环境，对于断电后会逸失信息的部件，如内存、寄存器等暂存部件，要在网络转换时作清零处理，防止遗留信息窜网；对于断电后不会逸失信息的设备，如磁带机、硬盘等存储设备，内部网与外部网信息要以不同存储设备分开存储；对移动存储介质，如光盘、软盘、USB 硬盘等，应在网络转换前提示用户干预或禁止在双网都能使用这些设备。

5.1.1.2 配置管理

开发者应为隔离部件产品的不同版本提供唯一的标识。

隔离部件产品的每个版本应当使用它们的唯一标识作为标签。

5.1.1.3 交付与运行

5.1.1.3.1 交付

开发者应使用一定的交付程序交付物理断开隔离部件，并将交付过程文档化。

交付文档应描述在给用户方交付物理断开隔离部件的各版本时，为维护安全所必需的所有程序。

5.1.1.3.2 安装生成

开发者应提供文档说明物理断开隔离部件的安装、生成和启动的过程。

5.1.1.4 安全功能开发过程

5.1.1.4.1 功能设计

开发者应提供隔离部件产品的安全功能设计。

功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能设计应是内在一致的并能完备地表示安全功能。

5.1.1.4.2 表示对应性

开发者应在隔离部件安全功能表示的所有相邻对之间提供对应性分析。

对于隔离部件安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.1.1.5 指导性文档

5.1.1.5.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 隔离部件可以使用的管理功能和接口；

b) 怎样安全地管理隔离部件；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与隔离部件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。

管理员指南应与为评估而提供的其他所有文档保持一致。

5.1.1.5.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 隔离部件的非管理用户可使用的安全功能和接口；

b) 隔离部件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) 隔离部件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。

用户指南应与为评估而提供的其他所有文档保持一致。

5.1.1.6 测试

5.1.1.6.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明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。

5.1.1.6.2 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其它测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.1.1.7 生命周期支持

开发者应提供开发安全文件。

开发安全文件应描述在隔离部件的开发环境中，为保护隔离部件设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在隔离部件的开发和维护过程中执行安全措施的证据。

5.1.2 增强级要求

5.1.2.1 访问控制

5.1.2.1.1 安全属性定义

对于信息存储与传输部件（主要是处于不同安全域的存储设备、网络接入设备），物理断开隔离部件应为其设定唯一的、为了执行安全功能策略所必需的安全属性。

5.1.2.1.2 属性修改

物理断开隔离部件安全功能应向端设备用户提供修改与安全相关属性的参数的能力。

5.1.2.1.3 属性查询

物理断开隔离部件安全功能应向端设备用户提供安全属性查询的能力。

5.1.2.1.4 访问授权与拒绝

物理断开隔离部件的安全功能应对被隔离的计算机信息资源提供明确的访问保障能力和访问拒绝能力。在技术上确保：

a) 在信息物理传导上使内外网络隔断，确保外部网不能通过网络连接侵入内部网；同时阻止内部网信息通过网络连接泄露到外部网；

b) 在信息物理存储上隔断两个网络环境，对于断电后会逸失信息的部件，如内存、寄存器等暂存部件，要在网络转换时作清零处理，防止遗留信息窜网；对于断电后不会逸失信息的设备，如磁带机、硬盘等存储设备，内部网与外部网信息要以不同存储设备分开存储；对移动存储

介质，如光盘、软盘、USB 硬盘等，应在网络转换前提示用户干预或禁止在双网都能使用这些设备。

5.1.2.2 不可旁路

在与安全有关的操作（例如安全属性的修改）被允许执行之前，物理断开隔离部件安全功能应确保其通过安全功能策略的检查。

5.1.2.3 客体重用

在为所有内部或外部网上的主机连接进行资源分配时，物理断开隔离部件安全功能应保证不提供以前连接的任何信息内容。

5.1.2.4 配置管理

5.1.2.4.1 配置管理能力

开发者应使用配置管理系统并提供配置管理文档，以及为隔离部件产品的不同版本提供唯一的标识。

配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项。

配置管理文档应包括配置清单和配置管理计划。在配置清单中，应对每一配置项给出相应的描述；在配置管理计划中，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。

配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效地维护的证据。

5.1.2.4.2 配置管理范围

开发者应提供配置管理文档。

配置管理文档应说明配置管理系统至少能跟踪：隔离部件实现表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档，并描述配置管理系统是如何跟踪配置项的。

5.1.2.5 交付与运行

5.1.2.5.1 交付

开发者应使用一定的交付程序交付物理断开隔离部件，并将交付过程文档化。

交付文档应描述在给用户方交付物理断开隔离部件的各版本时，为维护安全所必需的所有程序。

5.1.2.5.2 安装生成

开发者应提供文档说明物理断开隔离部件的安装、生成和启动的过程。

5.1.2.6 安全功能开发过程

5.1.2.6.1 功能设计

开发者应提供隔离部件的安全功能设计。

功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能设计应是内在一致的并能完备地表示安全功能。

5.1.2.6.2 高层设计

开发者应提供隔离部件安全功能的高层设计。

高层设计应以非形式方法表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强隔离部件安全功能的子系统和其它子系统分开。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提供安全功能子系统的作用、例外情

况和错误信息的细节。高层设计还应标识安全功能要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件或软件所实现的保护机制。

5.1.2.6.3 表示对应性

开发者应在隔离部件安全功能表示的所有相邻对之间提供对应性分析。

对于隔离部件安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.1.2.7 指导性文档

5.1.2.7.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 隔离部件管理员可以使用的管理功能和接口；
b) 怎样安全地管理隔离部件；
c) 在安全处理环境中应进行控制的功能和权限；
d) 所有对与隔离部件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。

管理员指南应与为评估而提供的其他所有文档保持一致。

5.1.2.7.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 隔离部件的非管理用户可使用的安全功能和接口；
b) 隔离部件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) 隔离部件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。

用户指南应与为评估而提供的其他所有文档保持一致。

5.1.2.8 生命周期支持

开发者应提供开发安全文件。

开发安全文件应描述在隔离部件的开发环境中，为保护隔离部件设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在隔离部件的开发和维护过程中执行安全措施的证据。

5.1.2.9 测试

5.1.2.9.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明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，**且该对应是完备的。**

5.1.2.9.2 测试深度

开发者应提供测试深度的分析。

在深度分析中，应说明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。

5.1.2.9.3　功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其它测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.1.2.9.4　独立性测试

开发商应提供用于适合测试的部件，且提供的测试集合应与其自测产品功能时使用的测试集合相一致。

5.1.2.10　脆弱性评定

5.1.2.10.1　指南检查

开发者应提供指南性文档。

在指南性文档中，应确定对隔离部件的所有可能的操作方式（包括失败和操作失误后的操作）、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出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。指南性文档应是完备的、清晰的、一致的、合理的。

5.1.2.10.2　脆弱性分析

开发者应从用户可能破坏安全策略的明显途径出发，对隔离部件的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用隔离部件的环境中该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的隔离部件可以抵御明显的穿透性攻击。

5.2　单向隔离部件

5.2.1　基本级要求

5.2.1.1　访问控制

5.2.1.1.1　安全属性定义

对于信息存储与传输部件（主要是处于不同安全域的存储设备、网络接入设备），单向隔离部件应为其设定唯一的、为了执行安全功能策略所必需的安全属性。

5.2.1.1.2　属性修改

单向隔离部件安全功能应向端设备用户提供修改与安全相关属性的参数的能力。

5.2.1.1.3　属性查询

单向隔离部件安全功能应向端设备用户提供安全属性查询的能力。

5.2.1.1.4　访问授权与拒绝

单向隔离部件的安全功能应对被隔离的计算机信息资源提供明确的访问保障能力和访问拒绝能力。在技术上确保：

a)　在信息物理传导上使内外网络隔断，确保内部网不能通过网络连接到外部网；同时保证限定外部网信息只能通过特定存储区域转移至内部网存储区域，从而阻止内部网信息通过网络连接泄露到外部网。

b) 在信息物理存储上隔断两个网络环境，对于断电后会逸失信息的部件，如内存、寄存器等暂存部件，要在网络转换时作清零处理，防止遗留信息窜网；对于断电后不会逸失信息的设备，如磁带机、硬盘等存储设备，内部网与外部网信息要分开存储并以硬件手段保证其特定的访问控制；对移动存储介质，如光盘、软盘、USB 硬盘等，应在网络转换前提示用户干预。

