ICS 13.310
A 91

GA

中华人民共和国公共安全行业标准

GA/T XXXX.2—XXXX

公安视频图像信息系统安全技术要求 第2部分：前端设备

Security technology requirements for video and image information system for public security - Part 2: Front- end device

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国公安部　发布

目　次

前　言

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。

GA/T XXXX《公安视频图像信息系统安全技术要求》分为4个部分：

——第 1 部分：通用要求；

——第 2 部分：前端设备；

——第 3 部分：安全交互；

——第 4 部分：安全管理平台。

本文件是 GA/T XXXX的第2部分。

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。

本文件由公安部科技信息化局提出。

本文件由全国安全防范报警系统标准化技术委员会（SAC/TC 100）归口。

本文件起草单位：公安部第一研究所、视频图像信息智能分析与共享应用技术国家工程实验室、浙江宇视科技有限公司、浙江大华技术股份有限公司、杭州海康威视数字技术股份有限公司、苏州科达科技股份有限公司、公安部安全与警用电子产品质量检测中心、格尔软件股份有限公司、北京市公安局、华为技术有限公司、北京天防安全科技有限公司、深信服科技股份有限公司、杭州迪普科技股份有限公司、锚丁科技（北京）有限责任公司、杭州安恒信息技术股份有限公司。

本文件主要起草人：栗红梅、常玉兰、王连朝、吕胜伟、郑裕林、刘明、杨学军、何迪、张春慧、尚旭亮、王建勇、张薇薇、严敏瑞、段伟恒、邱慎奋、仇俊杰、鲁大军。

本文件于202x年首次发布。

公安视频图像信息系统安全技术要求

第2部分：前端设备

1 范围

本文件规定了公安视频图像信息系统中前端设备的分类与分级说明，以及前端设备安全技术要求。

本文件适用于公安视频图像信息系统前端设备的设计、制造和检验。

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 20271 信息安全技术 信息系统通用安全技术要求

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

GB 35114—2017 公共安全视频监控联网信息安全技术要求

GM/T 0021 动态口令密码应用技术规范

GA/T 1400—2017 （所有部分）公安视频图像信息应用系统

GA/T XXXX.1—XXXX 公安视频图像信息系统安全技术要求 第1部分：通用要求

3 术语、定义和缩略语

3.1 术语和定义

GB/T 28181—2016、GB/T 20271、GB 35114—2017、GA/T XXXX.1—XXXX界定的术语和定义适用于本文件。

3.2 缩略语

下列缩略语适用于本文件。

HTTP：超文本传输协议（Hyper Text Transfer Protocol）

IP：网际互联协议（Internet Protocol）

MAC：介质访问控制（Media Access Control）

OTA：空中下载技术（Over the Air）

SIM：用户识别模块（Subscriber Identify Module）

SSH：安全外壳（Secure Shell）

SSID：服务集标识（Service Set Identifier）

TLS：安全传输层（Transport Layer Security）

WEP：有线等效保密（Wired Equivalent Privacy）

WIFI：无线保真（Wireless Fidelity）

WLAN:无线局域网（Wireless Local Area Network）

WPA：WiFi安全访问（Wi-Fi Protected Access）

WPS：WiFi保护装置（Wi-Fi Protect Setup）

WSSE：Web服务安全（Web Service Security）

4 前端设备分类与分级

4.1 前端设备按照传输方式分为有线前端设备和无线前端设备两类。前端设备基于无线通信技术完成接入、传输及使用的，即为无线前端设备。

4.2 有线前端设备按照应用场景分为采集类设备、接入类设备两类；无线前端设备按照应用场景分为采集类设备、接入类设备和交互类设备三类。

4.3 前端设备根据安全能力分为通用型、增强型 I、增强型 II 三级。其中增强型无线前端设备可通过纵向安全防护系统接入公安视频图像信息系统。

5 安全技术要求

5.1 总体要求

公安视频图像信息系统各类前端设备的安全要求应符合表1的规定。

表 1 前端设备安全要求与前端设备类别对应关系表

功能	条款	有线前端设备						无线前端设备						
		采集类			接入类			采集类			接入类		交互类	
		通用型	增强型 I	增强型 II	通用型	增强型 I	增强型 II	通用型	增强型 I	增强型 II	增强型 I	增强型 II	增强型 I	增强型 II
物理安全	5.2.1	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.2.2	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.2.3	—	●	●	—	●	●	—	●	●	●	●	●	●
身份鉴别	5.3.1.1	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.3.1.2	—	●	●	—	●	●	—	●	●	●	●	●	●
	5.3.1.3	●	●	●	●	●	●	●	—	—	—	—	—	—
	5.3.1.4	—	●	●	—	●	●	—	●	●	●	●	●	●
	5.3.2.1	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.3.2.2	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.3.3.1	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.3.3.2	●	●	●	●	●	●	●	●	●	●	●	●	●
访问控制	5.4.1	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.4.2	●	●	●	—	—	—	●	●	●	—	—	—	—
	5.4.3	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.4.4	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.4.5	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.4.6	—	—	●	—	—	●	—	—	●	●	●	●	●
	5.4.7	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.4.8	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.4.9	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.4.10	●	●	●	●	●	●	●	●	●	●	●	●	●

