

ICS 13.310
CCS A91



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB 35114-2017

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

公共安全视频监控联网信息安全技术要求

Issued on: November 1, 2017

Implemented on: November 1, 2018

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the People's Republic of China;
Standardization Administration of China**

Table of Contents

1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviations	1
3.1 Terms and Definitions	1
3.2 Abbreviations	3
4 Public safety video surveillance networked information security system interconnection structure	3
4.1 Interconnect structure	3
4.2 System Intranet	4
4.3 Intersystem networking	4
4.4 Networking Mode	4
5 Certificate and Key Requirements	4
5.1 Cryptographic Algorithm	4
5.2 Digital Certificate Type	5
5.3 Digital Certificate Format	5
5.4 Key Type 5 6 basic function requirements	5
6.1 Uniform coding rules	5
6.2 User Authentication	5
6.3 Front End Equipment Rating	5
6.4 Device Identity	6
6.5 Management Platform Authentication	6
6.6 Authorization and Access Control	6
6.7 Control Signaling Certification	6
6.8 Video Source Signature and Integrity Check	6
6.9 Video and Audio Encryption	7
6.10 Device Abnormal Management Alarm	7
6.11 Security Management	7
6.12 Log Management	7
6.13 Asymmetric Key Management	7
6.14 Symmetric Key Management	7
7 Performance requirements	7
7.1 Device Identity	7

7.2 Video data signature	8
45 Appendix E (informative) Export of encrypted video 101 Reference	103

Foreword

The full technical content of this standard is mandatory. This standard was drafted in accordance with the rules given in GB/T 1.1-2009. Please note that some of the contents of this document may involve patents. The issuing organization of this document is not responsible for identifying these patents. This standard is proposed and managed by the Ministry of Public Security of the People's Republic of China. This standard was drafted. The First Institute of the Ministry of Public Security, Beijing Zhongdun Security Technology Development Company, Hangzhou Hengsheng Digital Equipment Technology Co., Ltd. Division, Changchun Jida Zhengyuan Information Technology Co., Ltd., Beijing Jiangnan Tianan Technology Co., Ltd., National Cryptographic Administration Commercial Password Detection Center, National Security and Alarm System Product Quality Supervision and Inspection Center (Beijing), Suzhou Keda Technology Co., Ltd., Zhejiang Dahua Technology Co., Ltd., Hangzhou Hikvision Digital Technology Co., Ltd., Beijing Zhongxing Microelectronics Co., Ltd. The main drafters of this standard. Chen Chaowu, Li Hongmei, Wang Jianyong, Cha Minzhong, Zhao Huifang, Gao Li, Yan Xue, Luo Peng, Wang Bingyang, Li Guo, Lin Dong, Zhang Yue, Chen Ning, Han Guangxuan, Liu Hongwei, Sun Qiongfang, Cui Yunhong, Qi Jing, Qiu Yi, Lu Xiang, Kong Weisheng, Chen Weidong. Public safety video surveillance network information security skills requirement

1 Scope

GB 35114-2017 is the Chinese national standard on technical requirements for information security of video surveillance network system for public security, in the field of environment and health protection, safety. It carries no /T suffix, which in the Chinese system means compliance is mandatory: a product or a practice within its scope has to meet it to be lawfully made, sold or carried out in China. It was issued on 1 November 2017 by the General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China; Standardization Administration of China, and has been in force since 1 November 2018. Classification: ICS 13.310, CCS A91. This page is published from the official record of the standard held by the Chinese standards administration: the identification, the dates, the classification and the issuing body are taken from there. The clause text, the tables and the numeric limits are in the document itself, which is delivered complete in English translation.

This standard specifies the technical requirements for video surveillance networked video information and control signaling information security protection in the public security field, including Public safety video surveillance networked information security system

interconnection structure, certificate and key requirements, basic functional requirements, performance requirements, etc. Claim. This standard applies to the information security scheme design, system testing, acceptance and related equipment of the video surveillance system in the public security field. R & D and testing.

2 Normative references

The following documents are indispensable for the application of this document. For dated references, only dated versions apply to this article. Pieces. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 2260-2007 Administrative division code of the People's Republic of China

GB/T 2659-2000 World countries and regions name code

GB/T 7408-2005 Data element and exchange format information exchange date and time representation

GB/T 15843.3-2008 Information technology - Security technology - Entity identification - Part 3. Mechanisms using digital signature technology

GB/T 25724-2017 Public safety video surveillance digital video and audio codec technical requirements

GB/T 28181-2016 Technical requirements for information transmission, exchange and control of public safety video surveillance networking systems

GM/T 0005-2012 Randomness Test Specification

GM/T 0014-2012 Digital Certificate Authentication System

Cryptographic Protocol Specification

GM/T 0015-2012 Digital certificate format

specification based on SM2 cryptographic algorithm

GM/T 0034-2014 Certificate authentication system password based on SM2 cryptographic algorithm and related

security technical specifications

IETF RFC 2976 SIP INFO method (TheSIPINFOMethod)

IETF RFC 3261 Session Initiation Protocol (SIP. SessionInitiationProtocol)

IETF RFC 3548 Base16, Base32, Base64 data encoding (TheBase16, Base32, andBase64DataEncod-

Ing)

IETF RFC 3550 Real-Time Transport Protocol (RTP.

ATransportProtocolforReal-TimeApplications)

IETF RFC 3725 Current Best Practice for Third

Party Call Control (3PCC) in Session Initiation Protocol (SIP) [BestCurrent

PracticesforThirdPartyCalControl(3pcc)intheSessionInitiationProtocol(SIP)]

IETF RFC 4566 Session Description Protocol (SessionDescriptionProtocol)

3.1 Terms and definitions The following terms and definitions defined in

GB/T 28181-2016 apply to this document.

3.1.1 The symmetric key randomly generated by the front-end device with security function is changed according to a certain law and used to directly encrypt the video content. The confidentiality protection of video transmission.

3.1.2 Used to encrypt the video key to achieve confidentiality protection of its transmission.

3.1.3 protection.

3.1.4 Information collection, coding/processing, storage, transmission, security control, etc. installed in the monitoring site in the public safety video surveillance networking system equipment. 3.1.5 3.1.6 3.1.7 3.1.8

3.1.9 Body composition, with user identity authentication, device identity authentication, key management, rights management, signature verification, encryption and decryption, access control, auditing, Real-time on-demand/history playback/storage/download/distribution/export of encrypted video data, non-repudiation of video data sources, integrity check of control signaling Certificate and other functions.

3.1.10 The public platform is composed of four parts, which can guarantee the authenticity, integrity and confidentiality of video data and control signaling information. Networked system. 3.1.11 3.1.12

3.1.13 Registered and authorized in the public safety video surveillance networked information security system, operating or managing data and/or equipment within the system The user of the need.

3.1.14 The function of adding and authenticating the signaling identity is a SIP server with security functions.

3.1.15 A system of pairwise symmetric key management.

3.1.16

Note. A physical device can consist of multiple functional entities, and a functional entity can also consist of multiple physical devices.

3.2 Abbreviations The following abbreviations apply to this document. CRL. Certificate Revocation List (CertificateRevocationList) ECB. Codebook Mode (ElectronicCodeBook) FDWSF. Front-end device with security function (Front-endDeviceWithSafetyFunction) GOP. Group of Pictures (GroupofPictures) IV. Initialization Vector (InitializationVector) OFB. Output Feedback Mode (OutputFeedback) SHA. Secure Hash Algorithm (SecureHashAlgorithm) SIP. Session Initiation Protocol (SessionInitiationProtocol) VEK. Video Encryption Key (VideoEncryptionKey) VKEK. Video Key Encryption Key (VideoKeyEncryptionKey)

4 Public safety video surveillance network information security system interconnection structure

4.1 Interconnect structure The public security video surveillance network information security system (hereinafter referred to as the system) interconnection structure is shown in Figure 1. Figure 1 depicts a single system, The connection between functional entities in