5.2.1.2 配置管理

开发者应为隔离部件产品的不同版本提供唯一的标识。

隔离部件产品的每个版本应当使用它们的唯一标识作为标签。

5.2.1.3 交付与运行

5.2.1.3.1 交付

开发者应使用一定的交付程序交付单向隔离部件，并将交付过程文档化。

交付文档应描述在给用户方交付单向隔离部件的各版本时，为维护安全所必需的所有程序。

5.2.1.3.2 安装生成

开发者应提供文档说明单向隔离部件的安装、生成和启动的过程。

5.2.1.4 安全功能开发过程

5.2.1.4.1 功能设计

开发者应提供隔离部件产品的安全功能设计。

功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能设计应是内在一致的并能完备地表示安全功能。

5.2.1.4.2 表示对应性

开发者应在隔离部件安全功能表示的所有相邻对之间提供对应性分析。

对于隔离部件安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.2.1.5 指导性文档

5.2.1.5.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 隔离部件可以使用的管理功能和接口；

b) 怎样安全地管理隔离部件；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与隔离部件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。

管理员指南应与为评估而提供的其他所有文档保持一致。

5.2.1.5.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 隔离部件的非管理用户可使用的安全功能和接口；

b) 隔离部件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) 隔离部件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。

用户指南应与为评估而提供的其他所有文档保持一致。

5.2.1.6 测试

5.2.1.6.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明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。

5.2.1.6.2 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其它测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.2.1.7 生命周期支持

开发者应提供开发安全文件。

开发安全文件应描述在隔离部件的开发环境中，为保护隔离部件设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在隔离部件的开发和维护过程中执行安全措施的证据。

5.2.2 增强级要求

5.2.2.1 访问控制

5.2.2.1.1 安全属性定义

对于信息存储与传输部件（主要是处于不同安全域的存储设备、网络接入设备），单向隔离部件应为其设定唯一的、为了执行安全功能策略所必需的安全属性。

5.2.2.1.2 属性修改

单向隔离部件安全功能应向端设备用户提供修改与安全相关属性的参数的能力。

5.2.2.1.3 属性查询

单向隔离部件安全功能应向端设备用户提供安全属性查询的能力。

5.2.2.1.4 访问授权与拒绝

单向隔离部件的安全功能应对被隔离的计算机信息资源提供明确的访问保障能力和访问拒绝能力。在技术上确保：

a) 在信息物理传导上使内外网络隔断，确保内部网不能通过网络连接到外部网；同时保证限定外部网信息只能通过特定存储区域转移至内部网存储区域，从而阻止内部网信息通过网络连接泄露到外部网。

b) 在信息物理存储上隔断两个网络环境，对于断电后会逸失信息的部件，如内存、寄存器等暂存部件，要在网络转换时作清零处理，防止遗留信息窜网；对于断电后不会逸失信息的设备，如磁带机、硬盘等存储设备，内部网与外部网信息要以不同存储设备分开存储；对移动存储

介质，如光盘、软盘、USB 硬盘等，应在网络转换前提示用户干预或禁止在双网都能使用这些设备。

5.2.2.2 不可旁路

在与安全有关的操作（例如安全属性的修改）被允许执行之前，隔离部件安全功能应确保其通过安全功能策略的检查。

5.2.2.3 客体重用

在为所有内部或外部网上的主机连接进行资源分配时，隔离部件安全功能应保证不提供以前连接的任何信息内容。

5.2.2.4 配置管理

5.2.2.4.1 配置管理能力

开发者应使用配置管理系统并提供配置管理文档，以及为隔离部件产品的不同版本提供唯一的标识。

配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项。

配置管理文档应包括配置清单和配置管理计划。在配置清单中，应对每一配置项给出相应的描述；在配置管理计划中，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。

配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效地维护的证据。

5.2.2.4.2 配置管理范围

开发者应提供配置管理文档。

配置管理文档应说明配置管理系统至少能跟踪：隔离部件实现表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档，并描述配置管理系统是如何跟踪配置项的。

5.2.2.5 交付与运行

5.2.2.5.1 交付

开发者应使用一定的交付程序交付单向隔离部件，并将交付过程文档化。

交付文档应描述在给用户方交付单向隔离部件的各版本时，为维护安全所必需的所有程序。

5.2.2.5.2 安装生成

开发者应提供文档说明单向隔离部件的安装、生成和启动的过程。

5.2.2.6 安全功能开发过程

5.2.2.6.1 功能设计

开发者应提供隔离部件的安全功能设计。

功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能设计应是内在一致的并能完备地表示安全功能。

5.2.2.6.2 高层设计

开发者应提供隔离部件安全功能的高层设计。

高层设计应以非形式方法表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强隔离部件安全功能的子系统和其它子系统分开。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提供安全功能子系统的作用、例外情况和错误信息的细节。高层设计还应标识安全功能要求的所有基础性的硬件、固件和软件，并且支持

由这些硬件、固件或软件所实现的保护机制。

5.2.2.6.3 表示对应性

开发者应在隔离部件安全功能表示的所有相邻对之间提供对应性分析。

对于隔离部件安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.2.2.7 指导性文档

5.2.2.7.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 隔离部件管理员可以使用的管理功能和接口；
b) 怎样安全地管理隔离部件；
c) 在安全处理环境中应进行控制的功能和权限；
d) 所有对与隔离部件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。

管理员指南应与为评估而提供的其他所有文档保持一致。

5.2.2.7.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 隔离部件的非管理用户可使用的安全功能和接口；
b) 隔离部件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) 隔离部件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。

用户指南应与为评估而提供的其他所有文档保持一致。

5.2.2.8 生命周期支持

开发者应提供开发安全文件。

开发安全文件应描述在隔离部件的开发环境中，为保护隔离部件设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在隔离部件的开发和维护过程中执行安全措施的证据。

5.2.2.9 测试

5.2.2.9.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明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，**且该对应是完备的。**

5.2.2.9.2 测试深度

开发者应提供测试深度的分析。

在深度分析中，应说明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。

5.2.2.9.3　功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其它测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.2.2.9.4　独立性测试

开发商应提供用于适合测试的产品，且提供的测试集合应与其自测产品功能时使用的测试集合相一致。

5.2.2.10　脆弱性评定

5.2.2.10.1　指南检查

开发者应提供指南性文档。

在指南性文档中，应确定对隔离部件的所有可能的操作方式（包括失败和操作失误后的操作）、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出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。指南性文档应是完备的、清晰的、一致的、合理的。

5.2.2.10.2　脆弱性分析

开发者应从用户可能破坏安全策略的明显途径出发，对隔离部件的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用隔离部件的环境中该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的隔离部件可以抵御明显的穿透性攻击。

5.3　协议隔离部件

5.3.1　第一级

5.3.1.1　访问控制

5.3.1.1.1　安全属性定义

对于每一个授权管理员、构成系统的信息传输与控制部件、应用层数据采集与接受部件，协议隔离部件安全功能应为其提供一套唯一的、为了执行安全功能策略所必需的安全属性。

5.3.1.1.2　属性初始化

协议隔离部件安全功能应提供用默认值对授权管理员和主机属性初始化的能力。

5.3.1.1.3　属性修改

协议隔离部件安全功能应仅向授权管理员提供修改下述（包含但不仅限于）参数的能力：

标识与角色（例如：配置管理员等）的关系；

a）　数据采集与接收部件参数（例如：采集、接收部件主机的 IP 地址、应用服务参数等）；

b）　配置的安全参数（例如：最大鉴别失败次数等数据）。

5.3.1.1.4　属性查询

协议隔离部件安全功能应仅向授权管理员提供以下查询：

a）　数据采集与接收部件参数（例如：采集、接收部件主机的 IP 地址、应用服务参数等）；

b）　通过协议隔离部件传送信息的设备名。

5.3.1.1.5　访问授权与拒绝

协议隔离安全功能应根据数据发送方和接收方的安全属性值[主机名、IP 地址、预先定义的传输层协议和请求的服务（例如：源端口号或目的端口号）、应用层协议、应用数据关键字等]，提供明确的访问保障能力和拒绝访问能力。

