ICS 33.060.99
M 36

SparkLink

团　　体　　标　　准

T/XS 40001-2022

星闪无线通信系统
网络安全 通用要求

SparkLink Wireless Communication System - Cybersecurity –

General Requirements

版本：V1.0.0

2022-09-22 发布　　2022-09-22 实施

星　　闪　　联　　盟 发布

目　　次

前　言

《星闪无线通信系统》当前分别为如下部分：

- 星闪无线通信系统 架构；
- 星闪无线通信系统 基础服务层 设备发现与服务管理；
- 星闪无线通信系统 基础服务层 传输与控制；
- 星闪无线通信系统 基础服务层 服务质量管理；
- 星闪无线通信系统 基础服务层 多域协调与管理；
- 星闪无线通信系统 基础服务层 5G 蜂窝网络融合；
- 星闪无线通信系统 网络安全 通用要求；
- 星闪无线通信系统 媒体接入层标识分配；
- 无线短距通信 车载空口技术要求和测试方法
- 星闪无线通信系统 接入层 低功耗空口技术要求和测试方法
- 星闪无线通信系统 测试 星闪基础接入技术（SLB）设备要求和测试方法；
- 星闪无线通信系统 测试 星闪基础接入技术（SLB）设备安全要求和测试方法；

其中，《无线短距通信 车载空口技术要求和测试方法》（YD/T 4007-2022）由中国通信标准化协会制定，作为星闪基础接入技术。随着技术的发展，星闪无线通信系统还将制定后续的相关标准。

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由星闪联盟提出并归口。

本文件起草单位：中国标准化研究院、华为技术有限公司、郑州信大捷安信息技术股份有限公司、鼎桥通信技术有限公司、小米科技有限责任公司、中国汽车工程研究院股份有限公司、北京紫光展锐通信有限公司、湖南国科微电子股份有限公司、北京数字认证股份有限公司

本文件主要起草人：巫小波、王勇、刘为华、李文昭、蒋皓静、谢志利、王琰、陈璟、尹彦、王键、李明超、梁浩然、马骁菲、陈灿峰、董红磊、田晶晶、全代勇、刘冲、张向东、刘辉、刘献伦、牟洁、王新华、王本海、孙志勇、侯晶晶。

星闪无线通信系统 网络安全 通用要求

1 范围

本文件规定了星闪通用设备安全防护要求、星闪设备通信的通用安全保护要求。

本文件适用于星闪无线通信终端设备。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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/T 32915 信息安全技术 二元序列随机性检测方法
GB/T 35273 信息安全技术 个人信息安全规范
GB/T 38626 信息安全技术 智能联网设备口令保护指南
GB/T 38636 信息安全技术 传输层密码协议（TLCP）
YD/T 4007-2022 无线短距通信 车载空口技术要求和测试方法
T/XS 00001-2022 星闪无线通信系统 架构
T/XS 10002-2022 星闪无线通信系统 接入层 低功耗空口技术要求和测试方法
T/XS 20005-2022 星闪无线通信系统 基础服务层 5G蜂窝网络融合

3 术语和定义

GB/T 35273界定的以及下列术语和定义适用于本文件：

3.1

管理节点 Grant Node
星闪无线通信系统接入层发送数据调度信息的节点。

3.2

终端节点 Terminal Node
星闪无线通信系统接入层接收数据调度信息，根据数据调度信息发送数据的节点。

4 缩略语

下列缩略语适用于本文件。

PSK	Pre-Shared Key	预共享密钥
SLB	SparkLink Basic	星闪基础接入技术
SLE	Sparklink Low Energy	星闪低功耗接入技术
TLCP	Transport Layer Cryptography Protocol	传输层密码协议
TLS	Transport Layer Security	传输层安全性协议

5 概述

星闪无线通信系统架构参见 T/XS 00001-2022 的 6.2 节。星闪接入层根据实现功能的不同分为管理节点（G 节点）和终端节点（T 节点），其中 G 节点为其覆盖下的 T 节点提供连接管理、资源分配、网络安全等接入层服务。星闪无线通信系统安全架构如图 1 所示。

