ICS 13.310
A 91

中华人民共和国国家标准

GB 35114—2017

公共安全视频监控联网信息安全技术要求

Technical requirements for information security of video surveillance network system for public security

2017-11-01 发布　　2018-11-01 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

本标准的全部技术内容为强制性。

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：公安部第一研究所、北京中盾安全技术开发公司、杭州恒生数字设备科技有限公司、长春吉大正元信息技术股份有限公司、北京江南天安科技有限公司、国家密码管理局商用密码检测中心、国家安全防范报警系统产品质量监督检验中心（北京）、苏州科达科技股份有限公司、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、北京中星微电子有限公司。

本标准主要起草人：陈朝武、栗红梅、王建勇、查敏中、赵惠芳、高利、闫雪、罗鹏、王冰洋、李国、林冬、张跃、陈宁、韩光瞬、刘宏伟、孙琼芳、崔云红、裴静、邱嵩、芦翔、孔维生、陈卫东。

公共安全视频监控联网信息安全技术要求

1 范围

本标准规定了公共安全领域视频监控联网视频信息以及控制信令信息安全保护的技术要求，包括公共安全视频监控联网信息安全系统的互联结构、证书和密钥要求、基本功能要求、性能要求等技术要求。

本标准适用于公共安全领域视频监控系统的信息安全方案设计、系统检测、验收以及与之相关的设备研发与检测。

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/T 2260—2007 中华人民共和国行政区划代码

GB/T 2659—2000 世界各国和地区名称代码

GB/T 7408—2005 数据元和交换格式 信息交换 日期和时间表示法

GB/T 15843.3—2008 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

GB/T 25724—2017 公共安全视频监控数字视音频编解码技术要求

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

GM/T 0005—2012 随机性检测规范

GM/T 0014—2012 数字证书认证系统密码协议规范

GM/T 0015—2012 基于SM2密码算法的数字证书格式规范

GM/T 0034—2014 基于SM2密码算法的证书认证系统密码及其相关安全技术规范

IETF RFC 2976 SIP INFO方法(The SIP INFO Method)

IETF RFC 3261 会话初始协议(SIP：Session Initiation Protocol)

IETF RFC 3548 Base16，Base32，Base64数据编码(The Base16，Base32，and Base64 Data Encodings)

IETF RFC 3550 实时传输协议(RTP：A Transport Protocol for Real-Time Applications)

IETF RFC 3725 会话初始协议(SIP)中第三方呼叫控制(3PCC)的当前最佳实现[Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)]

IETF RFC 4566 会话描述协议(Session Description Protocol)

