Hikvision Network Camera Series iDS-2CD7x V5.9.22

Security Target

Version 1.5

Document history

Version	Date	Comment	Author
1.0	2025-03-06	First Release	Zhu zhenyu
1.1	2025-05-24	Update according to the CC:2020 version	Zhu zhenyu
1.2	2025-06-12	Review comments fix from NSCIB	Zhu zhenyu
1.3	2025-07-30	Review comments fix from NSCIB	Zhu zhenyu
1.4	2025-09-23	Review comments fix from NSCIB	Zhu zhenyu
1.5	2025-10-07	Review comments fix from NSCIB	Zhu zhenyu

Contents

1 Security Target Introduction

1.1 Security Target Reference

ST Title	Hikvision Network Camera Series iDS-2CD7x V5.9.22 Security Target
ST Version	1.5
ST Date	October 7th 2025
Author	Hangzhou Hikvision Digital Technology Co.,Ltd. No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China

Table 1 Security Target reference

1.2 TOE Reference

TOE Name	Hikvision Network Camera Series iDS-2CD7x
TOE Version	V5.9.22
TOE Components	The TOE is Hikvision Network Camera series consisting of the network camera models, firmware, and the guidance. The name of the camera models, the version of firmware are listed in *Table 4* The version of user guidance is listed in Table 5.
Developer	Hikvision
TOE Type	Network Camera

Table 2 TOE reference

x in the TOE name includes the models:

026G2-AP
046G2-AP
046G2/E-AP
086G2/E-AP
086G2-AP
126G2-IZ(H)S(Y)
146G2-IZ(H)S(Y)(1T)
186G2-IZ(H)S(Y)
A26G2-IZHS(Y)
A46G2-IZHS(Y)(1T)
A86G2-IZHS(Y)
A46G2-IZHS(Y)/5G
A86G2-IZHS(Y)/5G
546G2-XZHS(Y)
586G2-XZHS(Y)
A47G2-XZHS(Y)
A87G2-XZHS(Y)
A46G2-IZHS(Y)长焦
A45G2-IZHS(Y)
0C6G2-AP
0C6G2/E-IHSYR
1C6G2-IZ(H)S(Y)
AC6G2-IZHS(Y)
547G2-ZHS/RC(eF)
547G2-XZHS(Y)(eF)

587G2-XZHS(Y)(eF)
587G2-ZHS/RC(eF)
A46G2-IZHS(Y)(4G)
A86G2-IZHS(Y)(4G)
546G2/P-XZHS(Y)
586G2/P-XZHS(Y)
A46G2(/P)-IZHS(Y)(5G)
A86G2(/P)-IZHS(Y)(5G)
A46G2/P-IZHS(Y)(长焦)
A46G2/P-IZHS(Y)
A86G2/P-IZHS(Y)
A47G2/P-XZHS(Y)
A87G2/P-XZHS(Y)
A45G2/P-IZHS(Y)
046G2/P-AP
086G2/P-AP
046G2/EP-IHSY
086G2/EP-IHSY
547G2/P-XZHS(Y)(2.8-12mm
587G2/P-XZHS(Y)(2.8-12mm
A46G2/P-IZHS(Y)(4G)
A86G2/P-IZHS(Y)(4G)
026G2-AP
046G2-AP
046G2/E-AP
086G2/E-AP
086G2-AP
126G2-IZ(H)S(Y)
146G2-IZ(H)S(Y)(1T)
186G2-IZ(H)S(Y)
A26G2-IZHS(Y)
A46G2-IZHS(Y)(1T)
A86G2-IZHS(Y)
A46G2-IZHS(Y)/5G
A86G2-IZHS(Y)/5G
546G2-XZHS(Y)
586G2-XZHS(Y)
A47G2-XZHS(Y)
A87G2-XZHS(Y)
A46G2-IZHS(Y)长焦
A45G2-IZHS(Y)
0C6G2-AP
0C6G2/E-IHSYR
1C6G2-IZ(H)S(Y)
AC6G2-IZHS(Y)
547G2-ZHS/RC(eF)
547G2-XZHS(Y)(eF)
587G2-XZHS(Y)(eF)
587G2-ZHS/RC(eF)
A46G2-IZHS(Y)(4G)
A86G2-IZHS(Y)(4G)
546G2/P-XZHS(Y)
586G2/P-XZHS(Y)

A46G2(/P)-IZHS(Y)(5G)
A86G2(/P)-IZHS(Y)(5G)
A46G2/P-IZHS(Y)(长焦)
A46G2/P-IZHS(Y)
A86G2/P-IZHS(Y)
A47G2/P-XZHS(Y)
A87G2/P-XZHS(Y)
A45G2/P-IZHS(Y)
046G2/P-AP
086G2/P-AP
046G2/EP-IHSY
086G2/EP-IHSY
547G2/P-XZHS(Y)(2.8-12mm
587G2/P-XZHS(Y)(2.8-12mm
A46G2/P-IZHS(Y)(4G)
A86G2/P-IZHS(Y)(4G)

1.3 **TOE Overview**

1.3.1 TOE Type

The Target of Evaluation (TOE) is a Network Camera series developed by Hikvision and will hereafter be referred to as the TOE throughout this document. The TOE is a Network camera which comprises a hardware board and a specific firmware for the hardware. Hikvision has considered the European data law GDPR and as a result selected a set of SFRs to be included in the ST.

The TOE provides the following functionality:

- Management interface.
- Video over IP.
- Security audit

The TOE consists of Series iDS-2CD7. The following list details the models in scope for the family:

iDS-2CD7026G2-AP
iDS-2CD7046G2-AP
iDS-2CD7046G2/E-AP
iDS-2CD7086G2/E-AP
iDS-2CD7086G2-AP
iDS-2CD7126G2-IZ(H)S(Y)
iDS-2CD7146G2-IZ(H)S(Y)(1T)
iDS-2CD7186G2-IZ(H)S(Y)
iDS-2CD7A26G2-IZHS(Y)
iDS-2CD7A46G2-IZHS(Y)(1T)
iDS-2CD7A86G2-IZHS(Y)
iDS-2CD7A46G2-IZHS(Y)/5G
iDS-2CD7A86G2-IZHS(Y)/5G
iDS-2CD7546G2-XZHS(Y)
iDS-2CD7586G2-XZHS(Y)
iDS-2CD7A47G2-XZHS(Y)

iDS-2CD7A87G2-XZHS(Y)
iDS-2CD7A46G2-IZHS(Y)长焦
iDS-2CD7A45G2-IZHS(Y)
iDS-2CD70C6G2-AP
iDS-2CD70C6G2/E-IHSYR
iDS-2CD71C6G2-IZ(H)S(Y)
iDS-2CD7AC6G2-IZHS(Y)
iDS-2CD7547G2-ZHS/RC(eF)
iDS-2CD7547G2-XZHS(Y)(eF)
DS-2CD7587G2-XZHS(Y)(eF)
iDS-2CD7587G2-ZHS/RC(eF)
iDS-2CD7A46G2-IZHS(Y)(4G)
iDS-2CD7A86G2-IZHS(Y)(4G)
iDS-2CD7546G2/P-XZHS(Y)
iDS-2CD7586G2/P-XZHS(Y)
iDS-2CD7A46G2(/P)-IZHS(Y)(5G)
iDS-2CD7A86G2(/P)-IZHS(Y)(5G)
iDS-2CD7A46G2/P-IZHS(Y)(长焦)
iDS-2CD7A46G2/P-IZHS(Y)
iDS-2CD7A86G2/P-IZHS(Y)
iDS-2CD7A47G2/P-XZHS(Y)
iDS-2CD7A87G2/P-XZHS(Y)
iDS-2CD7A45G2/P-IZHS(Y)
iDS-2CD7046G2/P-AP
iDS-2CD7086G2/P-AP
iDS-2CD7046G2/EP-IHSY
iDS-2CD7086G2/EP-IHSY
iDS-2CD7547G2/P-XZHS(Y)(2.8-12mm
iDS-2CD7587G2/P-XZHS(Y)(2.8-12mm
iDS-2CD7A46G2/P-IZHS(Y)(4G)
iDS-2CD7A86G2/P-IZHS(Y)(4G)
iDS-2CD7026G2-AP
iDS-2CD7046G2-AP
iDS-2CD7046G2/E-AP
iDS-2CD7086G2/E-AP
iDS-2CD7086G2-AP
iDS-2CD7126G2-IZ(H)S(Y)
iDS-2CD7146G2-IZ(H)S(Y)(1T)
iDS-2CD7186G2-IZ(H)S(Y)
iDS-2CD7A26G2-IZHS(Y)
iDS-2CD7A46G2-IZHS(Y)(1T)
iDS-2CD7A86G2-IZHS(Y)
iDS-2CD7A46G2-IZHS(Y)/5G
iDS-2CD7A86G2-IZHS(Y)/5G
iDS-2CD7546G2-XZHS(Y)
iDS-2CD7586G2-XZHS(Y)
iDS-2CD7A47G2-XZHS(Y)
iDS-2CD7A87G2-XZHS(Y)
iDS-2CD7A46G2-IZHS(Y)长焦
iDS-2CD7A45G2-IZHS(Y)
iDS-2CD70C6G2-AP
iDS-2CD70C6G2/E-IHSYR
iDS-2CD71C6G2-IZ(H)S(Y)

iDS-2CD7AC6G2-IZHS(Y)
iDS-2CD7547G2-ZHS/RC(eF)
iDS-2CD7547G2-XZHS(Y)(eF)
DS-2CD7587G2-XZHS(Y)(eF)
iDS-2CD7587G2-ZHS/RC(eF)
iDS-2CD7A46G2-IZHS(Y)(4G)
iDS-2CD7A86G2-IZHS(Y)(4G)
iDS-2CD7546G2/P-XZHS(Y)
iDS-2CD7586G2/P-XZHS(Y)
iDS-2CD7A46G2(/P)-IZHS(Y)(5G)
iDS-2CD7A86G2(/P)-IZHS(Y)(5G)
iDS-2CD7A46G2/P-IZHS(Y)(长焦)
iDS-2CD7A46G2/P-IZHS(Y)
iDS-2CD7A86G2/P-IZHS(Y)
iDS-2CD7A47G2/P-XZHS(Y)
iDS-2CD7A87G2/P-XZHS(Y)
iDS-2CD7A45G2/P-IZHS(Y)
iDS-2CD7046G2/P-AP
iDS-2CD7086G2/P-AP
iDS-2CD7046G2/EP-IHSY
iDS-2CD7086G2/EP-IHSY
iDS-2CD7547G2/P-XZHS(Y)(2.8-12mm
iDS-2CD7587G2/P-XZHS(Y)(2.8-12mm
iDS-2CD7A46G2/P-IZHS(Y)(4G)
iDS-2CD7A86G2/P-IZHS(Y)(4G)

1.3.2 TOE Usage and Major Security Features

1.3.2.1 TOE Usage

TOE environment consists of a network which is isolated from other networks (e.g. other LANs or Internet) by Isolated Network Devices (e.g. it can be either Firewall/Gateway/Physical device). The TOE network may contain the following components: one or multiple TOEs (IPCs), video recording devices (such as NVR) and management computers (Test PC in Figure1) via ISAPI. Figure 1 illustrates the environment where the TOE is intended to be used:

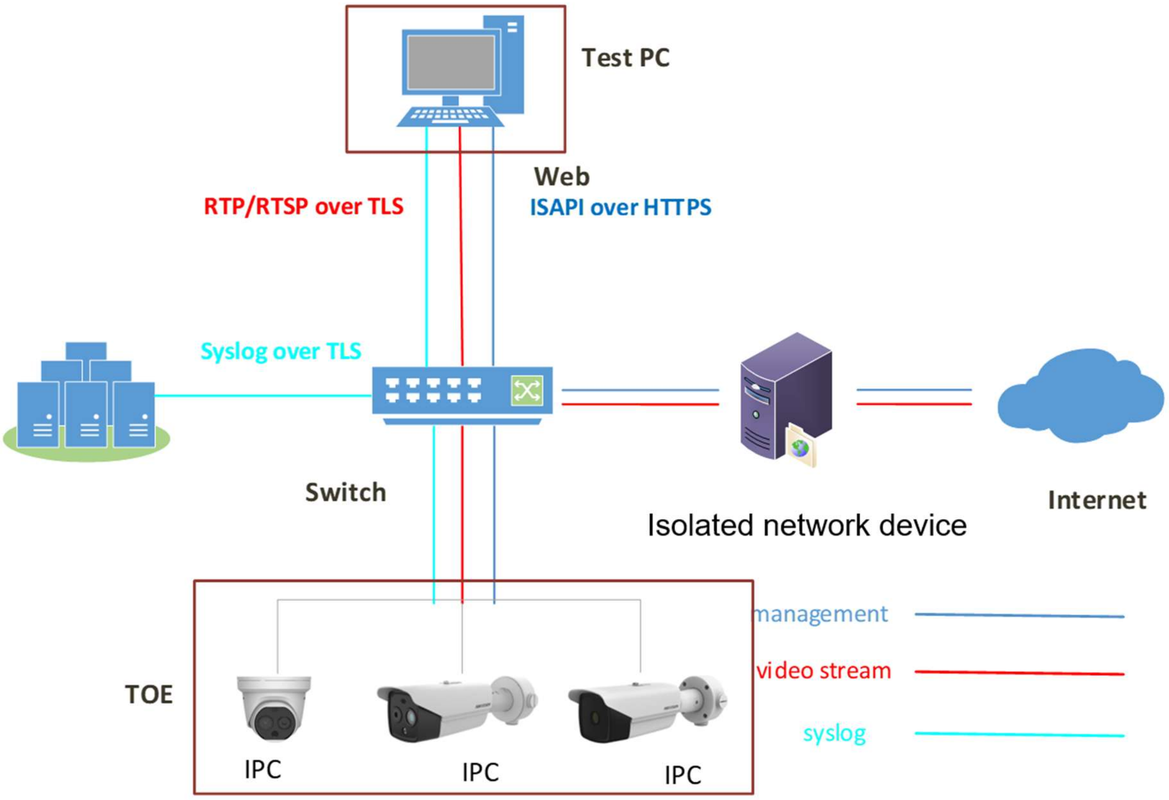

Figure 1 TOE usage scenario.

Note that neither the management nor the video stream are accessible from the internet. The "Isolated Network Device" depicted in Figure 1 TOE usage scenario. prevents accessing the TOE from internet, while allowing the access to other non-TOE devices that might be connected to the TOE LAN.

The usage scenarios in scope of the evaluation are:

- The test PC has the web browser to access the TOE to have all management functions.
- Media interface which is used to send audio and video to the clients connected to the Test PC and internet by going throw isolated network device.
- TOE's management interface being accessed from a browser or a client/platform software using ISAPI over HTTPS. ISAPI protocol is an HTTP-based application programming interface that enables the TOE to build communication between security devices/servers (e.g., NVR) and the client/platform programs. Client/platform programs must implement this ISAPI protocol.
- NVR is a physical device used to record and store video. The video is received via RTP/RTSP protocol over TLS. It is optional and out of the scope.
- Exporting audit logs to a trusted syslog server through syslog protocol over TLS.

1.3.2.2 TOE Major Security Features

The TOE provides the following major security features:

- Security management
- User identification and authentication
- