6.3 设计技术要求

6.3.1 安全计算环境设计技术要求

6.3.1.1 通用安全计算环境设计技术要求

本项要求包括：

a) 用户身份鉴别

应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份；在每次用户登录系统时，采用口令鉴别机制进行用户身份鉴别，并对口令数据进行保护。

b) 自主访问控制

应在安全策略控制范围内，使用户/用户组对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户/用户组。访问控制主体的粒度为用户/用户组级，客体的粒度为文件或数据库表级。访问操作包括对客体的创建、读、写、修改和删除等。

c) 用户数据完整性保护

可采用常规校验机制，检验存储的用户数据的完整性，以发现其完整性是否被破坏。

d) 恶意代码防范

应安装防恶意代码软件或配置具有相应安全功能的操作系统，并定期进行升级和更新，以防范和清除恶意代码。

e) 可信验证

可基于可信根对计算节点的 BIOS、引导程序、操作系统内核等进行可信验证，并在检测到其可信性受到破坏后进行报警。

6.3.1.2 云安全计算环境设计技术要求

本项要求包括：

a) 用户账号保护

应支持建立云租户账号体系，实现主体对虚拟机、云数据库、云网络、云存储等客体的访问授权。

b) 虚拟化安全

应禁止虚拟机对宿主机物理资源的直接访问；应支持不同云租户虚拟化网络之间安全隔离。

c) 恶意代码防范

物理机和宿主机应安装经过安全加固的操作系统或进行主机恶意代码防范。

6.3.1.3 移动互联安全计算环境设计技术要求

本项要求包括：

a) 用户身份鉴别

应采用口令、解锁图案以及其他具有相应安全强度的机制进行用户身份鉴别。

b) 应用管控

应提供应用程序签名认证机制，拒绝未经过认证签名的应用软件安装和执行。

6.3.1.4 物联网系统安全计算环境设计技术要求

本项要求包括：

a) 感知层设备身份鉴别

应采用常规鉴别机制对感知设备身份进行鉴别，确保数据来源于正确的感知设备。

b） 感知层设备访问控制

应通过制定安全策略如访问控制列表，实现对感知设备的访问控制。

6.3.1.5 工业控制系统安全计算环境设计技术要求

本项要求包括：

a） 工业控制身份鉴别

现场控制层设备及过程监控层设备应实施唯一性的标志、鉴别与认证，保证鉴别认证与功能完整性状态随时能得到实时验证与确认。在控制设备及监控设备上运行的程序、相应的数据集合应有唯一性标识管理。

b） 现场设备访问控制

应对通过身份鉴别的用户实施基于角色的访问控制策略，现场设备收到操作命令后，应检验该用户绑定的角色是否拥有执行该操作的权限，拥有权限的该用户获得授权，用户未获授权应向上层发出报警信息。

c） 控制过程完整性保护

应在规定的时间内完成规定的任务，数据应以授权方式进行处理，确保数据不被非法篡改、不丢失、不延误，确保及时响应和处理事件。

6.3.2 安全区域边界设计技术要求

6.3.2.1 通用安全区域边界设计技术要求

本项要求包括：

a） 区域边界包过滤

可根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议和请求的服务等，确定是否允许该数据包通过该区域边界。

