ICS 35.020
A 90

中华人民共和国国家标准

GB/T 35592—2017

公安物联网感知终端接入安全技术要求

Security technology requirements for sensing terminals access to IoTPS

2017-12-29 发布　　2017-12-29 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由中华人民共和国公安部提出并归口。

本标准起草单位：公安部第三研究所、公安部第一研究所、公安部安全防范报警系统质量监督检验测试中心、无锡物联网产业研究院、工业和信息化部电子工业标准化研究院、华为技术有限公司、浙江宇视科技有限公司、博康智能网络科技股份有限公司、上海辰锐信息科技公司、国家计算机网络应急技术处理协调中心。

本标准主要起草人：齐力、杨明、朱兴国、唐前进、陶源、李海涛、陆洪波、张艳、李旋、陈书义、龚洁中、陈家明、沈国华、廖双龙、郑武、王晖。

公安物联网感知终端接入安全技术要求

1 范围

本标准规定了感知终端接入公安物联网的安全接入方式及相关安全技术要求。

本标准适用于公安物联网的建设和管理。

2 规范性引用文件

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

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18794.2—2002 信息技术 开放系统互连 开放系统安全框架 第2部分:鉴别框架

GB/T 20275 信息安全技术 网络入侵检测系统技术要求和测试评价方法

GB/T 20281 信息安全技术 防火墙安全技术要求和测试评价方法

GB/T 25069—2010 信息安全技术 术语

GA/T 1266—2015 公安物联网术语

3 术语和定义

GB 17859—1999、GB/T 18794.2—2002、GB/T 25069—2010 和 GA/T 1266—2015 界定的以及下列术语和定义适用于本文件。

3.1

安全接入系统 security access system of core network

用于保障感知终端与公安物联网进行数据通信的安全性，并起到连接和应用映射作用的安全控制设施。

3.2

物联网网关 sensing layer gateway

部署在公安物联网感知层与网络层边界，实现物联网感知终端与网络层通信网络通信的一种网络连接、控制和管理设备。

4 缩略语

下列缩略语适用于本文件。

ID:身份标识号码(Identity)

IoTPS:公安物联网(Internet of Things of Public Security)

IP:互联网协议(Internet Protocol)

RFID:射频识别(Radio Frequency Identification)

5 感知终端接入概述

5.1 总体结构

感知终端接入公安物联网的总体结构见图 1,主要包括以下几个部分:

a) 感知终端位于公安物联网感知层中,为应用系统采集相关的数据信息;

b) 传输通道位于公安物联网网络层中,连接感知终端与安全接入系统的通信通道,包括有线和无线两种;

c) 安全接入系统位于公安物联网网络层中,为感知终端接入核心业务区提供终端接入、系统应用及管理、安全防护、隔离交换等服务,接入示例结构参见附录 A;