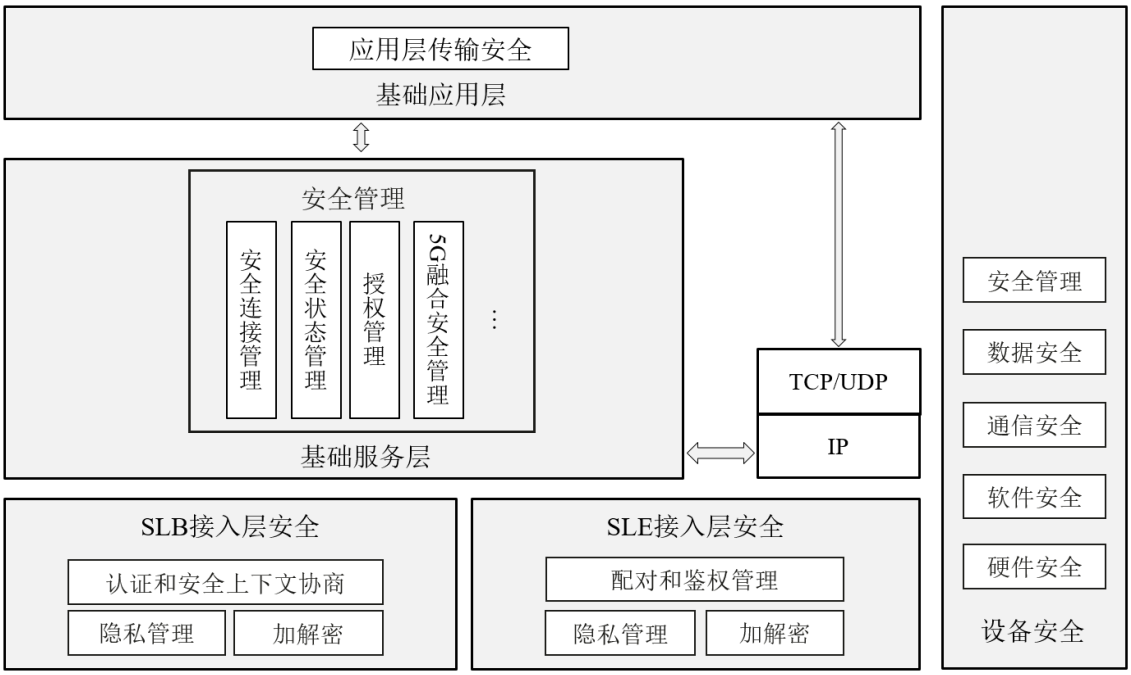

图1 星闪无线通信系统安全架构

星闪接入层为星闪上层提供 SLB 和 SLE 两种通信接口以及相应的接入层安全机制。SLB 接入层提供认证和安全上下文协商、隐私管理和加解密等接入层安全机制。SLE 接入层提供配对和鉴权管理、隐私管理和加解密等接入层安全机制。

基础服务层针对上层业务数据提供服务功能，其中基础服务层的安全管理功能单元提供基础服务层的网络安全服务功能，包括安全连接管理、安全状态管理、权限管理、5G融合安全管理等服务功能。

基础应用层用于实现各类应用功能，基础应用层针对共性的业务诉求，可以定义通用应用服务框架。基础应用层可以提供应用层传输安全机制以实现端到端的应用层传输安全。

为了提高星闪无线通信系统抵抗攻击的能力，星闪无线通信终端设备应满足设备安全要求，包括硬件安全、软件安全、通信安全、数据安全和安全管理等方面。

6 星闪接入层安全

星闪接入层安全包括SLB接入层安全和SLE接入层安全。

SLB接入层安全应符合YD/T 4007-2022章节9中的要求。

SLE接入层安全应符合T/XS 10002-2022章节9中的要求。

7 基础服务层安全

7.1 概述

星闪基础服务层的安全管理功能单元提供基础服务层的网络安全服务功能，包括安全连接管理、安全状态管理、授权管理和5G融合安全管理等服务功能。

7.2 安全连接管理

7.2.1 概述

安全连接过程在SLB中为认证和安全上下文协商流程，在SLE中为配对和鉴权流程。

安全连接服务为应用层提供如下服务：

a）建立安全连接；

b）取消安全连接；

c）安全连接状态查询；

d）安全连接状态通知。

7.2.2 建立安全连接

建立安全连接服务用于向应用提供和对端设备建立安全连接的功能，可根据对端设备地址和对端设备的能力建立安全连接。

调用建立安全连接功能之后，设备启动和对端设备的安全连接和鉴权流程。安全管理功能单元负责传递接入层和用户界面之间的交互信息，如口令值、数字比较值、输入口令通知、用户确认通知、用户确认等。

