

ICS 13.310

GA

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

GA/T 1788.2-2021

**Security technical requirements for video and image
information system for public security - Part 2: Front-end device
(English Translation)**

Issued on: July 20, 2021

Implemented on: December 1, 2021

Issued by: Ministry of Public Security of the People's Republic of China

Table of Contents

Foreword...	3
1 Scope...	4
2 Normative references...	4
3 Terms, definitions and abbreviations...	5
3.1 Terms and definitions...	5
3.2 Abbreviations...	5
4 Classification and grading of front-end device...	5
5 Security technical requirements...	6
5.1 General requirements...	6
5.2 Physical security...	8
5.3 Identification...	8
5.4 Access control...	9
5.5 Intrusion prevention...	10
5.6 Data security...	10
5.7 Certificate and key management...	11
5.8 Log security...	11
5.9 Management and control of wireless interactive front-end device...	11
5.10 Bearer business of wireless front-end device...	12

1 Scope

This document specifies the classification and grading description of the front-end device in the public security video and image information system, as well as the security technical requirements for the front-end device.

This document is applicable to the design, manufacture and inspection of the front-end device of the public security video and image information system.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 20271, Information security technology - Common security techniques requirement

for information system

GB/T 28181-2016, Technical requirements for information transport, switch and control in video surveillance network system for public security

GB 35114-2017, Technical requirements for information security of video surveillance network system for public security

GM/T 0021, One time password application of cryptography algorithm

GA/T 1400-2017 (all parts), Video and image information application system for public security - Part 1: General technical requirements

GA/T 1788.1-2021, Security technical requirements for video and image information system for public security - Part 1: General requirements

3.1 Terms and definitions

The terms and definitions defined in GB/T 28181-2016, GB/T 20271, GB 35114-2017, GA/T 1788.1-2021 apply to this document.

3.2 Abbreviations

The following abbreviations apply to this document.

HTTP: Hyper Text Transfer Protocol

IP: Internet Protocol

MAC: Media Access Control

OTA: Over the Air

SIM: Subscriber Identify Module

SSH: Secure Shell

SSID: Service Set Identifier

TLS: Transport Layer Security

WEP: Wired Equivalent Privacy

WIFI: Wireless Fidelity

WLAN: Wireless Local Area Network

WPA: Wi-Fi Protected Access)

WPS: Wi-Fi Protect Setup

WSSE: Web Service Security

4 Classification and grading of front-end device

4.1

Front-end device is divided into wired front-end device and wireless front-end device according to the transmission mode. Front-end device that completes access, transmission, and use based on wireless communication technology is called wireless front-end device.

front-end device transmitted using the GB/T 28181 protocol, the certification process shall comply with the provisions of 9.1 in GB/T 28181-2016. The front-end device using GA/T 1400 protocol transmission shall comply with the provisions of 7.2.1 and

7.3.1 in GA/T 1400.4-2017. The front-end device accessed by HTTP protocol shall support security mode for identity authentication, such as Digest authentication and

WSSE authentication.

5.3.1.4 When the front-end device is connected, and when the collection device is connected to the access device, the device identity authentication based on digital certificate is adopted. Its front-end device certification process shall comply with the provisions of C.2 in Annex C of GB 35114-2017.

5.3.2 Authentication failure processing

5.3.2.1

After the front-end device fails to authenticate 5 times in a row, it shall lock the account for no less than 5min. It can support the setting of consecutive authentication failure times and lock time.

5.3.2.2

After the account of the front-end device is locked, it can be unlocked through at least one or more methods, such as unlocking by a user with higher authority.

5.3.3 Timeout processing

5.3.3.1

The communication session shall support setting the maximum timeout period.

If the timeout period can be modified, it shall only be set by authorized users.

5.3.3.2 If the communication session does not perform any operations within the

maximum timeout period, the session shall be terminated. Identity verification shall be performed when operating again.

5.4 Access control

5.4.1

The default account shall be renamed or deleted on first login. For default accounts that cannot be deleted, their default passwords shall be modified.

5.4.2

Collection devices shall support the use of special tools to set management account passwords centrally and uniformly.

5.4.3

It shall support deletion or deactivation of redundant, expired accounts. Sharing accounts is prohibited.

5.4.4

It shall support granting the minimum permissions required by management users, so as to realize the separation of permissions for management users.

5.4.5

The granularity of access control shall at least include attributes such as IP/MAC.

5.4.6

It shall support setting the maximum number of sessions.

5.4.7

Unauthorized users shall be prohibited from accessing system files of the operating system.

5.4.8

Unauthorized users shall be prohibited from configuring or changing the software on the front-end device.

5.4.9

When the user accesses the front-end device through the public security video and image information system, the front-end device only receives protocol access based on GB/T 28181-2016, GA/T 1400-2017 or GB 35114-2017.

5.4.10 When a user directly accesses the front-end device, the front-end device only

receives access from a specific IP address or based on peripheral equipment.