d) 核心业务系统位于公安物联网应用层中,为信息采集、交换和数据处理提供信息化应用服务。

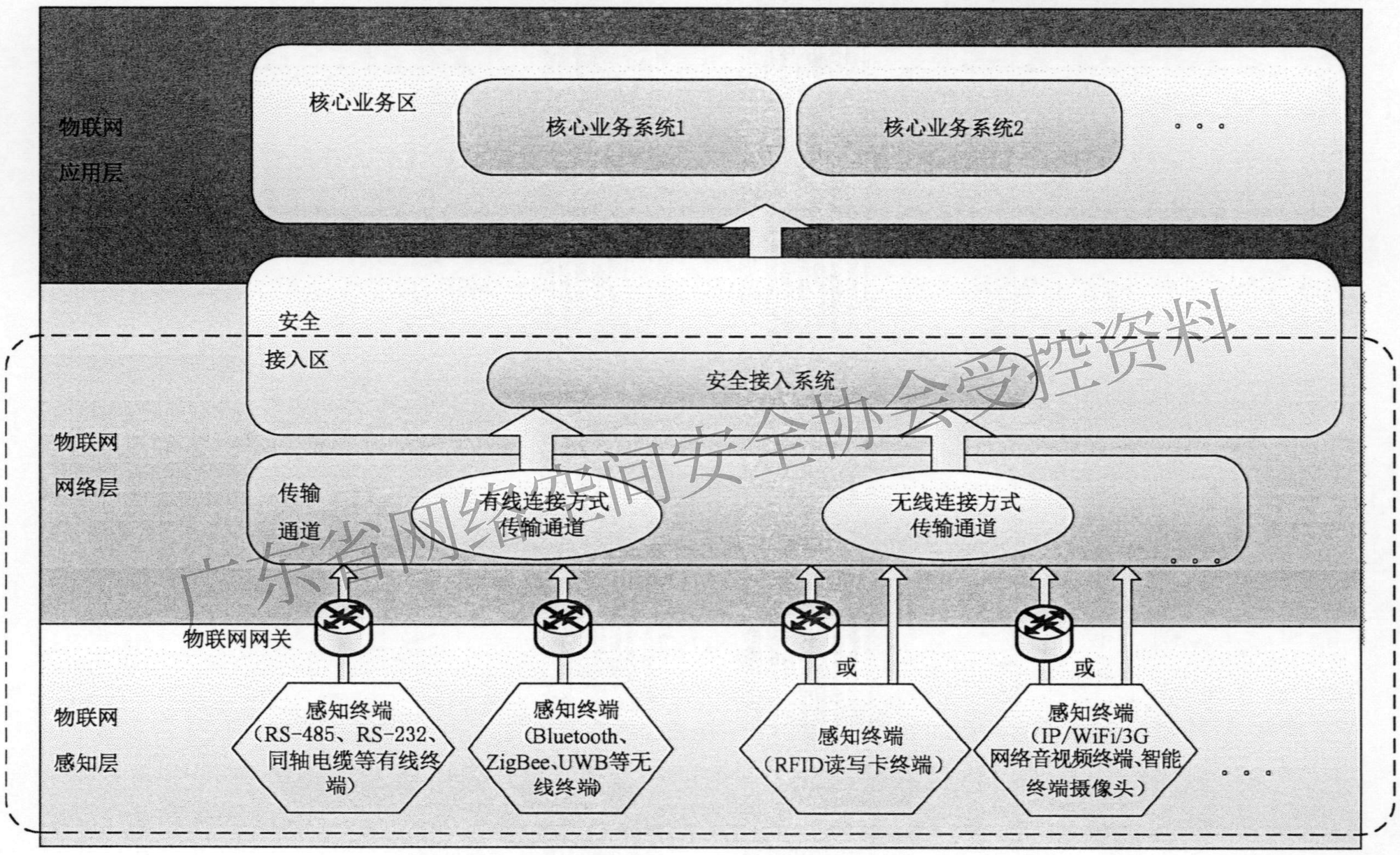

图 1 感知终端接入总体结构图

5.2 感知终端接入方式

感知终端与安全接入系统的连接方式见图 2,包括:

a) 直接接入方式:感知终端直接通过传输通道与安全接入系统连接。接入示例结构参见附录 A。

b) 间接接入方式:感知终端先连接到物联网网关,再通过传输通道与安全接入系统连接。接入示例结构参见附录 A。

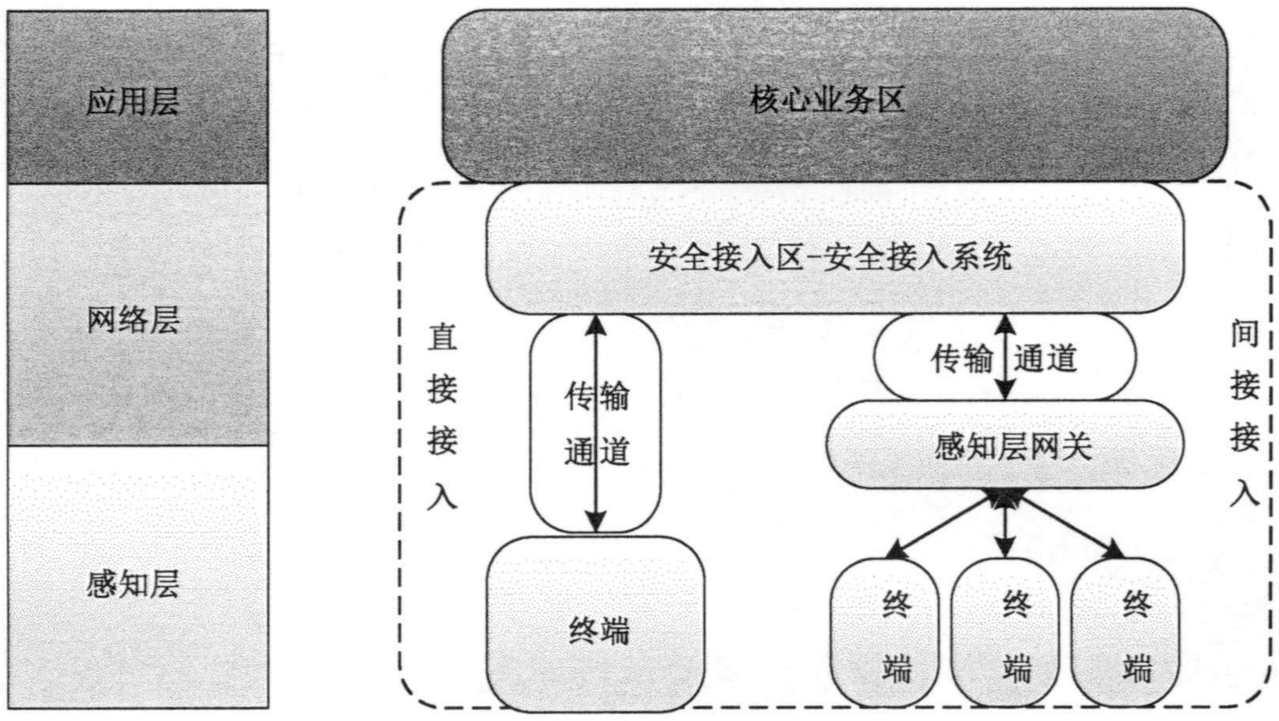

图 2　感知终端接入方式

6　感知终端接入及通道要求

6.1　感知终端直接接入要求

6.1.1　传输通道要求

6.1.1.1　有线连接方式

宜采用专用网络或建立加密通道方式保护数据通信。

6.1.1.2　无线连接方式

宜采用专用无线网络或通道。采用公众移动通信网时，应配置网络设备并建立虚拟专用拨号网(VPDN)或接入点(APN)。

6.1.2　安全功能要求

6.1.2.1　实体唯一标识及识别

感知终端应具备安全接入系统可识别的唯一标识信息。

6.1.2.2　支持实体认证

感知终端与安全接入系统应支持双向实体认证。

6.1.2.3　支持访问控制

感知终端应支持授权用户对包括外设、接口、应用软件和用户数据等终端资源的访问，并应阻断非授权的访问。

6.1.2.4　支持数据传输安全机制

感知终端宜具备安全功能硬件，并满足以下数据传输安全要求：

a)　数据保密性；

b)　数据完整性；

c)　数据时效性；

d） 数据不可抵赖性。

6.1.2.5 支持接入安全管理

感知终端与安全接入系统应支持终端接入安全策略管理和日志审计等功能。

6.2 感知终端间接接入要求

6.2.1 感知层传输通道要求

6.2.1.1 有线连接方式

感知终端采用专用线路、通道等与物联网网关进行连接。

6.2.1.2 无线连接方式

感知终端采用无线通信网络与物联网网关进行连接时，无线通信网络具备链路加密功能，并支持感知终端与物联网网关的加密通信。

6.2.2 连接安全要求

感知终端以间接接入方式连接安全接入系统，应满足以下条件：

a） 物联网网关与安全接入系统均不应旁路；

b） 物联网网关能对感知终端的接入进行管理。

6.2.3 安全功能要求

6.2.3.1 感知终端连接物联网网关的安全功能要求

6.2.3.1.1 实体标识及识别

感知终端与物联网网关的实体标识和识别应满足以下安全要求：

a） 感知终端、物联网网关均具备应用系统中唯一的标识信息；

b） 物联网网关具备识别感知终端标识的功能。

6.2.3.1.2 感知终端与物联网网关的连接认证

感知终端与物联网网关的连接认证应满足以下要求：

a） 支持感知终端接入物联网网关的单向实体接入认证；

b） 物联网网关能终止认证超时的感知终端的会话；

c） 物联网网关能终止规定次数认证失败的感知终端建立会话的尝试。

6.2.3.1.3 感知终端与物联网网关的数据安全传输

感知终端与物联网网关的数据传输宜满足以下安全要求：

a） 采用专用线路或国家规定的算法进行数据加密；

b） 采用国家规定的数据完整性安全机制；

c） 采用加入时间戳或包含时间序列的数据加密方式；

d） 采用国家规定的数字签名和验证算法。

6.2.3.1.4 物联网网关入侵检测

物联网网关宜具备入侵检测功能。

6.2.3.2 物联网网关连接安全接入系统的功能要求

6.2.3.2.1 实体标识要求

物联网网关应具备安全接入系统可识别的系统唯一标识。

6.2.3.2.2 支持实体认证

物联网网关应具备安全功能硬件，并满足与安全接入系统之间的双向实体认证要求。

6.2.3.2.3 支持访问控制

物联网网关应支持授权用户对感知层网络资源的访问，并应阻断非授权的访问。