5.3.1.2　身份鉴别

5.3.1.2.1　鉴别数据初始化

协议隔离部件安全功能应根据规定的鉴别机制，提供授权管理员鉴别数据的初始化功能,并确保仅允许授权管理员使用这些功能。

5.3.1.2.2　鉴别时机

在所有授权管理员请求执行的任何操作之前，协议隔离部件安全功能应确保对每个授权管理员进行了身份鉴别。

5.3.1.2.3　鉴别失败处理

在经过一定次数的鉴别失败以后，协议隔离部件安全功能应能终止进行登录尝试主机建立会话的过程。最多失败次数仅由授权管理员设定。

5.3.1.3　数据完整性

协议隔离部件安全功能应保护储存的鉴别数据和过滤策略不受未授权查阅、修改和破坏。

5.3.1.4　配置管理

开发者应为隔离部件产品的不同版本提供唯一的标识。

隔离部件产品的每个版本应当使用它们的唯一标识作为标签。

5.3.1.5　交付与运行

5.3.1.5.1　交付

开发者应使用一定的交付程序交付协议隔离部件，并将交付过程文档化。

交付文档应描述在给用户方交付协议隔离部件的各版本时，为维护安全所必需的所有程序。

5.3.1.5.2　安装生成

开发者应提供文档说明协议隔离部件的安装、生成和启动的过程。

5.3.1.6　安全功能开发过程

5.3.1.6.1　功能设计

开发者应提供隔离部件产品的安全功能设计。

功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能设计应是内在一致的并能完备地表示安全功能。

5.3.1.6.2　表示对应性

开发者应在隔离部件安全功能表示的所有相邻对之间提供对应性分析。

对于隔离部件安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.3.1.7　指导性文档

5.3.1.7.1　管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 隔离部件可以使用的管理功能和接口；
b) 怎样安全地管理隔离部件；
c) 在安全处理环境中应进行控制的功能和权限；
d) 所有对与隔离部件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。

管理员指南应与为评估而提供的其他所有文档保持一致。

5.3.1.7.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 隔离部件的非管理用户可使用的安全功能和接口；
b) 隔离部件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) 隔离部件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。

用户指南应与为评估而提供的其他所有文档保持一致。

5.3.1.8 测试

5.3.1.8.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明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。

5.3.1.8.2 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其它测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.3.1.9 生命周期支持

开发者应提供开发安全文件。

开发安全文件应描述在隔离部件的开发环境中，为保护隔离部件设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在隔离部件的开发和维护过程中执行安全措施的证据。

5.3.2 第二级

5.3.2.1 访问控制

5.3.2.1.1 安全属性定义

对于每一个授权管理员、构成系统的信息传输与控制部件、应用层数据采集与接受部件，协议隔离部件安全功能应为其提供一套唯一的、为了执行安全功能策略所必需的安全属性。

5.3.2.1.2 属性初始化

协议隔离部件安全功能应提供用默认值对授权管理员和主机属性初始化的能力。

5.3.2.1.3 属性修改

协议隔离部件安全功能应仅向授权管理员提供修改下述（包含但不仅限于）参数的能力：

标识与角色（例如：配置管理员等）的关系；

a) 数据采集与接收部件参数（例如：采集、接收部件主机的 IP 地址、应用服务参数等）；

b) 配置的安全参数（例如：最大鉴别失败次数等数据）。

5.3.2.1.4 属性查询

协议隔离部件安全功能应仅向授权管理员提供以下查询：

a) 数据采集与接收部件参数（例如：采集、接收部件主机的 IP 地址、应用服务参数等）；

b) 通过协议隔离部件传送信息的设备名。

5.3.2.1.5 访问授权与拒绝

协议隔离安全功能应根据数据发送方和接收方的安全属性值[主机名、IP 地址、预先定义的传输层协议和请求的服务（例如：源端口号或目的端口号）、应用层协议、应用数据关键字等]，提供明确的访问保障能力和拒绝访问能力。

5.3.2.1.6 不可旁路

在与安全有关的操作（例如安全属性的修改、内部网络主机向外部网络主机传送信息等）被允许执行之前，协议隔离部件安全功能应确保其通过安全功能策略的检查。

5.3.2.1.7 区分安全管理角色

协议隔离部件安全功能：

a) 应将与安全相关的管理功能与其他功能区分开；

b) 应包括安装、配置和管理隔离部件安全功能本身所需的所有功能，其中至少应包括：增加和删除主体（发送信息的主机）和客体（接受信息的主机），查阅安全属性，分配、修改和撤销安全属性，查阅和管理审计数据；

c) 应把执行与安全相关的管理功能的能力限定为一种安全管理职责，该职责具有一套特别授权的功能和响应的责任；

d) 应能把授权执行管理功能的授权管理员与使用隔离部件的所有其他个人或系统分开；

e) 应仅允许授权管理员承担安全管理职责；

f) 应在提出一个明确的请求以后，才会让授权管理员承担安全管理职责。

5.3.2.1.8 管理功能

协议隔离部件安全功能应向授权管理员提供如下管理功能：

a) 能设置和更新与安全相关的数据；

b) 能执行隔离部件的安装及初始化、系统启动和关闭、备份和恢复的能力，备份能力应有自动工具的支持；

c) 如果隔离部件安全功能支持外部或内部接口的远程管理，那么它应：

1) 具有对两个接口或其中之一关闭远程管理的选择权；

2) 能限制那些可进行远程管理的地址；

3) 能通过加密来保护远程管理对话。

5.3.2.2 身份鉴别

5.3.2.2.1 鉴别数据初始化

协议隔离部件安全功能应根据规定的鉴别机制,提供授权管理员鉴别数据的初始化功能,并确保仅允许授权管理员使用这些功能。

5.3.2.2.2 鉴别时机

在所有授权管理员请求执行的任何操作之前，协议隔离部件安全功能应确保对每个授权管理员进行了身份鉴别。

5.3.2.2.3 最少反馈

当进行鉴别时，协议隔离部件安全功能应仅将最少的反馈提供给用户。

5.3.2.2.4 鉴别失败处理

在经过一定次数的鉴别失败以后，协议隔离部件安全功能应能终止进行登录尝试主机建立会话的过程。最多失败次数仅由授权管理员设定。

5.3.2.3 客体重用

在为所有内部或外部网上的主机连接进行资源分配时，协议隔离部件安全功能应保证不提供以前连接的任何信息内容。

5.3.2.4 审计

5.3.2.4.1 审计数据生成

协议隔离部件安全功能应能对下列可审计事件生成一个审计记录：

a) 审计功能的启动和关闭；

b) 任何对审计记录进行操作的尝试，包括关闭审计功能或子系统，以及受影响客体的标识；

c) 任何读取、修改、破坏审计记录的尝试；

d) 所有对隔离部件规则覆盖的客体（内部或外部网络上的主机）执行操作的请求，以及受影响客体的标识；

e) 修改安全属性的所有尝试，以及修改后安全属性的新值；

f) 所有使用安全功能中鉴别数据管理机制的请求；

g) 所有访问鉴别数据的请求，以及访问请求的目标；

h) 任何对鉴别机制的使用；

i) 所有使用标识机制的尝试；

j) 所有对安全功能配置参数的修改（设置和更新），无论成功与否，以及配置参数的新值；

对于每一个审计记录，隔离部件安全功能应至少记录以下信息：事件发生的日期和时间，事件的类型，主体身份和成功或失败事件。

5.3.2.4.2 审计记录管理

协议隔离部件安全功能应使授权管理员能创建、存档、删除和清空审计记录。

5.3.2.4.3 可理解的格式

协议隔离部件安全功能应使存储于永久性审计记录中的所有审计数据可为人所理解。

5.3.2.4.4 限制审计记录访问

协议隔离部件安全功能应仅允许授权管理员访问审计记录。

5.3.2.4.5 可选择查阅审计

协议隔离部件安全功能应提供能按主体 ID（标识符）、客体 ID、日期、时间以及这些参数的逻辑组合等参数对审计数据进行查找和排序的审计查阅工具。

5.3.2.4.6 防止审计数据丢失

协议隔离部件安全功能应把生成的审计记录储存于一个永久性的审计记录中,并应限制由于故障

和攻击造成的审计事件丢失的数量；

对因故障或存储耗竭而导致审计数据丢失的最大审计存储容量，协议隔离部件的开发者应提供相应的分析结果。

5.3.2.5 数据完整性

协议隔离部件安全功能应保护储存于设备中的鉴别数据和信息传输策略不受未授权查阅、修改和破坏。

5.3.2.6 配置管理

5.3.2.6.1 配置管理能力

开发者应使用配置管理系统并提供配置管理文档，以及为隔离部件产品的不同版本提供唯一的标识。

配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项。

配置管理文档应包括配置清单和配置管理计划。在配置清单中，应对每一配置项给出相应的描述；在配置管理计划中，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。

配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效地维护的证据。

5.3.2.6.2 配置管理范围

开发者应提供配置管理文档。

配置管理文档应说明配置管理系统至少能跟踪：隔离部件实现表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档，并描述配置管理系统是如何跟踪配置项的。