当安全连接失败或成功后，通过安全连接状态服务通知用户安全连接结果。

7.2.3 取消安全连接

当应用希望取消和对端设备的安全连接时，可调用取消安全连接服务。

调用取消安全连接服务后，获得的状态包括：

a）取消安全连接成功；

b）取消安全连接失败，地址不存在；

c）取消安全连接失败，正在安全连接中。

7.2.4 安全连接状态查询

该服务用于应用查询和指定设备的安全连接的状态，状态包括：安全连接中、安全连接失败和安全连接成功。

7.2.5 安全连接状态通知

该服务用于向应用通知安全连接建立之后安全连接的状态。安全连接状态的通知方式为注册-通知的方式。安全连接状态包括：

a）安全连接中；

b）安全连接失败；

c）安全连接成功。

当安全连接失败时，可通知安全连接失败的原因，如：安全连接冲突，链路断开，鉴权失败等。

7.3 安全状态管理

7.3.1 概述

安全状态管理为上层应用提供如下服务：

a）安全状态查询；

b）安全状态通知。

7.3.2 安全状态查询

该服务用于应用查询当前链路的安全状态信息，以供应用确定当前链路的安全性是否满足要求，包括如下内容：

a）安全状态：包括加密和未加密状态、完整性保护和未完整性保护状态；

b）安全算法：包括加密算法和完整性保护算法（如果安全开启的话）；

c）链路状态：包括连接和断开；

d）鉴权状态：包括未鉴权，鉴权中，已鉴权和鉴权方式。

7.3.3 安全状态通知

该服务用于当链路的安全状态发生改变时，比如链路加密关闭，通知应用来决策和处理。

安全状态和状态参数定义如下：

状态	状态参数
安全状态	1. 加密、未加密 2. 完整性保护、未完整性保护
安全算法	1. 加密算法 2. 完整性保护算法
链路状态	连接或断开
鉴权状态	1. 未鉴权，鉴权中，已鉴权 2. 鉴权方式

7.4 授权管理

基础服务层的授权由基础服务层的功能单元决定对端设备的服务访问是否被允许。

当对端设备访问基础服务层的功能单元服务时，可能需要基础服务层的功能单元对该服务访问进行授权。基础服务层安全管理将该授权请求发送给基础服务层的功能单元，基础服务层的功能单元可以自行判断或者请求用户确定以得到授权结果。基础服务层的功能单元得到授权结果之后，将该授权结果发送回基础服务层安全管理。基础服务层安全管理保存该授权结果。基础服务层安全管理为基础服务层的服务访问提供该授权结果。

基础应用层的授权由基础应用层决定对端设备的服务访问是否被允许。

当对端设备访问基础应用层的服务时，可能需要基础应用层对该服务访问进行授权。基础服务层安全管理将该授权请求发送给基础应用层，基础应用层可以自行判断或者请求用户确定以得到授权结果。基础应用层得到授权结果之后，将该授权结果发送回基础服务层安全管理。基础服务层安全管理保存该授权结果。基础服务层安全管理为基础应用层的服务访问提供该授权结果。

7.5 5G 融合安全管理

7.5.1 概述

根据T/XS 20005-2022，在T节点通过星闪可信接入网（TSAN）注册到5G核心网的5G融合场景中，T节点和G节点存在两类PSK：非可信5G-PSK；可信5G-PSK。因此同时具有5G融合业务和非5G融合业务（普通业务）的T节点和G节点将存在三类PSK：非可信5G-PSK；可信5G-PSK；普通PSK。