6.2.3.2.4 支持数据传输安全机制

物联网网关与安全接入系统之间的传输安全机制应满足以下要求：

a) 数据保密性；
b) 数据完整性；
c) 数据时效性；
d) 数据不可抵赖性。

6.2.3.2.5 支持接入安全管理

物联网网关与安全接入系统应支持终端接入安全策略管理和日志审计等功能。

6.2.3.2.6 物联网网关的安全管理

物联网网关应具备权限管理和安全功能配置管理，满足以下安全要求：

a) 提供查阅和配置鉴别/认证、访问控制和数据传输等功能；
b) 当具备入侵检测、数据过滤等功能时，提供相应的查阅和配置的功能；
c) 提供查阅和管理日志/审计信息的功能。

6.2.3.2.7 物联网网关日志/审计功能

物联网网关应能生成安全事件日志信息，包括：

a) 记录授权鉴别/认证成功和失败；
b) 记录接入终端鉴别/认证成功和失败；
c) 记录系统入侵警告、病毒隔离防护事件。

7 安全接入系统要求

7.1 安全设备要求

安全接入系统应至少包括以下安全设备：

a) 符合 GB/T 20281 的防火墙；
b) 符合 GB/T 20275 的入侵检测设备；
c) 安全接入网关。

7.2 实体接入认证

7.2.1 接入认证

有线接入宜采用基于数字证书的双向认证，无线接入应采用基于数字证书的双向认证。

7.2.2 认证失败处理

安全接入系统对接入的终端或物联网网关进行认证时，应支持以下失败处理：

a） 能终止认证超时的当前会话；

b） 能终止规定次数认证失败的接入会话的尝试。

7.3 访问控制

7.3.1 访问控制策略

安全接入系统应支持感知终端或物联网网关访问控制安全策略的配置和执行，并满足以下安全要求：

a） 对不同用户/用户组制定不同的感知终端或物联网网关感知数据资源的访问控制策略；

b） 执行用户访问感知终端或物联网网关获取感知数据的策略。

7.3.2 自主访问控制

自主访问控制应满足以下安全要求：

a） 通过访问控制列表(ACL)来进行用户对感知终端或物联网网关的访问控制；

b） 阻断用户对非授权的感知终端或物联网网关的访问行为，并产生报警信息。

7.3.3 强制访问控制

强制访问控制应满足以下安全要求：

a） 支持对主体和被授权的感知终端和物联网网关资源设置敏感标记；

b） 支持基于敏感标记和访问控制策略的强制访问控制。

7.4 数据传输安全要求

数据传输应采用国家规定的加密算法，以端到端信道加密方式保障数据传输安全。

7.5 终端或物联网网关的证书管理机制

采用基于数字证书双向认证的安全接入系统时，应支持证书管理，满足以下安全要求：

a） 用于认证的数字证书的签发、恢复、废除、重发等；

b） 用于认证和通信的密钥的产生、分发、更新和注销等。

7.6 防火墙策略

防火墙应向安全接入网关开放指定的 IP 地址和端口映射，最小化控制开放端口的数量。

7.7 入侵检测和防病毒机制

安全接入系统应满足以下防护机制安全要求：

a） 支持应用数据格式、控制协议等的检查和对内容的过滤，只允许合法协议和数据通过；

b） 具备对感知终端或物联网网关发起的攻击或异常行为的检测能力；

c) 具备对已知病毒、木马等恶意代码的检测和阻断能力。

7.8 可靠性要求

安全接入系统宜支持安全接入网关的双机热备和负载均衡。

附 录 A
（资料性附录）
公安物联网终端安全接入应用结构示例

物联网感知网络和终端设备接入物联网核心业务网络应用时，应部署安全接入系统，并具备与之匹配的感知终端支持安全技术。其安全接入系统结构示例如图 A.1 中虚线框所示。