5.3.2.7 交付与运行

5.3.2.7.1 交付

开发者应使用一定的交付程序交付协议隔离部件，并将交付过程文档化。

交付文档应描述在给用户方交付协议隔离部件的各版本时，为维护安全所必需的所有程序。

5.3.2.7.2 安装生成

开发者应提供文档说明协议隔离部件的安装、生成、启动和日志生成的过程。

5.3.2.8 安全功能开发过程

5.3.2.8.1 功能设计

开发者应提供隔离部件的安全功能设计。

功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能设计应是内在一致的并能完备地表示安全功能。

5.3.2.8.2 高层设计

开发者应提供隔离部件安全功能的高层设计。

高层设计应以非形式方法表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强隔离部件安全功能的子系统和其它子系统分开。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提供安全功能子系统的作用、例外情况和错误信息的细节。高层设计还应标识安全功能要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件或软件所实现的保护机制。

5.3.2.8.3 表示对应性

开发者应在隔离部件安全功能表示的所有相邻对之间提供对应性分析。

对于隔离部件安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.3.2.9 指导性文档

5.3.2.9.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 隔离部件管理员可以使用的管理功能和接口；
b) 怎样安全地管理隔离部件；
c) 在安全处理环境中应进行控制的功能和权限；
d) 所有对与隔离部件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。

管理员指南应与为评估而提供的其他所有文档保持一致。

5.3.2.9.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 隔离部件的非管理用户可使用的安全功能和接口；
b) 隔离部件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) 隔离部件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。

用户指南应与为评估而提供的其他所有文档保持一致。

5.3.2.10 生命周期支持

开发者应提供开发安全文件。

开发安全文件应描述在隔离部件的开发环境中，为保护隔离部件设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在隔离部件的开发和维护过程中执行安全措施的证据。

5.3.2.11 测试

5.3.2.11.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明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，**且该对应是完备的。**

5.3.2.11.2 测试深度

开发者应提供测试深度的分析。

在深度分析中，应说明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。

5.3.2.11.3 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其它测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.3.2.11.4 独立性测试

开发商应提供用于适合测试的产品，且提供的测试集合应与其自测产品功能时使用的测试集合相一致。

5.3.2.12 脆弱性评定

5.3.2.12.1 指南检查

开发者应提供指南性文档。

在指南性文档中，应确定对隔离部件的所有可能的操作方式（包括失败和操作失误后的操作）、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出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。指南性文档应是完备的、清晰的、一致的、合理的。

5.3.2.12.2 脆弱性分析

开发者应从用户可能破坏安全策略的明显途径出发，对隔离部件的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用隔离部件的环境中该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的隔离部件可以抵御明显的穿透性攻击。

5.3.3 第三级

5.3.3.1 访问控制

5.3.3.1.1 安全属性定义

对于每一个授权管理员、构成系统的信息传输与控制部件、应用层数据采集与接受部件，协议隔离部件安全功能应为其提供一套唯一的、为了执行安全功能策略所必需的安全属性。

5.3.3.1.2 属性初始化

协议隔离部件安全功能应提供用默认值对授权管理员和主机属性初始化的能力。

5.3.3.1.3 属性修改

协议隔离部件安全功能应仅向授权管理员提供修改下述（包含但不仅限于）参数的能力：

标识与角色（例如：配置管理员等）的关系；

a) 数据采集与接收部件参数（例如：采集、接收部件主机的 IP 地址、应用服务参数等）；

b) 配置的安全参数（例如：最大鉴别失败次数等数据）。

5.3.3.1.4 属性查询

协议隔离部件安全功能应仅向授权管理员提供以下查询：

a) 数据采集与接收部件参数（例如：采集、接收部件主机的 IP 地址、应用服务参数等）；

b) 通过协议隔离部件传送信息的设备名。

5.3.3.1.5 隔离部件强制访问控制

协议隔离部件安全功能应通过授权管理员和授权管理员控制的安全功能数据的敏感标记，控制授

权管理员对相关安全功能数据的直接访问。

5.3.3.1.6 访问授权与拒绝

协议隔离安全功能应根据数据发送方和接收方的安全属性值[主机名、IP 地址、预先定义的传输层协议和请求的服务（例如：源端口号或目的端口号）、应用层协议、应用数据关键字等]，提供明确的访问保障能力和拒绝访问能力。**若访问被拒绝，隔离部件应以有效手段实时通知授权管理员。**

5.3.3.1.7 安全功能区域分隔

为保护协议隔离部件安全功能免遭不可信主体（内部或外部网络上的主机）的干扰和篡改，协议隔离部件安全功能应为其自身的执行过程设定一个安全区域，并把协议隔离部件控制范围内的各个主体（内部或外部网络上的主机）的安全区域分隔开。

5.3.3.1.8 不可旁路

在与安全有关的操作（例如安全属性的修改、内部网络主机向外部网络主机传送信息等）被允许执行之前，协议隔离部件安全功能应确保其通过安全功能策略的检查。

5.3.3.1.9 区分安全管理角色

协议隔离部件安全功能：

a) 应将与安全相关的管理功能与其他功能区分开；
b) 应包括安装、配置和管理隔离部件安全功能本身所需的所有功能，其中至少应包括：增加和删除主体（发送信息的主机）和客体（接受信息的主机），查阅安全属性，分配、修改和撤销安全属性，查阅和管理审计数据；
c) 应把执行与安全相关的管理功能的能力限定为一种安全管理职责，该职责具有一套特别授权的功能和响应的责任；
d) 应能把授权执行管理功能的授权管理员与使用隔离部件的所有其他个人或系统分开；
e) 应仅允许授权管理员承担安全管理职责；
f) 应在提出一个明确的请求以后，才会让授权管理员承担安全管理职责。

5.3.3.1.10 管理功能

协议隔离部件安全功能应向授权管理员提供如下管理功能：

a) 能设置和更新与安全相关的数据；
b) 能执行隔离部件的安装及初始化、系统启动和关闭、备份和恢复的能力，备份能力应有自动工具的支持；
c) 如果隔离部件安全功能支持外部或内部接口的远程管理，那么它应：
   1) 有对两个接口或其中之一关闭远程管理的选择权；
   2) 限制那些可进行远程管理的地址；
   3) 通过加密来保护远程管理对话。

5.3.3.2 标记

协议隔离部件安全功能应维护与授权管理员以及授权管理员可直接访问的协议隔离部件中安全功能数据和存储客体相关的敏感标记。

5.3.3.3 身份鉴别

5.3.3.3.1 鉴别数据初始化

协议隔离部件安全功能应根据规定的鉴别机制，提供授权管理员鉴别数据的初始化功能,并确保仅允许授权管理员使用这些功能。

5.3.3.3.2 鉴别时机

在所有授权管理员请求执行的任何操作之前，协议隔离部件安全功能应确保对每个授权管理员进行了身份鉴别。

5.3.3.3.3 最少反馈

当进行鉴别时，协议隔离部件安全功能应仅将最少的反馈提供给用户。

5.3.3.3.4 多鉴别机制

协议隔离部件安全功能应提供多鉴别机制以支持用户多鉴别。

5.3.3.3.5 鉴别失败处理

在经过一定次数的鉴别失败以后，协议隔离部件安全功能应能终止进行登录尝试主机建立会话的过程。最多失败次数仅由授权管理员设定。

5.3.3.4 客体重用

在为所有内部或外部网上的主机连接进行资源分配时，协议隔离部件安全功能应保证不提供以前连接的任何信息内容。

5.3.3.5 审计

5.3.3.5.1 审计数据生成

协议隔离部件安全功能应能对下列可审计事件生成一个审计记录：

a) 审计功能的启动和关闭；
b) 任何对审计记录进行操作的尝试，包括关闭审计功能或子系统，以及受影响客体的标识；
c) 任何读取、修改、破坏审计记录的尝试；
d) 所有对隔离部件规则覆盖的客体（内部或外部网络上的主机）执行操作的请求，以及受影响客体的标识；
e) 修改安全属性的所有尝试，以及修改后安全属性的新值；
f) 所有使用安全功能中鉴别数据管理机制的请求；
g) 所有访问鉴别数据的请求，以及访问请求的目标；
h) 任何对鉴别机制的使用；
i) 所有使用标识机制的尝试；
j) 所有对安全功能配置参数的修改（设置和更新），无论成功与否，以及配置参数的新值；
k) 因鉴别尝试不成功的次数超出了设定的限制，导致的会话连接终止，以及会话连接使用的标识符。