表 1 前端设备安全要求与前端设备类别对应关系表（续）

功能	条款	有线前端设备						无线前端设备						
		采集类			接入类			采集类			接入类		交互类	
		通用型	增强型 I	增强型 II	通用型	增强型 I	增强型 II	通用型	增强型 I	增强型 II	增强型 I	增强型 II	增强型 I	增强型 II
入侵防范	5.5.1	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.5.2	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.5.3	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.5.4	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.5.5	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.5.6	—	●	●	—	●	●	—	●	●	●	●	●	●
	5.5.7	—	—	—	—	—	—	●	●	●	●	●	—	—
	5.5.8	—	—	—	—	—	—	●	●	●	●	●	—	—
	5.5.9	—	—	—	—	—	—	●	●	●	●	●	—	—
	5.5.10	—	—	—	—	—	—	●	●	●	●	●	—	—
数据安全	5.6.1	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.6.2	—	—	—	—	—	—	—	—	—	—	—	●	●
	5.6.3	—	—	●	—	—	●	—	—	●	—	●	—	●
	5.6.4	—	—	—	—	—	—	—	—	●	—	●	—	●
	5.6.5	—	—	●	—	—	●	—	—	●	●	●	●	●
证书和密钥管理	5.7.1	—	●	●	—	●	●	—	●	●	●	●	●	●
	5.7.2	—	●	●	—	●	●	—	●	●	●	●	●	●
日志安全	5.8.1	●	●	●	●	●	●	●	●	●	●	●	●	●
	5.8.2	○	○	○	○	○	○	○	○	○	○	○	○	○
	5.8.3	●	●	●	●	●	●	●	●	●	●	●	●	●
无线交互类前端设备管控	5.9.1	—	—	—	—	—	—	—	—	—	—	—	●	●
	5.9.2	—	—	—	—	—	—	—	—	—	—	—	●	●
	5.9.3	—	—	—	—	—	—	—	—	—	—	—	●	●
	5.9.4	—	—	—	—	—	—	—	—	—	—	—	●	●
	5.9.5	—	—	—	—	—	—	—	—	—	—	—	●	●
	5.9.6	—	—	—	—	—	—	—	—	—	—	—	●	●
	5.9.7	—	—	—	—	—	—	—	—	—	—	—	●	●
	5.9.8	—	—	—	—	—	—	—	—	—	—	—	●	●
无线前端设备承载业务	5.10.1	—	—	—	—	—	—	●	●	●	—	—	—	—
	5.10.2	—	—	—	—	—	—	●	●	●	●	●	●	●
注：●表示应满足相应条款；○表示宜满足相应条款；—表示不需要满足相应条款。														

5.2 物理安全

5.2.1 前端设备应根据使用环境和安全需要，采取相应防物理破坏、防电磁干扰、防阻挡屏蔽、防雷、防水、防尘、稳定电力供应等措施。

5.2.2 前端设备的重要部件应有明显的不易除去的标记。

5.2.3 前端设备的密码模块遭到破坏时应报警。

5.3 身份鉴别

5.3.1 身份标识与鉴别

5.3.1.1 前端设备应具有唯一电子身份标识。采用 GB/T 28181 协议或 GA/T 1400 协议传输的前端设备，其电子身份标识的编码规则应符合 GB/T 28181—2016 的相关规定。

5.3.1.2 具有密码模块的前端设备，其密码模块应具有不可更改的唯一电子身份标识，编码规则应符合 GB 35114-2017 中附录 B 的规定。

5.3.1.3 前端设备接入时，以及采集类设备连接接入类设备时，采用基于口令的数字摘要认证方式进行认证，其口令应具有复杂度控制、定期更换、加密传输和存储的能力，应和账号不同；采用动态口令方式认证时，动态口令的认证流程应符合 GM/T 0021 的规定；采用 GB/T 28181 协议传输的前端设备，认证流程应符合 GB/T 28181-2016 中 9.1 的规定；采用 GA/T 1400 协议传输的前端设备，应符合 GA/T 1400.4-2017 中 7.2.1 及 7.3.1 的规定；采用 HTTP 协议访问的前端设备，应支持安全模式进行身份认证，如 Digest 认证，WSSE 认证。

5.3.1.4 前端设备接入时，以及采集类设备连接接入类设备时，采用基于数字证书的设备身份认证，其前端设备认证流程应符合 GB 35114-2017 附录 C 中 C.2 的规定。