三类PSK使用原则如下：

a）针对5G融合业务，应使用5G-PSK（非可信5G-PSK或可信5G-PSK）；如果有可信5G-PSK，则使用可信5G-PSK；

b）针对非5G融合业务，应使用普通PSK。

G节点和T节点进行业务时需根据PSK类型确定该连接的业务范围：基于非可信5G-PSK或可信5G-PSK建立的连接（包括安全上下文）只能用于5G融合业务；基于普通PSK建立的连接（包括安全上下文）只能用于普通业务。

7.5.2 无安全上下文场景

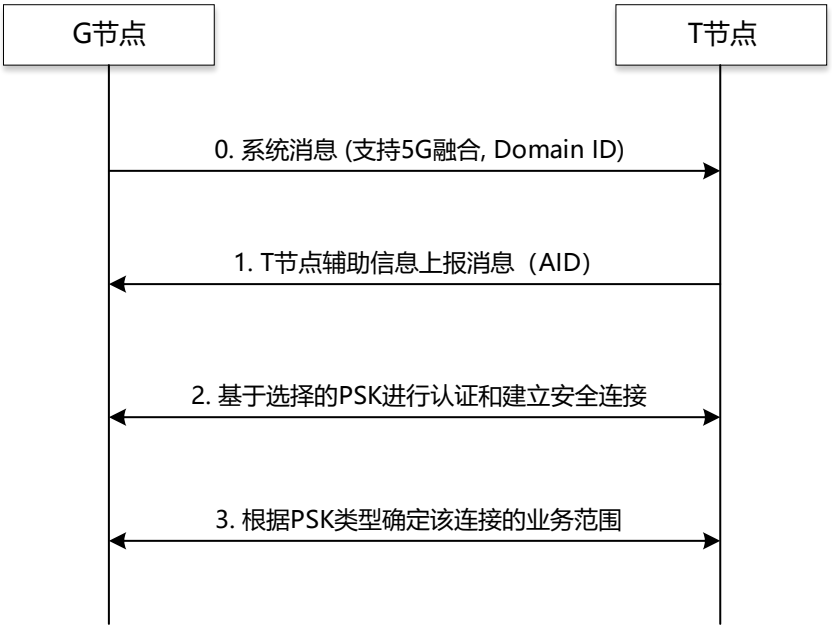

图 2 5G 融合认证和安全上下文协商（无安全上下文场景）

当T节点无安全上下文时，应进行认证和安全上下文协商流程。流程参见图2，流程描述如下：

a）（可选）G 节点给 T 节点发送系统消息，携带该 G 节点支持 5G 融合的指示信息和 G 节点的身份（Domain ID）。

b）T 节点向 G 节点发送 T 节点辅助信息上报消息，携带应用标识 AID。

c)G 节点根据 AID 对应的业务类型，确定 T 节点 ID 对应的 PSK。当 AID 指示 5G 融合业务时，选择 5G-PSK（非可信 5G-PSK 或可信 5G-PSK），当 AID 指示的不是 5G 融合业务时，选择普通 PSK。G 节点和 T 节点基于选择的该 PSK 根据《无线短距通信车载空口技术要求和测试方法》进行认证和建立安全连接。

d）安全连接建立之后，G节点和T节点进行业务时需根据PSK类型确定该连接的业务范围。具体的，基于可信5G-PSK建立的连接（包括安全上下文）只能用于5G融合业务；基于普通PSK建立的连接（包括安全上下文）只能用于普通业务。相应的，T节点在发送T节点辅助信息上报消息之前，T节点需确定这次连接的业务类型（5G融合业务、普通业务等），根据业务类型选择相应的PSK。如果是5G融合业务，有可信5G-PSK则使用可信5G-PSK（如果使用可信5G-PSK建立连接失败，则再使用非可信5G-PSK），没有可信5G-PSK则使用非可信5G-PSK。非可信5G-PSK可以是一个默认的值。如果不是5G融合业务，则使用普通PSK。

7.5.3 有安全上下文场景

当T节点有安全上下文时，无需进行认证和安全上下文协商，直接使用现有的安全上下文建立关联。当T节点多次无法使用保存的安全上下文和G节点建立关联时，T节点可尝试删除保存的安全上下文，使用无安全上下文的关联流程（参见章节7.5.2）。

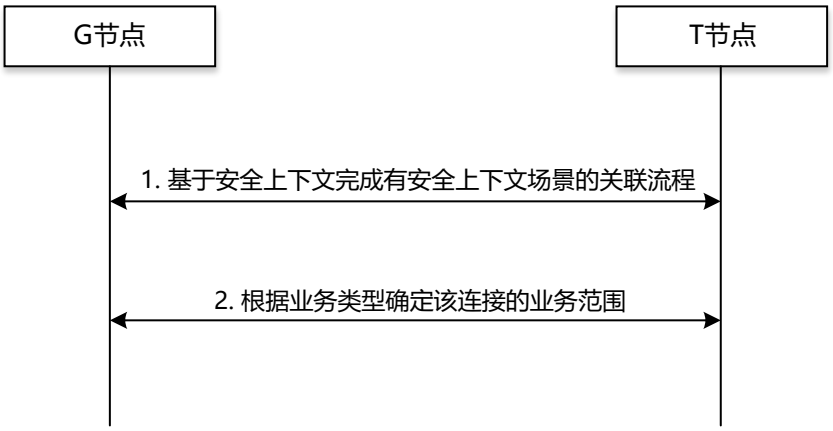

图 3 5G 融合认证和安全上下文协商（有安全上下文场景）

有安全上下文的5G融合安全流程如图3所示，流程描述如下：

a）如果 T 节点有多套安全上下文，T 节点安全管理功能单元根据这次连接的业务类型（5G 融合业务、普通业务等）选择相应的安全上下文，以及该安全上下文对应的 Kgt ID。G 节点根据 T 节点的临时 ID 和 Kgt ID 获取相应的安全上下文。G 节点和 T 节点基于安全上下文根据《无线短距通信车载空口技术要求和测试方法》完成有安全上下文场景的关联流程。

b）G 节点根据 T 节点的临时 ID 和 Kgt ID 确定相应的安全上下文和业务类型，即该 Kgt ID 对应的业务类型。安全连接建立之后，G 节点和 T 节点进行业务时需根据业务类型确定该连接的业务范围。具体的，基于 5G 融合业务建立的连接（包括安全上下文）只能用于 5G 融合业务；基于普通业务建立的连接（包括安全上下文）只能用于普通业务。

8 基础应用层安全

8.1 概述

根据星闪无线通信系统的应用场景，可能需要使用应用层传输安全机制。

8.2 应用层传输安全

a) 星闪无线通信系统设备可支持应用层传输安全机制。当需要支持应用层传输安全机制时，针对基于Non-IP的传输，星闪无线通信系统设备使用的应用层传输安全机制由具体应用实现，本文件不进行定义；对基于IP的传输，星闪无线通信系统设备宜支持TLS/TLCP协议。星闪无线通信系统设备支持的TLS应满足如下要求：
   1) 应支持TLS 1.2以上版本，应禁用TLS 1.1以下版本和SSL；
   2) 如使用TLS1.2，应遵守TLS 1.2 (RFC 5246)中规定的允许和强制加密套件（cipher suite）的规则；
   3) 如使用TLS1.3，应遵守TLS 1.3 (RFC 8446)中规定的允许和强制加密套件（cipher suite）的规则；
   4) 应支持禁用非认证加密模式的加密套件；
   5) 应支持禁用非完全前向保密特性的加密套件；
   6) 应支持禁用无完整性保护的加密套件；
   7) 支持禁用匿名加密套件；
   8) 应支持安全的加密套件，应支持禁用不安全的加密套件。

b） 应用应具备会话安全保护机制（例如：使用随机生成会话ID等机制）；
c） 应用对外传输个人敏感信息时，应符合GB/T 35273的要求，并应满足如下要求：
应用发送个人敏感信息之前，应实现通信端之间的双向认证。

9 设备安全要求

9.1 概述

图 4 星闪无线通信系统设备安全框架

设备安全主要由硬件安全、软件安全、通信安全、数据安全和安全管理部分构成，具体如图 4 所示。

9.2 硬件安全

9.2.1 芯片安全

应满足如下芯片安全要求：
a) 应具备芯片固件的物理写保护的功能，防止固件被篡改；
b) 芯片的硬件特征信息应与芯片固件绑定，如果芯片固件程序被篡改或更换，设备应能够停止加载芯片固件程序并反馈异常信息；
c) 宜具备安全芯片或硬件密码模块，物理保护设备密钥、证书等的安全；
d) 芯片宜具备固件读保护功能，防止固件被非法读取；
e) 宜支持安全启动，保障运行环境安全。

9.2.2 接口安全

应满足如下接口安全要求：
a） 调试接口应禁用或进行安全访问控制；
b） 如果具备摄像头、麦克风等隐私信息采集的传感器，默认处于关闭状态，并提供用户可控的开关、直观便捷的状态指示；
c） 对于具有Console接口的设备，需配置用户名、口令等方式进行认证授权，禁止直接登录；
d） 禁用闲置的物理端口。

9.2.3 防止物理攻击

应满足如下防止物理攻击要求：
a) 设备密码模块应具备抵抗物理攻击能力；
b) 对于需要获取时间的设备，应支持与授权时间同步。

9.2.4 密钥生成与保护

应满足如下密钥生成与保护要求：

a) 使用到的随机数符合随机数相关标准（例如：GB/T 32915等），保证由已验证、安全的随机数生成器产生；
b) 密钥应存储并运行于安全区域，无法被外部获取。

9.2.5 加密运算安全

在整个加密周期中应保持加密运算的机密性，满足如下要求：
a) 本地加密密钥应被安全存储；
b) 非本地加密密钥应在业务结束时应从本地销毁；
c) 加密运算过程中应防止密钥信息的泄露，确保密钥安全。

9.3 软件安全

9.3.1 系统安全

应满足如下系统安全要求：
a) 支持合法程序/固件版本更新机制，更新前需验证程序/固件包的合法性、完整性，高版本的才可以更新，发生更新失败时支持恢复到更新前的版本；
b) 默认关闭远程登录管理功能，即仅支持本地登录管理；
c) 关闭不必要的服务及端口，避免被攻击和利用的风险；
d) 软件开发遵循安全编码流程，上线前应经过严格的漏洞扫描和渗透测试并对暴露的问题进行修复处理；
e) 支持用户的身份验证、权限控制机制，保证正确的操作者身份和操作权限才可以进行操作，并对用户的操作进行日志审计；
f) 支持系统的备份和恢复机制，在本地系统损坏后可以进行恢复原来备份的系统和数据、配置等；
g) 宜支持本地部署监测Agent软件，监测本地软件执行过程并记录运行日志，如果出现异常则进行上报并采取措施及时处理；
h) 符合密码学要求，不应直接在代码中写入密钥。

9.3.2 应用安全

应满足如下应用安全要求：
a) 应在用户访问应用前，对其身份进行鉴别，并提供鉴别失败处理措施；
b) 应具备登录超时后的锁定或注销功能；
c) 当应用使用过程中涉及用户口令，应满足章节9.6中对口令的要求，还应满足如下要求：
   1) 不应默认保存用户上次的账号及口令信息；
   2) 应支持口令时效性检查机制，如提醒用户定期更换口令。
d) 不应以明文形式存储用户敏感信息；
e) 若具备数据删除功能，在删除数据前应明确提示用户，并由用户再次确认是否删除数据；
f) 不应存在已公开发布6个月以上的高危及以上等级漏洞；
g) 应用的运行不应长时间固定或无限制占用设备资源；
h) 不应存在非授权收集或泄露个人敏感信息、非授权数据外传等恶意行为；
i) 当应用软件支持升级时，应满足如下要求：
   1) 应用软件应从安全合规的来源下载；
   2) 下载的应用软件应包含签名信息，且签名信息真实可信；
   3) 应用软件的升级应在用户授权的情况下进行，当升级行为不能保证设备系统、其他应用软件、软件本身的安全时，应在说明中明示用户可能带来的安全风险；
   4) 当应用软件升级失败时，应保证应用软件能保持在可用状态。

9.4 通信安全

应满足如下通信安全要求：

a) 支持对通信双方主体身份进行鉴别认证后建立通信连接；
b) 对于鉴权信息、隐私数据和重要业务数据等敏感信息，通信过程中需要提供完整性保护和机密性保护等；
c) 应采用计数器、时间戳等机制防止重放攻击。

9.5 数据安全

9.5.1 用户数据的收集

若设备出于业务需要收集用户个人信息，应在收集前明示收集的目的和范围，并且只有在用户同意的情况下方可继续，且应提供关闭数据收集功能。

9.5.2 用户数据的存储

a） 支持数据按照类型选择不同的逻辑区域进行存储，可支持加密存储和逻辑隔离以及物理隔离（如安全芯片内），并设置不同的访问权限和身份验证；
b） 个人敏感信息应加密存储。

9.5.3 用户数据的授权访问

设备应提供本地存储的用户数据的授权访问能力，防止未授权访问。

9.5.4 用户数据的转移

a) 设备进行用户数据转移应按照约定目的和用途进行，传输数据之前应对双方进行身份认证和授权；
b) 若通过公共网络传输账户设置类、传感采集类、金融支付类用户个人信息时，应采用数字签名等技术手段保证数据的完整性和抗抵赖性，同时应采用密文方式传输；
c) 宜先对用户个人信息进行脱敏加工，消除能够识别特定个体的所有数据字段后再进行转移。

9.5.5 用户数据的删除

销毁用户的个人敏感信息要遵循物理层面删除的原则，保证数据不可恢复。

9.6 安全管理

应满足如下安全管理要求：

a） 运行安全管理服务统一进行安全管理，接收设备异常上报机制，并及时发现攻击和威胁；
b） 宜支持对设备进行安全策略管理，根据设备使用地点和安全要求进行动态配置，并支持按需更新；
c） 对设备程序/固件等进行统一的版本管理、软件包签名、升级服务，保证软件更新的安全；
d） 安全管理和其他安全产品如防火墙、入侵检测系统、恶意代码监测等进行联动，及时发现网络攻击和异常行为，并及时响应和处理；
e） 持续跟踪设备相关的硬件、软件漏洞公布信息和软件升级信息，并及时进行补救和缓解；
f） 定期对设备进行漏洞、病毒扫描和恶意代码检测等，检测设备内的程序、固件变动情况等，并对运行日志进行异常检查等，及时发现问题并处理；
g） 应支持安全事件的安全日志记录功能；
h） 安全日志应进行安全存储，防止未授权的修改、删除、覆盖等；

i） 应支持如下密码算法安全要求：

1） 使用已验证、安全的加密算法和参数；

2） 同一个密钥不复用于不同用途。

j） 星闪无线通信系统使用口令时，应符合GB/T 38626的要求，并应满足如下要求：

口令不能和帐号或者帐号的倒写一样；

若设置的口令不符合要求中的规则，应进行告警。

附 录 A
（资料性）
口令安全建议

口令安全除满足章节 9.6 中的口令要求外，建议考虑如下要求：

a） 系统应提供锁定用户的机制。可选择如下两种方式之一：

方式一：当重复输入错误口令次数（默认 5 次，次数系统可以设置）超过系统限制时，系统要锁定该用户；

方式二：系统还可以设置下次允许输入口令的间隔时间加倍，采用这种方式时，用户可以不设置自动锁定。

b） 系统可设置自动解锁时间（只适用于由于口令尝试被锁定的用户）

1） 对于口令尝试N次失败被锁定的用户，系统要能够设置自动解锁时间，建议默认解锁时间为5分钟；

2） 用户被锁时间达到预定义时间，可自动解锁该用户，或者也可通过安全管理员手工解锁该用户；

3） 在锁定时间内，仅能允许应用安全管理员角色所属账号手动解锁该用户。

c） 系统可提供和维护弱口令字典，不应使用弱口令字典中的口令；

d） 系统可设置前 n 次口令不可重复使用：系统要在技术上能够检测新设置的口令与前 N 个口令不重复（建议 N 值在 0～12 之间可配置，建议默认值为 5 次）

e） 可设置口令最长有效期限。对于采用静态口令认证技术的设备，应支持按天配置口令生存期功能：

1）口令使用N天（建议默认值90天）内可以对口令做变更，对于特权用户应M天（建议默认值30天）就变更一次口令；

2）口令到期前一段时间（建议默认值为7天）可以通知用户更改口令；

3）对于口令到期通知的提前时间，安全管理员应可配置。