对于每一个审计记录，隔离部件安全功能应至少记录以下信息：事件发生的日期和时间，事件的类型，主体身份和成功或失败事件。

5.3.3.5.2 用户身份关联

协议隔离部件安全功能应能将每个可审计事件与引起该事件的用户身份相关联。

5.3.3.5.3 审计记录管理

协议隔离部件安全功能应使授权管理员能创建、存档、删除和清空审计记录。

5.3.3.5.4 可理解的格式

协议隔离部件安全功能应使存储于永久性审计记录中的所有审计数据可为人所理解。

5.3.3.5.5 限制审计记录访问

协议隔离部件安全功能应仅允许授权管理员访问审计记录。

5.3.3.5.6 可选择查阅审计

协议隔离部件安全功能应提供能按主体 ID、客体 ID、日期、时间以及这些参数的逻辑组合等参数对审计数据进行查找和排序的审计查阅工具。

5.3.3.5.7 防止审计数据丢失

协议隔离部件安全功能：

a) 应把生成的审计记录储存于一个永久性的审计记录中,并应限制由于故障和攻击造成的审计事件丢失的数量；

b) **一旦审计存储容量达到事先规定的警戒值，应能发出警告信息，并保证在授权管理员所采取的审计行为以外,防止其他可审计行为的出现。**

对因故障或存储耗竭而导致审计数据丢失的最大审计存储容量，协议隔离部件的开发者应提供相应的分析结果。

5.3.3.6 数据完整性

协议隔离部件安全功能应保护储存于设备中的鉴别数据和信息传输策略不受未授权查阅、修改和破坏。

5.3.3.7 密码支持

协议隔离部件安全功能应保证其远程管理会话的加密符合国家密码主管部门的有关规定。

5.3.3.8 配置管理

5.3.3.8.1 配置管理自动化

开发者应使用配置管理系统，并提供配置管理计划。

配置管理系统应确保只有已授权开发人员才能对隔离部件产品实现进行修改，并支持隔离部件基本配置项的生成。

配置管理计划应描述在配置管理系统中使用的工具软件。

5.3.3.8.2 配置管理能力

开发者应使用配置管理系统并提供配置管理文档，以及为隔离部件产品的不同版本提供唯一的标识。

配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项，**还应支持隔离部件基本配置项的生成。**

配置管理文档应包括配置清单、配置管理计划**以及接受计划。**配置清单用来描述组成隔离部件的配置项。在配置管理计划中，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。**在接受计划中，应描述对修改过或新建的配置项进行接受的程序。**

配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效地维护的证据。

5.3.3.8.3 配置管理范围

开发者应提供配置管理文档。

配置管理文档应说明配置管理系统至少能跟踪：隔离部件实现表示、设计文档、测试文档、用户文档、管理员文档、配置管理文档**和安全缺陷，**并描述配置管理系统是如何跟踪配置项的。

5.3.3.9 交付和运行

5.3.3.9.1 交付

开发者应使用一定的交付程序交付协议隔离部件，并将交付过程文档化。

交付文档应包括以下内容：

a) 在给用户方交付协议隔离部件的各版本时，为维护安全所必需的所有程序；

b）开发者的向用户提供的协议隔离部件版本和用户收到的版本之间的差异以及如何监测对协议隔离部件的修改；

c）如何发现他人伪装成开发者修改用户的协议隔离部件。

5.3.3.9.2 安装生成

开发者应提供文档说明协议隔离部件的安装、生成、启动和日志生成的过程。

5.3.3.10 安全功能开发过程

5.3.3.10.1 功能设计

开发者应提供隔离部件的安全功能设计。

安全功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能设计应是内在一致的，能完备地表示安全功能，**并提供安全基本原理证明安全功能的表示是完备的。**

5.3.3.10.2 高层设计

开发者应提供隔离部件安全功能的高层设计。

高层设计应以非形式方法表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强隔离部件安全功能的子系统和其它子系统分开。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提供安全功能子系统的作用、例外情况和错误信息的细节。高层设计还应标识安全功能要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件或软件所实现的保护机制。

5.3.3.10.3 安全功能的实现

开发者应为选定的隔离部件安全功能子集提供实现表示。

实现表示应无歧义而且详细地定义隔离部件安全功能，使得不需要进一步的设计就能生成该安全功能的子集。实现表示应是内在一致的。

5.3.3.10.4 低层设计

开发者应提供隔离部件安全功能的低层设计。

低层设计应是非形式化、内在一致的。在描述隔离部件安全功能时，低层设计应采用模块术语，说明每一个安全功能模块的目的，并标识安全功能模块的所有接口和安全功能模块可为外部所见的接口，以及安全功能模块所有接口的目的与方法，适当时，还应提供接口的作用、例外情况和错误信息的细节。

低层设计还应包括以下内容：

a） 以安全功能性术语及模块的依赖性术语，定义模块间的相互关系；

b） 说明如何提供每一个安全策略的强化功能；

c） 说明如何将隔离部件加强安全策略的模块和其它模块分离开。

5.3.3.10.5 表示对应性

开发者应在隔离部件安全功能表示的所有相邻对之间提供对应性分析。

对于隔离部件安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.3.3.10.6 安全策略模型

开发者应提供安全策略模型并阐明安全功能设计和安全策略模型之间的对应性。

安全策略模型应是非形式化的。对于所有可以模型化的安全策略，在模型中应描述其规则和特性，并阐明该模型对所有可模型化的安全策略来说是一致的、完备的。在阐明隔离部件安全策略模型和安全功能设计之间的对应性时，应说明，所有安全功能设计中的安全功能对与安全策略模型是一致的、是完备的。

5.3.3.11 指导性文档

5.3.3.11.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 隔离部件管理员可以使用的管理功能和接口；

b) 怎样安全地管理隔离部件；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与隔离部件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。

管理员指南应与为评估而提供的其他所有文档保持一致。

5.3.3.11.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 隔离部件的非管理用户可使用的安全功能和接口；

b) 隔离部件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) 隔离部件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。

用户指南应与为评估而提供的其他所有文档保持一致。

5.3.3.12 生命周期支持

5.3.3.12.1 开发安全

开发者应提供开发安全文件。

开发安全文件应描述在隔离部件的开发环境中，为保护隔离部件设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在隔离部件的开发和维护过程中执行安全措施的证据。

5.3.3.12.2 生命周期模型

开发者应建立生命周期模型并提供生命周期定义文档。

在生命周期定义文档中，应描述用于开发和维护隔离部件的模型。为了对隔离部件开发和维护进行必要的控制，该模型应提供相应的支持。

5.3.3.12.3 工具和技术

开发者应标识用于开发隔离部件的工具，并对开发工具中已选择的依赖实现的选项文档化。

在开发工具文档中，应明确定义所有用于实现的开发工具和实现中每个语句的含义，以及所有基于实

现的选项的含义。

5.3.3.13　测试

5.3.3.13.1　范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明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，且该对应是完备的。

5.3.3.13.2　测试深度

开发者应提供测试深度的分析。

在深度分析中，应说明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。

5.3.3.13.3　功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其它测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.3.3.13.4　独立性测试

开发商应提供用于适合测试的产品，且提供的测试集合应与其自测产品功能时使用的测试集合相一致。

5.3.3.14　脆弱性评定

5.3.3.14.1　指南检查

在指南性文档中，应确定对隔离部件的所有可能的操作方式（包括失败和操作失误后的操作）、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出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。指南性文档应是完备的、清晰的、一致的、合理的。**在分析文档中，应阐明指南性文档是完备的。**

5.3.3.14.2　脆弱性分析

开发者应从用户可能破坏安全策略的明显途径出发，对隔离部件的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用隔离部件的环境中该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的隔离部件可以抵御明显的穿透性攻击。

5.4　网闸隔离部件

5.4.1　第一级

5.4.1.1　访问控制

5.4.1.1.1　安全属性定义

对于每一个授权管理员、构成系统的信息传输与控制部件和主机，网闸隔离部件安全功能应为其提供一套唯一的、为了执行安全功能策略所必需的安全属性。

5.4.1.1.2　属性初始化

网闸隔离部件安全功能应提供用默认值对授权管理员和主机属性初始化的能力。

5.4.1.1.3　属性修改

网闸隔离部件安全功能应仅向授权管理员提供修改下述（包含但不仅限于）参数的能力：

标识与角色（例如：配置管理员等）的关系；

a) 源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）；

b) 配置的安全参数（例如：最大鉴别失败次数等数据）。

5.4.1.1.4 属性查询

网闸隔离部件安全功能应仅向授权管理员提供以下查询：

a) 源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）；

b) 通过网闸隔离部件传送信息的主机信息。

5.4.1.1.5 访问授权与拒绝

网闸隔离部件安全功能应根据主体和客体的安全属性值[源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号）、应用层协议、应用层关键字等]，提供明确的访问保障能力和拒绝访问能力。网闸隔离部件还应对内外网数据传输链路进行物理上的时分切换，既内外网络在物理链路上不能同时与中间交换单元连通。