3 术语、定义和缩略语

3.1 术语和定义

GB/T 28181—2016界定的以及下列术语和定义适用于本文件。

3.1.1

视频加密密钥(视频密钥) video encryption key

具有安全功能的前端设备随机产生的对称密钥,按照一定的规律变化,用于直接加密视频内容,实现视频传输的机密性保护。

3.1.2

视频密钥加密密钥 video key encryption key

由视频监控安全管理平台产生并分发给具有安全功能前端设备的对称密钥,按照一定的规律变化,用于对视频密钥进行加密,实现其传输的机密性保护。

3.1.3

视频导出传输密钥 video export transmission key

在视频导出过程中由视频监控安全管理平台生成,用于对视频密钥进行加密,实现其导出的机密性保护。

3.1.4

前端设备 front-end device

公共安全视频监控联网系统中安装于监控现场的信息采集、编码/处理、存储、传输、安全控制等设备。

3.1.5

具有安全功能的前端设备 front-end device with safety function

具有基于数字证书的设备身份认证、视频签名、视频加密等信息安全保护功能的前端设备。

3.1.6

具有安全功能的用户终端 user terminal with safety function

具有基于数字证书的用户身份认证、加密视频解密等安全功能的用户终端。

3.1.7

具有安全功能的中心信令控制服务器 central control server with safety function

具有基于数字证书的设备身份认证、信令安全、密钥分发等安全功能的中心信令控制服务器。

3.1.8

具有安全功能的媒体服务器 media server with safety function

具有基于数字证书的设备身份认证、视频加密及解密等安全功能的媒体服务器。

3.1.9

视频监控安全管理平台 security management platform in video surveillance

由具有安全功能的中心信令控制服务器、具有安全功能的媒体服务器、信令安全路由网关等功能实体组成,具备用户身份认证、设备身份认证、密钥管理、权限管理、签名验签、加密解密、访问控制、审计、加密视频数据的实时点播/历史回放/存储/下载/分发/导出、视频数据源抗抵赖,控制信令的完整性验证等功能。

3.1.10

公共安全视频监控联网信息安全系统 information security system in video surveillance network in public security use

由具有安全功能的前端设备、具有安全功能的用户终端、视频安全密钥服务系统、视频监控安全管理平台四个部分组成,能够保障视频数据及控制信令信息真实性、完整性、保密性的公共安全视频监控联网系统。

3.1.11

安全模块 security module

含有密码算法、安全功能,可实现密钥管理机制的相对独立的软件、硬件、固件或其组合。

3.1.12

密码模块　cryptographic module

在前端设备中实现随机数产生和密码运算功能的、相对独立的软件、硬件、固件或其组合。

3.1.13

用户　user

在公共安全视频监控联网信息安全系统中注册并被授权的、对系统内的数据和/或设备有操作或管理需求的使用者。

3.1.14

信令安全路由网关　secure signal routing gateway

具有接收或转发域内外 SIP 信令功能，并且完成信令安全路由网关间路由信息的传递以及路由信令、信令身份标识的添加和鉴别等功能，是一种具有安全功能的 SIP 服务器。

3.1.15

视频安全密钥服务系统　key service system for video security

具备用户和设备身份证书的制发功能，为视频监控安全管理平台提供证书查询和验证等服务，并完成对对称密钥管理的系统。

3.1.16

功能实体　functional entity

实现一些特定功能的逻辑单元的集合。

注：一个物理设备可以由多个功能实体组成，一个功能实体也可以由多个物理设备组成。

3.2　缩略语

下列缩略语适用于本文件。

CRL：证书撤销列表(Certificate Revocation List)

ECB：电码本模式(Electronic Code Book)

FDWSF：具有安全功能的前端设备(Front-end Device With Safety Function)

GOP：画面组(Group of Pictures)

IV：初始化向量(Initialization Vector)

OFB：输出反馈模式(Output Feedback)

SHA：安全哈希算法(Secure Hash Algorithm)

SIP：会话初始协议(Session Initiation Protocol)

VEK：视频加密密钥(Video Encryption Key)

VKEK：视频密钥加密密钥(Video Key Encryption Key)

4　公共安全视频监控联网信息安全系统互联结构

4.1　互联结构

公共安全视频监控联网信息安全系统(以下简称系统)互联结构见图 1。图 1 描述了单个系统内、不同系统间两种情况下，功能实体之间的连接关系。功能实体之间的通道互联协议分为会话通道协议、媒体流通道协议和证书通道协议三种类型。