5.3.2 鉴别失败处理

5.3.2.1 前端设备在连续鉴别失败 5 次后，应锁定该账号不低于 5min，可支持对连续鉴别失败次数和锁定时间设置。

5.3.2.2 前端设备的账号锁定后可通过至少 1 种及以上方式进行解锁,如由更高权限用户进行解锁等。

5.3.3 超时处理

5.3.3.1 通信会话应支持设置最大超时时间；超时时间可修改的，应仅由已授权的用户进行设定。

5.3.3.2 通信会话在最大超时时间内若没有进行任何操作应终止会话，再次操作时应进行身份鉴别。

5.4 访问控制

5.4.1 首次登录时应重命名或删除默认账户，对于无法删除的默认账户应修改其默认口令。

5.4.2 采集类设备应支持采用专用工具集中统一设置管理账户口令。

5.4.3 应支持删除或停用多余的、过期的账户，禁止共享账户。

5.4.4 应支持授予管理类用户所需的最小权限，实现管理类用户的权限分离。

5.4.5 访问控制的粒度应至少包括 IP/MAC 等属性。

5.4.6 应支持设置最大会话数量。

5.4.7 应禁止非授权用户访问操作系统的系统文件。

5.4.8 应禁止非授权用户对前端设备上的软件进行配置或变更。

5.4.9 用户通过公安视频图像信息系统访问前端设备时，前端设备只接收基于 GB/T 28181—2016、GA/T 1400—2017 或 GB 35114—2017 的协议访问。

5.4.10 用户直接访问前端设备时，前端设备只接收特定 IP 地址的访问或基于外设的访问。

5.5 入侵防范

5.5.1 应支持遵循最小安装要求，可仅安装必要的组件和应用程序。

5.5.2 应支持关闭不需要的系统服务、默认共享和高危端口。

5.5.3 应支持以版本升级等方式修补漏洞。

5.5.4 应支持采用 SSH、TLS 等安全协议进行业务访问和远程管理。

5.5.5 应支持通过数字签名校验的升级包进行升级。

5.5.6 应有信令校验失败等事件的检测能力并记录日志或告警提示。

5.5.7 应支持对系统文件进行监控，对新增或修改文件进行病毒检测，可对恶意的病毒文件进行查杀。

5.5.8 无线前端设备应支持接入认证功能，禁止使用 WEP 方式进行认证。

5.5.9 无线前端设备应默认关闭 WPA 功能。

5.5.10 无线前端设备应能检测 SSID 广播、WPS 等高风险功能的开启状态，默认关闭 SSID 广播。

5.6 数据安全

5.6.1 前端设备应保证用户数据不能被未授权用户查询、修改和删除。

5.6.2 支持本地删除的前端设备应支持安全删除存储器中被用户需要删除的数据索引及数据内容。

5.6.3 重点区域、重点行业或重要部位前端设备的视频流的传输、存储、调看等应符合 GB 35114—2017 的 C 级规定。

5.6.4 无线前端设备采集数据的完整性和保密性应符合 GB 35114—2017 的规定。

5.6.5 前端设备采集的除视频流外的重要数据应确保其传输、存储的保密性和完整性。

5.7 证书和密钥管理

5.7.1 前端设备的数字证书格式应符合 GB 35114—2017 中附录 A 的规定。

5.7.2 前端设备的非对称密钥和对称密钥管理应符合 GB 35114—2017 的 6.14 的规定。

5.8 日志安全

5.8.1 具有本地存储功能的前端设备，应支持启用日志功能，日志应覆盖到每个用户，并对重要的用户行为和重要安全事件进行日志记录。

5.8.2 具有本地存储功能的前端设备，用户行为日志和安全事件日志宜保存 180 天或支持以 syslog 等方式上传。

5.8.3 具有本地存储功能的前端设备，日志记录应包括事件的日期和时间，登录、重启、注销、异常报警、账户锁定等事件类型以及源 IP 地址、目标 IP 地址、用户等信息。

5.9 无线交互类前端设备管控

5.9.1 应通过预置或管控接口对本机硬件能力和外围接口进行配置，管控对象如USB、扩展存储、蓝牙、定位服务、网络连接、摄像头，麦克等。配置操作可包括禁用、强制开启、受限访问、不管控等。

5.9.2 应通过预置移动通信网络连接参数或管控接口配置,限制前端设备仅能使用运营商VPDN或无线专网链路接入公安视频传输网，禁止跨网络和互联网连接。

5.9.3 应通过预置或管控接口对前端设备WLAN模块进行配置，禁止前端设备开启热点、相互直连。

5.9.4 应通过预置或管控接口配置前端设备网络访问规则，禁止前端设备操作系统或应用与未知或未授权服务器进行交互。

5.9.5 在发布、下载、安装应用时，应通过数字签名确保应用的完整性、一致性和安全性，应通过黑白名单对应用的安装、卸载、更新等权限进行控制。

5.9.6 应通过管控接口对前端设备状态进行监测采集，采集上报的信息包括但不限于：获取ROOT权限行为、登录失败行为、SIM/USIM卡状态、密码模块状态、证书状态和互联网连通性状态。

5.9.7 应通过管控接口对前端设备进行远程管理，操作包括但不限于：远程锁定/解锁、数据擦除、远程关机/重启、定位信息上报。

5.9.8 应通过刷机、OTA等方式升级更新操作系统，并通过数字签名确保升级包的完整性和一致性。

5.10 无线前端设备承载业务

5.10.1 采集类无线前端设备用于将采集和感知的数据回传到视频图像信息系统中。

5.10.2 无线前端设备应按照公安无线相关标准要求与业务系统进行交互。