5.4.1.2 身份鉴别

5.4.1.2.1 鉴别数据初始化

网闸隔离部件安全功能应根据规定的鉴别机制，提供授权管理员鉴别数据的初始化功能,并确保仅允许授权管理员使用这些功能。

5.4.1.2.2 鉴别时机

在所有授权管理员请求执行的任何操作之前，网闸隔离部件安全功能应确保对每个授权管理员进行了身份鉴别。

5.4.1.2.3 鉴别失败处理

在经过一定次数的鉴别失败以后，网闸隔离部件安全功能应能终止进行登录尝试主机建立会话的过程。最多失败次数仅由授权管理员设定。

5.4.1.3 数据完整性

网闸隔离部件安全功能应保护储存的鉴别数据和过滤策略不受未授权查阅、修改和破坏。

5.4.1.4 配置管理

开发者应为隔离部件产品的不同版本提供唯一的标识。

隔离部件产品的每个版本应当使用它们的唯一标识作为标签。

5.4.1.5 交付与运行

5.4.1.5.1 交付

开发者应使用一定的交付程序交付网闸隔离部件，并将交付过程文档化。

交付文档应描述在给用户方交付网闸隔离部件的各版本时，为维护安全所必需的所有程序。

5.4.1.5.2 安装生成

开发者应提供文档说明网闸隔离部件的安装、生成和启动的过程。

5.4.1.6 安全功能开发过程

5.4.1.6.1 功能设计

开发者应提供隔离部件产品的安全功能设计。

功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与

方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能设计应是内在一致的并能完备地表示安全功能。

5.4.1.6.2 表示对应性

开发者应在隔离部件安全功能表示的所有相邻对之间提供对应性分析。

对于隔离部件安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.4.1.7 指导性文档

5.4.1.7.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 隔离部件可以使用的管理功能和接口；

b) 怎样安全地管理隔离部件；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与隔离部件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。

管理员指南应与为评估而提供的其他所有文档保持一致。

5.4.1.7.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 隔离部件的非管理用户可使用的安全功能和接口；

b) 隔离部件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) 隔离部件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。

用户指南应与为评估而提供的其他所有文档保持一致。

5.4.1.8 测试

5.4.1.8.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明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。

5.4.1.8.2 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其它测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.4.1.9 生命周期支持

开发者应提供开发安全文件。

开发安全文件应描述在隔离部件的开发环境中，为保护隔离部件设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在隔离部件的开发和维护过程中执行安全措施的证据。

5.4.2 第二级

5.4.2.1 访问控制

5.4.2.1.1 安全属性定义

对于每一个授权管理员、构成系统的信息传输与控制部件和主机，网闸隔离部件安全功能应为其提供一套唯一的、为了执行安全功能策略所必需的安全属性。

5.4.2.1.2 属性初始化

网闸隔离部件安全功能应提供用默认值对授权管理员和主机属性初始化的能力。

5.4.2.1.3 属性修改

网闸隔离部件安全功能应仅向授权管理员提供修改下述（包含但不仅限于）参数的能力：

标识与角色（例如：配置管理员等）的关系；

a) 源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）；

b) 配置的安全参数（例如：最大鉴别失败次数等数据）。

5.4.2.1.4 属性查询

网闸隔离部件安全功能应仅向授权管理员提供以下查询：

a) 源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）；

b) 通过网闸隔离部件传送信息的主机信息。

5.4.2.1.5 访问授权与拒绝

网闸隔离部件安全功能应根据主体和客体的安全属性值[源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号）、应用层协议、应用层关键字等]，提供明确的访问保障能力和拒绝访问能力。网闸隔离部件还应对内外网数据传输链路进行物理上的时分切换，既内外网络在物理链路上不能同时与中间交换单元连通。

5.4.2.1.6 不可旁路

在与安全有关的操作（例如安全属性的修改、内部网络主机向外部网络主机传送信息等）被允许执行之前，网闸隔离部件安全功能应确保其通过安全功能策略的检查。

5.4.2.1.7 区分安全管理角色

网闸隔离部件安全功能：

a) 应将与安全相关的管理功能与其他功能区分开；

b) 应包括安装、配置和管理隔离部件安全功能本身所需的所有功能，其中至少应包括：增加和删除主体（发送信息的主机）和客体（接受信息的主机），查阅安全属性，分配、修改和撤销安全属性，查阅和管理审计数据；

c) 应把执行与安全相关的管理功能的能力限定为一种安全管理职责，该职责具有一套特别授权的功能和响应的责任；

d) 应能把授权执行管理功能的授权管理员与使用隔离部件的所有其他个人或系统分开；

e） 应仅允许授权管理员承担安全管理职责；

f） 应在提出一个明确的请求以后，才会让授权管理员承担安全管理职责。

5.4.2.1.8 管理功能

网闸隔离部件安全功能应向授权管理员提供如下管理功能：

a） 能设置和更新与安全相关的数据；

b） 能执行隔离部件的安装及初始化、系统启动和关闭、备份和恢复的能力，备份能力应有自动工具的支持；

c） 如果隔离部件安全功能支持外部或内部接口的远程管理，那么它应：

1） 具有对两个接口或其中之一关闭远程管理的选择权；

2） 能限制那些可进行远程管理的地址；

3） 能通过加密来保护远程管理对话。

5.4.2.2 身份鉴别

5.4.2.2.1 鉴别数据初始化

网闸隔离部件安全功能应根据规定的鉴别机制，提供授权管理员鉴别数据的初始化功能，并确保仅允许授权管理员使用这些功能。

5.4.2.2.2 鉴别时机

在所有授权管理员请求执行的任何操作之前，网闸隔离部件安全功能应确保对每个授权管理员进行了身份鉴别。

5.4.2.2.3 最少反馈

当进行鉴别时，网闸隔离部件安全功能应仅将最少的反馈提供给用户。

5.4.2.2.4 鉴别失败处理

在经过一定次数的鉴别失败以后，网闸隔离部件安全功能应能终止进行登录尝试主机建立会话的过程。最多失败次数仅由授权管理员设定。

5.4.2.3 客体重用

在为所有内部或外部网上的主机连接进行资源分配时，隔离部件安全功能应保证不提供以前连接的任何信息内容。

5.4.2.4 审计

5.4.2.4.1 审计数据生成

网闸隔离部件安全功能应能对下列可审计事件生成一个审计记录：

a） 审计功能的启动和关闭；

b） 任何对审计记录进行操作的尝试，包括关闭审计功能或子系统，以及受影响客体的标识；

c） 任何读取、修改、破坏审计记录的尝试；

d） 所有对隔离部件规则覆盖的客体（内部或外部网络上的主机）执行操作的请求，以及受影响客体的标识；

e） 修改安全属性的所有尝试，以及修改后安全属性的新值；

f） 所有使用安全功能中鉴别数据管理机制的请求；

g） 所有访问鉴别数据的请求，以及访问请求的目标；

h） 任何对鉴别机制的使用；

i） 所有使用标识机制的尝试；

j） 所有对安全功能配置参数的修改（设置和更新），无论成功与否，以及配置参数的新值；

对于每一个审计记录，隔离部件安全功能应至少记录以下信息：事件发生的日期和时间，事件的类型，主体身份和成功或失败事件。

5.4.2.4.2 审计记录管理

网闸隔离部件安全功能应使授权管理员能创建、存档、删除和清空审计记录。

5.4.2.4.3 可理解的格式

网闸隔离部件安全功能应使存储于永久性审计记录中的所有审计数据可为人所理解。

5.4.2.4.4 限制审计记录访问

网闸隔离部件安全功能应仅允许授权管理员访问审计记录。

5.4.2.4.5 可选择查阅审计

网闸隔离部件安全功能应提供能按主体 ID（标识符）、客体 ID、日期、时间以及这些参数的逻辑组合等参数对审计数据进行查找和排序的审计查阅工具。

5.4.2.4.6 防止审计数据丢失

网闸隔离部件安全功能应把生成的审计记录储存于一个永久性的审计记录中,并应限制由于故障和攻击造成的审计事件丢失的数量；

对因故障或存储耗竭而导致审计数据丢失的最大审计存储容量，网闸隔离部件的开发者应提供相应的分析结果。

5.4.2.5 数据完整性

网闸隔离部件安全功能应保护储存于设备中的鉴别数据和信息传输策略不受未授权查阅、修改和破坏。

5.4.2.6 配置管理

5.4.2.6.1 配置管理能力

开发者应使用配置管理系统并提供配置管理文档，以及为隔离部件产品的不同版本提供唯一的标识。

配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项。

配置管理文档应包括配置清单和配置管理计划。在配置清单中，应对每一配置项给出相应的描述；在配置管理计划中，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。

配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效地维护的证据。

5.4.2.6.2 配置管理范围

开发者应提供配置管理文档。

配置管理文档应说明配置管理系统至少能跟踪：隔离部件实现表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档，并描述配置管理系统是如何跟踪配置项的。

5.4.2.7 交付与运行

5.4.2.7.1 交付

开发者应使用一定的交付程序交付网闸隔离部件，并将交付过程文档化。

交付文档应描述在给用户方交付网闸隔离部件的各版本时，为维护安全所必需的所有程序。

5.4.2.7.2 安装生成

开发者应提供文档说明网闸隔离部件的安装、生成、启动和日志生成的过程。

5.4.2.8 安全功能开发过程

5.4.2.8.1 功能设计

开发者应提供隔离部件的安全功能设计。

功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能设计应是内在一致的并能完备地表示安全功能。

5.4.2.8.2 高层设计

开发者应提供隔离部件安全功能的高层设计。

高层设计应以非形式方法表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强隔离部件安全功能的子系统和其它子系统分开。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提供安全功能子系统的作用、例外情况和错误信息的细节。高层设计还应标识安全功能要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件或软件所实现的保护机制。

5.4.2.8.3 表示对应性

开发者应在隔离部件安全功能表示的所有相邻对之间提供对应性分析。

对于隔离部件安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.4.2.9 指导性文档

5.4.2.9.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 隔离部件管理员可以使用的管理功能和接口；
b) 怎样安全地管理隔离部件；
c) 在安全处理环境中应进行控制的功能和权限；
d) 所有对与隔离部件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。

管理员指南应与为评估而提供的其他所有文档保持一致。

5.4.2.9.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 隔离部件的非管理用户可使用的安全功能和接口；
b) 隔离部件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) 隔离部件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。

用户指南应与为评估而提供的其他所有文档保持一致。

5.4.2.10 生命周期支持

开发者应提供开发安全文件。

开发安全文件应描述在隔离部件的开发环境中，为保护隔离部件设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在隔离部件的开发和维护过程中执行安全措施的证据。

5.4.2.11 测试

5.4.2.11.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明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，**且该对应是完备的。**

5.4.2.11.2 测试深度

开发者应提供测试深度的分析。

在深度分析中，应说明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。

5.4.2.11.3 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其它测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.4.2.11.4 独立性测试

开发商应提供用于适合测试的产品，且提供的测试集合应与其自测产品功能时使用的测试集合相一致。

5.4.2.12 脆弱性评定

5.4.2.12.1 指南检查

开发者应提供指南性文档。

在指南性文档中，应确定对隔离部件的所有可能的操作方式（包括失败和操作失误后的操作）、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出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。指南性文档应是完备的、清晰的、一致的、合理的。

5.4.2.12.2 脆弱性分析

开发者应从用户可能破坏安全策略的明显途径出发，对隔离部件的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用隔离部件的环境中该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的隔离部件可以抵御明显的穿透性攻击。

5.4.3 第三级

5.4.3.1 访问控制

5.4.3.1.1 安全属性定义

对于每一个授权管理员、构成系统的信息传输与控制部件和主机，网闸隔离部件安全功能应为其提供一套唯一的、为了执行安全功能策略所必需的安全属性。

5.4.3.1.2 属性初始化

网闸隔离部件安全功能应提供用默认值对授权管理员和主机属性初始化的能力。

5.4.3.1.3 属性修改

网闸隔离部件安全功能应仅向授权管理员提供修改下述（包含但不仅限于）参数的能力：

标识与角色（例如：配置管理员等）的关系；

a) 源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）；

b) 配置的安全参数（例如：最大鉴别失败次数等数据）。

5.4.3.1.4 属性查询

网闸隔离部件安全功能应仅向授权管理员提供以下查询：

a) 源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）；

b) 通过网闸隔离部件传送信息的主机信息。

5.4.3.1.5 客体访问控制策略

对于网闸隔离部件的主体（未经网闸隔离部件鉴别的发送信息的主机）和客体（内部或外部网上的接收信息的主机）以及安全功能策略（SFP）所包括的主体、客体的所有操作，网闸隔离部件安全功能应执行未鉴别的端到端策略，并确保安全功能策略包括了控制范围中的任何主体和客体之间的所有操作。

5.4.3.1.6 隔离部件强制访问控制

网闸隔离部件安全功能应通过授权管理员和授权管理员控制的安全功能数据的敏感标记，控制授权管理员对相关安全功能数据的直接访问。

5.4.3.1.7 访问授权与拒绝

网闸隔离部件安全功能应根据主体和客体的安全属性值[源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号）、应用层协议、应用层关键字、**应用层通讯模式**等]，提供明确的访问保障能力和拒绝访问能力。网闸隔离部件还应对内外网数据传输链路进行物理上的时分切换，既内外网络在物理链路上不能同时与中间交换单元连通。**若访问被拒绝，隔离部件应以有效手段实时通知授权管理员。**

5.4.3.1.8 安全功能区域分隔

为保护网闸隔离部件安全功能免遭不可信主体（内部或外部网络上的主机）的干扰和篡改，网闸隔离部件安全功能应为其自身的执行过程设定一个安全区域，并把网闸隔离部件控制范围内的各个主体（内部或外部网络上的主机）的安全区域分隔开。

5.4.3.1.9 不可旁路

在与安全有关的操作（例如安全属性的修改、内部网络主机向外部网络主机传送信息等）被允许执行之前，网闸隔离部件安全功能应确保其通过安全功能策略的检查。

5.4.3.1.10 区分安全管理角色

网闸隔离部件安全功能：

a) 应将与安全相关的管理功能与其他功能区分开；

b) 应包括安装、配置和管理隔离部件安全功能本身所需的所有功能，其中至少应包括：增加和删除主体（发送信息的主机）和客体（接受信息的主机），查阅安全属性，分配、修改和撤销