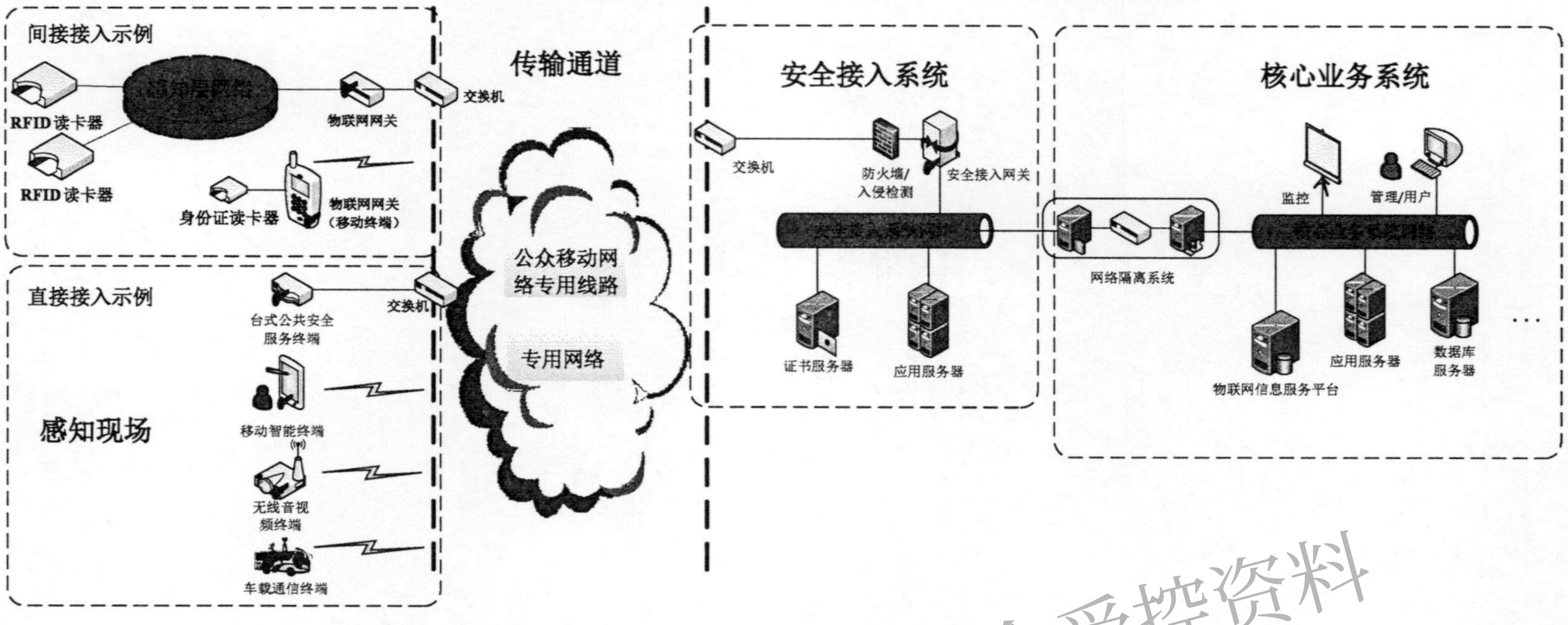

图 A.1 公安物联网终端安全接入应用结构示例图

公安物联网终端安全接入示例包括：感知现场、传输通道、安全接入系统、核心业务系统等。

感知现场包括：间接接入应用示例（RFID 应用、可穿戴装备应用等），如图 A.1 左上方框内所示。其中 RFID 读卡器、身份证读卡器等非 IP 类终端根据接入安全技术要求，需要连接经过安全接入系统认证和建立可信连接的物联网网关，才能形成物联网安全接入。直接接接入应用示例（台式服务终端、移动智能终端、无线音视频终端、车载通信终端），如图 A.1 左下方框内所示。其中，台式公共服务终端、移动智能终端、无线音视频终端、车载通信终端等 IP 类带操作系统终端根据接入安全技术要求，与安全接入系统进行认证和建立可信连接，即可形成物联网安全接入。

安全接入系统包括：防火墙设备、入侵检测设备、安全接入网关、证书服务设备等。形成对物联网终端接入的认证和可信接入，建立感知终端与核心业务区的数据通路，形成物联网应用。

参 考 文 献

[1] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[2] GB/T 20270—2006 信息安全技术 网络基础安全技术要求
[3] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[4] GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求
[5] GB/T 21052—2007 信息安全技术 信息系统物理安全技术要求
[6] GB/T 28181—2016 公共安全视频监控联网系统信息传输、交换、控制技术要求
[7] GA/T 390—2002 计算机信息系统安全等级保护通用技术要求
[8] GM/T 0002—2012 SM4 分组密码算法
[9] GM/T 0003—2012 SM2 椭圆曲线公钥密码算法
[10] GM/T 0004—2012 SM3 密码杂凑算法

中 华 人 民 共 和 国
国 家 标 准
公安物联网感知终端接入安全技术要求
GB/T 35592—2017
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
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 1 字数 20 千字
2017 年 12 月第一版 2017 年 12 月第一次印刷
*
书号:155066·1-58839 定价 18.00 元

GB/T 35592-2017