b） 区域边界恶意代码防范

可在安全区域边界设置防恶意代码软件，并定期进行升级和更新，以防止恶意代码入侵。

c） 可信验证

可基于可信根对区域边界计算节点的BIOS、引导程序、操作系统内核等进行可信验证，并在检测到其可信性受到破坏后进行报警。

6.3.2.2 云安全区域边界设计技术要求

本项要求包括：

a） 区域边界结构安全

应保证虚拟机只能接收到目的地址包括自己地址的报文或业务需求的广播报文，同时限制广播攻击。

b） 区域边界访问控制

应保证当虚拟机迁移时，访问控制策略随其迁移。

6.3.2.3 移动互联安全区域边界设计技术要求

应遵守 6.3.2.1。

6.3.2.4 物联网系统安全区域边界设计技术要求

应遵守 6.3.2.1。

6.3.2.5 工业控制系统区域边界设计技术要求

应遵守 6.3.2.1。

6.3.3 安全通信网络设计技术要求

6.3.3.1 通用安全通信网络设计技术要求

本项要求包括：

a) 通信网络数据传输完整性保护

可采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护。

b) 可信连接验证

通信节点应采用具有网络可信连接保护功能的系统软件或可信根支撑的信息技术产品，在设备连接网络时，对源和目标平台身份进行可信验证。

6.3.3.2 云安全通信网络设计技术要求

应遵守6.3.3.1。

6.3.3.3 移动互联安全通信网络设计技术要求

应遵守6.3.3.1。

6.3.3.4物联系统安全通信网络设计技术要求

应遵守6.3.3.1。

6.3.3.5 工业控制系统安全通信网络设计技术要求

应遵守6.3.3.1。

7 第二级系统安全保护环境设计

7.1 设计目标

第二级系统安全保护环境的设计目标是：按照GB 17859-1999对第二级系统的安全保护要求，在第一级系统安全保护环境的基础上，增加系统安全审计、客体重用等安全功能，并实施以用户为基本粒度的自主访问控制，使系统具有更强的自主安全保护能力，并保障基础计算资源和应用程序可信。

7.2 设计策略

第二级系统安全保护环境的设计策略是：遵循GB 17859—1999的4.2中相关要求，以身份鉴别为基础，提供单个用户和(或)用户组对共享文件、数据库表等的自主访问控制；以包过滤手段提供区域边界保护；以数据校验和恶意代码防范等手段，同时通过增加系统安全审计、客体安全重用等功能，使用户对自己的行为负责，提供用户数据保密性和完整性保护，以增强系统的安全保护能力。第二级系统安全保护环境在使用密码技术设计时，应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准。

第二级系统安全保护环境的设计通过第二级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。计算节点都应基于可信根实现开机到操作系统启动，再到应用程序启动的可信验证，并将验证结果形成审计记录。

7.3 设计技术要求

7.3.1 安全计算环境设计技术要求

7.3.1.1 通用安全计算环境设计技术要求

本项要求包括：

a) 用户身份鉴别

应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，**并确保在系统整个生存周期用户标识的唯一性**；在每次用户登录系统时，采用**受控的口令或具有相应安全强度的其他机制**进行用户身份鉴别，并使用密码技术对鉴别数据进行**保密性和完整性**保护。

b) 自主访问控制

应在安全策略控制范围内，使**用户**对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他**用户**。访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。访问操作包括对客体的创建、读、写、修改和删除等。

c) 系统安全审计

应提供安全审计机制，记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。该机制应提供审计记录查询、分类和存储保护，并可由安全管理中心管理。

d) 用户数据完整性保护

可采用常规校验机制，检验存储的用户数据的完整性，以发现其完整性是否被破坏。

e) 用户数据保密性保护

可采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保护。

f) 客体安全重用

应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。

g) 恶意代码防范

应安装防恶意代码软件或配置具有相应安全功能的操作系统，并定期进行升级和更新，以防范和清除恶意代码。

h) 可信验证

可基于可信根对计算节点的 BIOS、引导程序、操作系统内核、**应用程序**等进行可信验证，并在检测到其可信性受到破坏后进行报警，**并将验证结果形成审计记录**。

7.3.1.2 云安全计算环境设计技术要求

本项要求包括：

a) **用户身份鉴别**

应支持注册到云计算服务的云租户建立主子账号，并采用用户名和用户标识符标识主子账号用户身份。

b) 用户账号保护

应支持建立云租户账号体系，实现主体对虚拟机、云数据库、云网络、云存储等客体的访问授权。

c) **安全审计**

应支持云服务商和云租户远程管理时执行特权命令进行审计。

应支持租户收集和查看与本租户资源相关的审计信息，保证云服务商对云租户系统和数据的访问操作可被租户审计。

d) 入侵防范

应能检测到虚拟机对宿主机物理资源的异常访问。

e) 数据备份与恢复

应采取冗余架构或分布式架构设计；应支持数据多副本存储方式；应支持通用接口确保云租户可以将业务系统及数据迁移到其他云计算平台和本地系统，保证可移植性。

f) 虚拟化安全

应实现虚拟机之间的CPU、内存和存储空间安全隔离；应禁止虚拟机对宿主机物理资源的直接访问；应支持不同云租户虚拟化网络之间安全隔离。

g) 恶意代码防范

物理机和宿主机应安装经过安全加固的操作系统或进行主机恶意代码防范；虚拟机应安装经过安全加固的操作系统或进行主机恶意代码防范；应支持对Web应用恶意代码检测和防护的能力。

h) 镜像和快照安全

应支持镜像和快照提供对虚拟机镜像和快照文件的完整性保护；防止虚拟机镜像、快照中可能存在的敏感资源被非授权访问；针对重要业务系统提供安全加固的操作系统镜像或支持对操作系统镜像进行自加固。