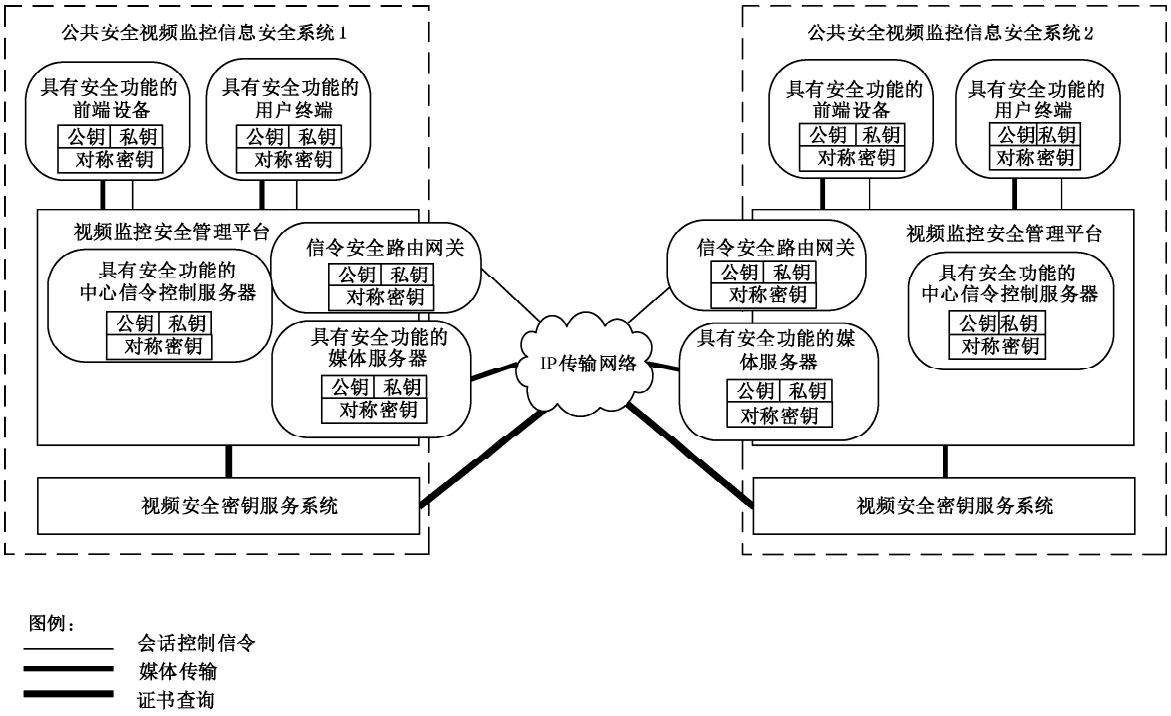

图 1　公共安全视频监控信息安全系统互联结构示意图

4.2　系统内联网

系统由具有安全功能的前端设备、具有安全功能的用户终端、视频安全密钥服务系统(以下简称视频密钥系统)、视频监控安全管理平台(以下简称管理平台)四个部分组成。各部分以传输网络为基础，通过会话通道协议、媒体流通道协议和证书通道协议连接。

4.3　系统间联网

若干个相对独立的系统以信令安全路由网关、具有安全功能的媒体服务器为核心，通过 IP 传输网络，实现系统间控制信令信息和媒体信息的传输、交换、控制。视频密钥系统间以传输网络为基础，实现证书信息的查询和交换。

4.4　联网方式

4.4.1　级联

系统的级联方式依据 GB/T 28181—2016 中的 4.1.4.1 执行。

4.4.2　互联

系统的互连方式依据 GB/T 28181—2016 中的 4.1.4.2 执行。

5　证书和密钥要求

5.1　密码算法

系统使用国家密码管理行政机构批准的非对称密码算法、对称密码算法、密码杂凑算法和随机数生成算法，算法应采用获得国家密码管理行政机构批准的安全密码产品实现。算法及使用方法如下：

a) 非对称密码算法使用 SM2 椭圆曲线密码算法，用于身份认证、数字签名、密钥协商等；
b) 对称密码算法使用 SM1、SM4 分组密码算法 OFB 模式，用于视频数据的加密保护。使用 SM4 分组密码算法 ECB 模式，用于密钥协商数据的加密保护；
c) 密码杂凑算法使用 SM3 密码杂凑算法，用于完整性校验；
d) 随机数生成算法生成的随机数应能通过 GM/T 0005—2012 中规定的方法进行检测。

5.2 数字证书类型

系统应使用基于非对称密码算法的数字证书体系实现用户身份认证、前端设备认证、服务器设备认证、管理平台间认证等安全功能。应为用户、前端设备、服务器设备以及管理平台签发数字证书。证书类型具体如下：

a) 用户证书：用于对用户的身份认证；
b) 前端设备证书：用于前端设备的身份认证以及对设备产生视频数据的数字签名；
c) 服务器设备证书：用于服务器设备的身份认证；
d) 管理平台证书：用于管理平台的身份认证。

5.3 数字证书格式

应支持 GM/T 0015—2012 中对证书格式和证书撤销列表(CRL)的规定。统一的证书格式见附录 A。

5.4 密钥种类

系统的密钥分为非对称密钥类和对称密钥类。非对称密钥类包括管理平台内功能实体的签名公私钥和加密公私钥、FDWSF 签名公私钥、具有安全功能的用户终端签名公私钥等。对称密钥类有视频密钥加密密钥、视频加密密钥等。

6 基本功能要求

6.1 统一编码规则

系统对 FDWSF、服务器设备、具有安全功能的用户终端进行统一编码，见 GB/T 28181—2016 的附录 D 中 D.1。集成在 FDWSF 的密码模块，应有唯一的标识，编码规则见附录 B。

6.2 用户身份认证

应对用户基本信息、属性信息以及用户 ID 与用户证书的对应关系作管理。应对所有用户进行身份认证。应支持基于数字证书的用户认证，认证流程见附录 C 中 C.1。

6.3 前端设备分级

6.3.1 根据安全保护强弱，将 FDWSF 的安全能力分为三个等级，由弱到强分别是 A 级、B 级、C 级，见表 1。

6.3.2 A 级应基于数字证书与管理平台双向身份认证的能力，达到身份真实目标。

6.3.3 B 级应具备基于数字证书与管理平台双向身份认证的能力和对视频数据签名的能力，达到身份真实和视频来源于真实设备，能够校验视频内容是否遭到篡改的目标。

6.3.4 C 级应具备基于数字证书与管理平台双向身份认证的能力、视频数据签名能力和视频数据加密能力，达到身份真实和视频来源于真实设备，能够校验视频内容是否遭到篡改，能够达到对视频内容加密保护目标。

表 1　前端设备分级

等级	基于数字证书与管理平台双向设备认证能力，达到身份真实目标	基于数字证书的视频数据签名能力，达到视频来源于真实设备且可校验视频是否遭到篡改的目标	视频加密能力，达到视频加密保护目标
A 级	√	—	—
B 级	√	√	—
C 级	√	√	√

6.4　设备身份认证

6.4.1　管理平台应对 FDWSF 的基本信息、属性信息以及 FDWSF 的 ID、其密码模块 ID 与设备证书的对应关系作管理。

6.4.2　管理平台应对所有接入的 FDWSF 进行单向设备身份认证或者双向设备身份认证。认证流程见 C.2，消息示例参见 D.1 和 D.2。

6.5　管理平台间认证

管理平台互联互通时应进行管理平台间的双向身份认证。认证流程见 C.3。

6.6　授权与访问控制

6.6.1　在设备身份认证的基础上，管理平台应采用基于属性或基于角色的访问控制模型对用户进行授权管理和访问控制。

6.6.2　管理平台访问控制的粒度应至少包含前端设备的安全能力等级以及存储视频是否加密等属性。

6.6.3　在系统中访问加密视频信息的用户应是经过基于数字证书认证的用户，包括对加密视频的播放、回放、下载、删除等操作。

6.6.4　当跨域访问时，应采用信令 Monitor-User-Identity 携带的用户身份信息进行访问控制。对 C 级设备的访问要做严格的控制。

6.7　控制信令认证

6.7.1　管理平台和 FDWSF 应采用带密钥的杂凑算法 SM3 对设备遥控等重要的 SIP 控制信令做认证。

6.7.2　在 SIP 消息头域中，启用 Date 域，增加 Note 域。Note＝(Digest nonce＝"", algorithm＝)，nonce 的值为杂凑运算结果经过 Base64 编码后的值，algorithm 的值为杂凑算法名称。控制信令认证的流程和方法规定见 C.4，消息示例参见 D.3。

6.7.3　当跨域访问时，若该信令是由本域的用户发起，则信令安全路由网关应将发送到外域的信令添加 Monitor-User-Identity 头域，其取值为信令安全路由网关 ID 和用户的身份信息；若该信令不是由本域的用户发起，则只在原有 Monitor-User-Identity 域值前添加信令安全路由网关 ID；各段分隔符为“-”。用户的身份为用户 ID 以及用户身份属性信息(用户身份属性信息包括：用户隶属机构属性、用户类别属性和用户职级属性)。

6.8　视频源签名及完整性校验

6.8.1　所有 B 级和 C 级 FDWSF 应对采集的视频进行视频数据签名操作并基于 TCP 协议进行传输。

6.8.2　所有 B 级和 C 级 FDWSF 应支持对视频 I 帧及其他关键帧的签名。

6.8.3　管理平台应支持对视频数据签名结果的接收、存储和验证，实现视频源的抗抵赖及完整性校验。

6.8.4　视频数据签名和验签的格式和流程见 C.5，消息示例参见 D.4。

6.9 视音频加密

6.9.1 所有C级FDWSF应对采集的视频及音频进行加密操作并传输。

6.9.2 管理平台应支持视频及音频加密数据的传输，支持用户在权限范围内对实时加密视音频播放、历史加密视音频回放、加密视音频的存储/下载/分发/导出等操作。

6.9.3 视音频加密格式和流程见C.6，消息示例参见D.5～D.11。

6.9.4 视频导出时管理平台应更换视频密钥加密密钥，具体流程参见附录E。

6.9.5 加密视频直接存储到存储设备。

6.10 设备异常管理报警

6.10.1 管理平台应能及时发现FDWSF的异常情况，如非授权处理、密码模块损坏或丢失。

6.10.2 管理平台应能及时感知设备异常情况，如报警等，并同时写入日志。

6.11 安全管理

6.11.1 系统应设置安全管理员、安全操作员和安全审计员三类管理员角色。

6.11.2 安全管理员负责系统的安全参数配置、系统服务器启动和停止，不具有安全业务操作的权限。

6.11.3 安全操作员按其权限进行具体的安全业务操作，包括密钥生成、导入、备份和恢复等操作。

6.11.4 安全审计员负责系统的审计管理，负责对涉及系统安全的事件和各类管理、操作人员的行为进行审计和监督。

6.11.5 系统应使用数字证书和静态口令、动态口令、生物识别等其他认证因子相结合的方式认证安全管理员、安全操作员及安全审计员的身份，身份认证成功后才能登录系统进行操作。

6.12 日志管理

6.12.1 管理平台应对用户认证、设备认证、密钥管理等安全操作和各种异常安全事件，包括密钥协商失败、数据加解密失败、完整性校验失败等记录日志。

6.12.2 管理平台应具备获取FDWSF各种异常安全事件日志的功能。包括设备认证失败、密钥协商失败、数据加解密失败、完整性校验失败等。

6.13 非对称密钥管理

非对称密钥对及其证书应按照GM/T 0034—2014进行管理。

6.14 对称密钥管理

6.14.1 系统应对所使用的对称密钥进行完整生命周期的管理。

6.14.2 视频密钥加密密钥VKEK在设备注册时更新，并安全传输到具有安全功能前端设备的密码模块中安全存储。管理平台应使用安全模块安全保存所有前端设备的VKEK，保存周期应满足历史视频保存时间的要求。

6.14.3 视频密钥加密密钥VKEK更新周期不大于1天。视频加密密钥VEK更新周期不大于1 h。

7 性能要求

7.1 设备身份认证

在符合GB/T 28181—2016中5.5网络传输质量要求前提下，设备身份双向认证时间延迟不超过400 ms。双向认证时间延迟，不包含穿越安全边界平台及设备等实际网络中其他必须存在的设备

延时。

7.2 视频数据签名

FDWSF 视频数据签名，应不小于 1 次/s。

7.3 视频加解密

C 级 FDWSF 应能支持全码流加密，在符合 GB/T 28181—2016 中 5.5 网络传输质量要求前提下，视频加密/解密增加的延时不超过 400 ms。