安全属性，查阅和管理审计数据；

c） 应把执行与安全相关的管理功能的能力限定为一种安全管理职责，该职责具有一套特别授权的功能和响应的责任；

d） 应能把授权执行管理功能的授权管理员与使用隔离部件的所有其他个人或系统分开；

e） 应仅允许授权管理员承担安全管理职责；

f） 应在提出一个明确的请求以后，才会让授权管理员承担安全管理职责。

5.4.3.1.11 管理功能

网闸隔离部件安全功能应向授权管理员提供如下管理功能：

a) 能设置和更新与安全相关的数据；

b) 能执行隔离部件的安装及初始化、系统启动和关闭、备份和恢复的能力，备份能力应有自动工具的支持；

c) 如果隔离部件安全功能支持外部或内部接口的远程管理，那么它应：

1) 有对两个接口或其中之一关闭远程管理的选择权；

2) 限制那些可进行远程管理的地址；

3) 通过加密来保护远程管理对话。

5.4.3.2 标记

网闸隔离部件安全功能应维护与授权管理员以及授权管理员可直接访问的网闸隔离部件中安全功能数据和存储客体相关的敏感标记。

5.4.3.3 身份鉴别

5.4.3.3.1 鉴别数据初始化

网闸隔离部件安全功能应根据规定的鉴别机制，提供授权管理员鉴别数据的初始化功能,并确保仅允许授权管理员使用这些功能。

5.4.3.3.2 鉴别时机

在所有授权管理员请求执行的任何操作之前，网闸隔离部件安全功能应确保对每个授权管理员进行了身份鉴别。

5.4.3.3.3 最少反馈

当进行鉴别时，网闸隔离部件安全功能应仅将最少的反馈提供给用户。

5.4.3.3.4 多鉴别机制

网闸隔离部件安全功能应提供多鉴别机制以支持用户多鉴别。

5.4.3.3.5 鉴别失败处理

在经过一定次数的鉴别失败以后，网闸隔离部件安全功能应能终止进行登录尝试主机建立会话的过程。最多失败次数仅由授权管理员设定。

5.4.3.4 客体重用

在为所有内部或外部网上的主机连接进行资源分配时，网闸隔离部件安全功能应保证不提供以前连接的任何信息内容。

5.4.3.5 审计

5.4.3.5.1 审计数据生成

网闸隔离部件安全功能应能对下列可审计事件生成一个审计记录：

a) 审计功能的启动和关闭；

b) 任何对审计记录进行操作的尝试，包括关闭审计功能或子系统，以及受影响客体的标识；

c) 任何读取、修改、破坏审计记录的尝试；

d) 所有对隔离部件规则覆盖的客体（内部或外部网络上的主机）执行操作的请求，以及受影响客体的标识；

e) 修改安全属性的所有尝试，以及修改后安全属性的新值；

f) 所有使用安全功能中鉴别数据管理机制的请求；

g) 所有访问鉴别数据的请求，以及访问请求的目标；

h) 任何对鉴别机制的使用；

i) 所有使用标识机制的尝试；

j) 所有对安全功能配置参数的修改（设置和更新），无论成功与否，以及配置参数的新值；

k) 因鉴别尝试不成功的次数超出了设定的限制，导致的会话连接终止，以及会话连接使用的标识符。

对于每一个审计记录，隔离部件安全功能应至少记录以下信息：事件发生的日期和时间，事件的类型，主体身份和成功或失败事件。

5.4.3.5.2 用户身份关联

网闸隔离部件安全功能应能将每个可审计事件与引起该事件的用户身份相关联。

5.4.3.5.3 审计记录管理

网闸隔离部件安全功能应使授权管理员能创建、存档、删除和清空审计记录。

5.4.3.5.4 可理解的格式

网闸隔离部件安全功能应使存储于永久性审计记录中的所有审计数据可为人所理解。

5.4.3.5.5 限制审计记录访问

网闸隔离部件安全功能应仅允许授权管理员访问审计记录。

5.4.3.5.6 可选择查阅审计

网闸隔离部件安全功能应提供能按主体 ID、客体 ID、日期、时间以及这些参数的逻辑组合等参数对审计数据进行查找和排序的审计查阅工具。

5.4.3.5.7 防止审计数据丢失

网闸隔离部件安全功能：

a) 应把生成的审计记录储存于一个永久性的审计记录中,并应限制由于故障和攻击造成的审计事件丢失的数量；

b) 一旦审计存储容量达到事先规定的警戒值，应能发出警告信息，并保证在授权管理员所采取的审计行为以外,防止其他可审计行为的出现。

对因故障或存储耗竭而导致审计数据丢失的最大审计存储容量，网闸隔离部件的开发者应提供相应的分析结果。

5.4.3.6 数据完整性

网闸隔离部件安全功能应保护储存于设备中的鉴别数据和信息传输策略不受未授权查阅、修改和破坏。

5.4.3.7 密码支持

网闸隔离部件安全功能应保证其远程管理会话的加密符合国家密码主管部门的有关规定。

5.4.3.8 配置管理

5.4.3.8.1 配置管理自动化

开发者应使用配置管理系统，并提供配置管理计划。

配置管理系统应确保只有已授权开发人员才能对隔离部件产品实现进行修改，并支持隔离部件基本配置项的生成。

配置管理计划应描述在配置管理系统中使用的工具软件。

5.4.3.8.2 配置管理能力

开发者应使用配置管理系统并提供配置管理文档，以及为隔离部件产品的不同版本提供唯一的标识。

配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项，**还应支持隔离部件基本配置项的生成。**

配置管理文档应包括配置清单、配置管理计划**以及接受计划。**配置清单用来描述组成隔离部件的配置项。在配置管理计划中，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。**在接受计划中，应描述对修改过或新建的配置项进行接受的程序。**

配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效地维护的证据。

5.4.3.8.3 配置管理范围

开发者应提供配置管理文档。

配置管理文档应说明配置管理系统至少能跟踪：隔离部件实现表示、设计文档、测试文档、用户文档、管理员文档、配置管理文档**和安全缺陷，**并描述配置管理系统是如何跟踪配置项的。

5.4.3.9 交付和运行

5.4.3.9.1 交付

开发者应使用一定的交付程序交付网闸隔离部件，并将交付过程文档化。

交付文档应包括以下内容：

a) 在给用户方交付网闸隔离部件的各版本时，为维护安全所必需的所有程序；

b) **开发者的向用户提供的网闸隔离部件版本和用户收到的版本之间的差异以及如何监测对网闸隔离部件的修改；**

c) **如何发现他人伪装成开发者修改用户的网闸隔离部件。**

5.4.3.9.2 安装生成

开发者应提供文档说明网闸隔离部件的安装、生成、启动和日志生成的过程。

5.4.3.10 安全功能开发过程

5.4.3.10.1 功能设计

开发者应提供隔离部件的安全功能设计。

安全功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能设计应是内在一致的，能完备地表示安全功能，**并提供安全基本原理证明安全功能的表示是完备的。**

5.4.3.10.2 高层设计

开发者应提供隔离部件安全功能的高层设计。

高层设计应以非形式方法表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强隔离部件安全功能的子系统和其它子系统分开。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及

哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提供安全功能子系统的作用、例外情况和错误信息的细节。高层设计还应标识安全功能要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件或软件所实现的保护机制。

5.4.3.10.3 安全功能的实现

开发者应为选定的隔离部件安全功能子集提供实现表示。

实现表示应无歧义而且详细地定义隔离部件安全功能，使得不需要进一步的设计就能生成该安全功能的子集。实现表示应是内在一致的。

5.4.3.10.4 低层设计

开发者应提供隔离部件安全功能的低层设计。

低层设计应是非形式化、内在一致的。在描述隔离部件安全功能时，低层设计应采用模块术语，说明每一个安全功能模块的目的，并标识安全功能模块的所有接口和安全功能模块可为外部所见的接口，以及安全功能模块所有接口的目的与方法，适当时，还应提供接口的作用、例外情况和错误信息的细节。

低层设计还应包括以下内容：

a) 以安全功能性术语及模块的依赖性术语，定义模块间的相互关系；

b) 说明如何提供每一个安全策略的强化功能；

c) 说明如何将隔离部件加强安全策略的模块和其它模块分离开。

5.4.3.10.5 表示对应性

开发者应在隔离部件安全功能表示的所有相邻对之间提供对应性分析。

对于隔离部件安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.4.3.10.6 安全策略模型

开发者应提供安全策略模型并阐明安全功能设计和安全策略模型之间的对应性。

安全策略模型应是非形式化的。对于所有可以模型化的安全策略，在模型中应描述其规则和特性，并阐明该模型对所有可模型化的安全策略来说是一致的、完备的。在阐明隔离部件安全策略模型和安全功能设计之间的对应性时，应说明，所有安全功能设计中的安全功能对与安全策略模型是一致的、是完备的。

5.4.3.11 指导性文档

5.4.3.11.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 隔离部件管理员可以使用的管理功能和接口；

b) 怎样安全地管理隔离部件；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与隔离部件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。

管理员指南应与为评估而提供的其他所有文档保持一致。

5.4.3.11.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 隔离部件的非管理用户可使用的安全功能和接口；

b) 隔离部件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) 隔离部件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。

用户指南应与为评估而提供的其他所有文档保持一致。

5.4.3.12 生命周期支持

5.4.3.12.1 开发安全

开发者应提供开发安全文件。

开发安全文件应描述在隔离部件的开发环境中，为保护隔离部件设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在隔离部件的开发和维护过程中执行安全措施的证据。

5.4.3.12.2 生命周期模型

开发者应建立生命周期模型并提供生命周期定义文档。

在生命周期定义文档中，应描述用于开发和维护隔离部件的模型。为了对隔离部件开发和维护进行必要的控制，该模型应提供相应的支持。

5.4.3.12.3 工具和技术

开发者应标识用于开发隔离部件的工具，并对开发工具中已选择的依赖实现的选项文档化。

在开发工具文档中，应明确定义所有用于实现的开发工具和实现中每个语句的含义，以及所有基于实现的选项的含义。

5.4.3.13 测试

5.4.3.13.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明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，且该对应是完备的。

5.4.3.13.2 测试深度

开发者应提供测试深度的分析。

在深度分析中，应说明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。

5.4.3.13.3 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其它测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.4.3.13.4 独立性测试

开发商应提供用于适合测试的产品，且提供的测试集合应与其自测产品功能时使用的测试集合相一致。

5.4.3.14　脆弱性评定

5.4.3.14.1　指南检查

在指南性文档中，应确定对隔离部件的所有可能的操作方式（包括失败和操作失误后的操作）、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出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。指南性文档应是完备的、清晰的、一致的、合理的。**在分析文档中，应阐明指南性文档是完备的。**

5.4.3.14.2　脆弱性分析

开发者应从用户可能破坏安全策略的明显途径出发，对隔离部件的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用隔离部件的环境中该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的隔离部件可以抵御明显的穿透性攻击。

参考文献

[1] GB/T 18336-2001 信息技术 安全技术 信息技术安全性评估准则
[2] GA 370-2001 端设备隔离部件安全技术要求
[3] GA/T 390-2002 计算机信息系统安全等级保护通用技术要求