7.3.1.3 移动互联安全计算环境设计技术要求

本项要求包括：

a) 用户身份鉴别

应采用口令、解锁图案以及其他具有相应安全强度的机制进行用户身份鉴别。

b) 应用管控

应提供应用程序签名认证机制，拒绝未经过认证签名的应用软件安装和执行。

c) 安全域隔离

应能够为重要应用提供应用级隔离的运行环境，保证应用的输入、输出、存储信息不被非法获取。

d) 数据保密性保护

应采取加密、混淆等措施，对移动应用程序进行保密性保护，防止被反编译。

e) 可信验证

应能对移动终端的操作系统、应用等程序的可信性进行验证，阻止非可信程序的执行。

7.3.1.4 物联网系统安全计算环境设计技术要求

本项要求包括：

a) 感知层设备身份鉴别

应采用常规鉴别机制对感知设备身份进行鉴别，确保数据来源于正确的感知设备；应对感知设备和感知层网关进行统一入网标识管理和维护，并确保在整个生存周期设备标识的唯一性。

b) 感知层设备访问控制

应通过制定安全策略如访问控制列表，实现对感知设备的访问控制；感知设备和其他设备（感知层网关、其他感知设备）通信时，应根据安全策略对其他设备进行权限检查。

7.3.1.5 工业控制系统安全计算环境设计技术要求

本项要求包括：

a) 工业控制身份鉴别

现场控制层设备及过程监控层设备应实施唯一性的标志、鉴别与认证，保证鉴别认证与功能完整性状态随时能得到实时验证与确认。在控制设备及监控设备上运行的程序、相应的数据集合应有唯一性标识管理。

b) 现场设备访问控制

应对通过身份鉴别的用户实施基于角色的访问控制策略，现场设备收到操作命令后，应检验该用户绑定的角色是否拥有执行该操作的权限，拥有权限的该用户获得授权，用户未获授权应向上层发出报警信息。

c) 现场设备数据保密性保护

可采用密码技术支持的保密性保护机制或可采用物理保护机制，对现场设备层设备及连接到现场控制层的现场总线设备内存储的有保密需要的数据、程序、配置信息等进行保密性保护。

d) 控制过程完整性保护

应在规定的时间内完成规定的任务，数据应以授权方式进行外理，确保数据不被非法篡改、不丢失、不延误，确保及时响应和外理事件，保护系统的同步机制、校时机制，保持控制周期稳定、现场总线轮询周期稳定。

7.3.2 安全区域边界设计技术要求

7.3.2.1 通用安全区域边界设计技术要求

本项要求包括：

a) 区域边界包过滤

应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议和请求的服务等，确定是否允许该数据包通过该区域边界。

b) 区域边界安全审计

应在安全区域边界设置审计机制，并由安全管理中心统一管理。

c) 区域边界恶意代码防范

可在安全区域边界设置防恶意代码网关，由安全管理中心管理。

d) 区域边界完整性保护

应在区域边界设置探测器，探测非法外联等行为，并及时报告安全管理中心。

e) 可信验证

可基于可信根对区域边界计算节点的BIOS、引导程序、操作系统内核、区域边界安全管控程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录。

7.3.2.2 云安全区域边界设计技术要求

本项要求包括：

a) 区域边界结构安全

应保证虚拟机只能接收到目的地址包括自己地址的报文或业务需求的广播报文，同时限制广播攻击。

b) 区域边界访问控制

应保证当虚拟机迁移时，访问控制策略随其迁移；应允许云租户设置不同虚拟机之间的访问控

制策略；应建立租户私有网络实现不同租户之间的安全隔离。

7.3.2.3 移动互联安全区域边界设计技术要求

本项要求包括：

a) 区域边界访问控制

应能限制移动设备在不同工作场景下对 WiFi、3G、4G 等网络的访问能力。

b) 区域边界完整性保护

应具备无线接入设备检测功能，对于非法无线接入设备进行报警。

7.3.2.4 物联网系统安全区域边界设计技术要求

本项要求包括：

a) 区域边界准入控制

应在安全区域边界设置准入控制机制，能够对设备进行认证。

b) 区域边界协议过滤与控制

应在安全区域边界设置协议检查，对通信报文进行合规检查。

7.3.2.5 工业控制系统安全区域边界设计技术要求

应遵守 7.3.2.1。

7.3.3 安全通信网络设计技术要求

7.3.3.1 通用安全通信网络设计技术要求

本项要求包括：

a) 通信网络安全审计

应在安全通信网络设置审计机制，由安全管理中心管理。

b) 通信网络数据传输完整性保护

可采用由密码等技术支持的完整性校验机制，以实现通信网络传输完整性保护。

c) 通信网络数据传输保密性保护

可采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

d) 可信连接验证

通信节点应采用具有网络可信连接保护功能的系统软件或可信根支撑的信息技术产品，在设备连接网络时，对源和目标平台身份、执行程序进行可信验证，并将验证结果形成审计记录。

7.3.3.2 云安全通信网络设计技术要求

本项要求包括：

a) 通信网络数据传输保密性

可支持云租户远程通信数据保密性保护。

b) 通信网络安全审计

应支持租户收集和查看与本租户资源相关的审计信息；应保证云服务商对云租户通信网络的访问操作可被租户审计。

7.3.3.3 移动互联安全通信网络设计技术要求

应遵守 7.3.3.1。

7.3.3.4 物联网系统安全通信网络设计技术要求

本项要求包括：

a) **异构网安全接入保护**

应采用接入认证等技术建立异构网络的接入认证系统，保障控制信息的安全传输。

7.3.3.5 工业控制系统安全通信网络设计技术要求

本项要求包括：

a) 现场总线网络数据传输完整性保护

可采用适应现场总线特点的报文短、时延小的密码技术支持的完整性校验机制或可采用物理保护机制，实现现场总线网络数据传输完整性保护。

b) **无线网络数据传输完整性保护**

可采用密码技术支持的完整性校验机制，以实现无线网络数据传输完整性保护。

7.3.4 安全管理中心设计技术要求

7.3.4.1 系统管理

可通过系统管理员对系统的资源和运行进行配置、控制和可信管理，包括用户身份、可信证书、**可信基准库**、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复以及恶意代码防范等。

应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

在进行云计算平台安全设计时，安全管理应提供查询云租户数据及备份存储位置的方式。

在进行物联网系统安全设计时，应通过系统管理员对感知设备、感知层网关等进行统一身份标识管理。

7.3.4.2 审计管理

可通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。

应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。

在进行云计算平台安全设计时，云计算平台应对云服务器、云数据库、云存储等云服务的创建、删除等操作行为进行审计。

在进行工业控制系统安全设计时，应通过安全管理员对工业控制现场控制设备、网络安全设备、网络设备、服务器、操作站等设备中主体和客体进行登记，并对各设备的网络安全监控和报警、网络安全日志信息进行集中管理。根据安全审计策略对各类网络安全信息进行分类管理与查询，并生成统一的审计报告。

8 第三级系统安全保护环境设计

8.1 设计目标

第三级系统安全保护环境的设计目标是：按照 GB 17859—1999 对第三级系统的安全保护要求，在第二级系统安全保护环境的基础上，通过实现基于安全策略模型和标记的强制访问控制以及增强系统

的审计机制，使系统具有在统一安全策略管控下，保护敏感资源的能力，并保障基础计算资源和应用程序可信，确保关键执行环节可信。

8.2 设计策略

第三级系统安全保护环境的设计策略是：在第二级系统安全保护环境的基础上，遵循 GB 17859—1999 的 4.3 中相关要求，构造非形式化的安全策略模型，对主、客体进行安全标记，表明主、客体的级别分类和非级别分类的组合，以此为基础，按照强制访问控制规则实现对主体及其客体的访问控制。第三级系统安全保护环境在使用密码技术设计时，应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准。

第三级系统安全保护环境的设计通过第三级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。计算节点都应基于可信根实现开机到操作系统启动，再到应用程序启动的可信验证，并在应用程序的关键执行环节对其执行环境进行可信验证，主动抵御病毒入侵行为，并将验证结果形成审计记录，送至管理中心。

8.3 设计技术要求

8.3.1 安全计算环境设计技术要求

8.3.1.1 通用安全计算环境设计技术要求

本项要求包括：

a) 用户身份鉴别

应支持用户标识和用户鉴别。在对每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录系统时，采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。

b) 自主访问控制

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和(或)记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。

c) 标记和强制访问控制

在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。

d) 系统安全审计

应记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；确保对特定安全事件进行报警；确保审计记录不被破坏或非授权访问。应为安全管理中心提供接口；对不能由系统独立处理的安全事件，提供由授权主体调用的接口。

e) 用户数据完整性保护

应采用密码等技术支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。

f) 用户数据保密性保护

应采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行

保密性保护。

g) 客体安全重用

应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。

h) 可信验证

可基于可信根对计算节点的BIOS、引导程序、操作系统内核、应用程序等进行可信验证，并在应用程序的关键执行环节对系统调用的主体、客体、操作可信验证，并对中断、关键内存区域等执行资源进行可信验证，并在检测到其可信性受到破坏时采取措施恢复，并将验证结果形成审计记录，送至管理中心。

i) 配置可信检查

应将系统的安全配置信息形成基准库，实时监控或定期检查配置信息的修改行为，及时修复和基准库中内容不符的配置信息。

j) 入侵检测和恶意代码防范

应通过主动免疫可信计算检验机制及时识别入侵和病毒行为，并将其有效阻断。

8.3.1.2 云安全计算环境设计技术要求

本项要求包括：

a) 用户身份鉴别

应支持注册到云计算服务的云租户建立主子账号，并采用用户名和用户标识符标识主子账号用户身份。

b) 用户账号保护

应支持建立云租户账号体系，实现主体对虚拟机、云数据库、云网络、云存储等客体的访问权。

c) 安全审计

应支持对云服务商和云租户远程管理时执行的特权命令进行审计。

应支持租户收集和查看与本租户资源相关的审计信息，保证云服务商对云租户系统和数据的访问操作可被租户审计。

d) 入侵防范

应能检测到虚拟机对宿主机物理资源的异常访问。应支持对云租户进行行为监控，对云租户发起的恶意攻击或恶意对外连接进行检测和告警。

e) 数据保密性保护

应提供重要业务数据加密服务，加密密钥由租户自行管理；应提供加密服务，保证虚拟机在迁移过程中重要数据的保密性。

f) 数据备份与恢复

应采取冗余架构或分布式架构设计；应支持数据多副本存储方式；应支持通用接口确保云租户可以将业务系统及数据迁移到其他云计算平台和本地系统，保证可移植性。

g) 虚拟化安全

应实现虚拟机之间的CPU、内存和存储空间安全隔离，能检测到非授权管理虚拟机等情况，并进行告警；应禁止虚拟机对宿主机物理资源的直接访问，应能对异常访问进行告警；应支持不同云租户虚拟化网络之间安全隔离；应监控物理机、宿主机、虚拟机的运行状态。

h) 恶意代码防范

物理机和宿主机应安装经过安全加固的操作系统或进行主机恶意代码防范；虚拟机应安装经过安全加固的操作系统或进行主机恶意代码防范；应支持对Web应用恶意代码检测和防护的

能力。

i) 镜像和快照安全

应支持镜像和快照提供对虚拟机镜像和快照文件的完整性保护；防止虚拟机镜像、快照中可能存在的敏感资源被非授权访问；针对重要业务系统提供安全加固的操作系统镜像或支持对操作系统镜像进行自加固。

8.3.1.3 移动互联安全计算环境设计技术要求

本项要求包括：

a) 用户身份鉴别

应对移动终端用户实现基于口令或解锁图案、数字证书或动态口令、生物特征等方式的两种或两种以上的组合机制进行用户身份鉴别。

b) 标记和强制访问控制

应确保用户或进程对移动终端系统资源的最小使用权限；应根据安全策略，控制移动终端接入访问外设，外设类型至少应包括扩展存储卡、gps等定位设备、蓝牙、NFC等通信外设，并记录日志。

c) 应用管控

应具有软件白名单功能，能根据白名单控制应用软件安装、运行；应提供应用程序签名认证机制，拒绝未经过认证签名的应用软件安装和执行。

d) 安全域隔离

应能够为重要应用提供基于容器、虚拟化等系统级隔离的运行环境，保证应用的输入、输出、存储信息不被非法获取。

e) 移动设备管控

应基于移动设备管理软件，实行对移动设备全生命周期管控，保证移动设备丢失或被盗后，通过网络定位搜寻设备的位置、远程锁定设备、远程擦除设备上的数据、使设备发出警报音，确保在能够定位和检索的同时最大程度地保护数据。

f) 数据保密性保护

应采取加密、混淆等措施，对移动应用程序进行保密性保护，防止被反编译；应实现对扩展存储设备的加密功能，确保数据储存的安全。

g) 可信验证

应能对移动终端的引导程序、操作系统内核、应用程序等进行可信验证，确保每个部件在加载前的真实性和完整性。

8.3.1.4 物联网系统安全计算环境设计技术要求

本项要求包括：

a) 感知层设备身份鉴别

应采用密码技术支持的鉴别机制实现感知层网关与感知设备之间的双向身份鉴别，确保数据来源于正确的设备；应对感知设备和感知层网关进行统一入网标识管理和维护，并确保在整个生存周期设备标识的唯一性；应采取措施对感知设备组成的组进行组认证以减少网络拥塞。

b) 感知层设备访问控制

应通过制定安全策略如访问控制列表，实现对感知设备的访问控制；感知设备和其他设备（感知层网关、其他感知设备）通信时，根据安全策略对其他设备进行权限检查；感知设备进行更新配置时，根据安全策略对用户进行权限检查。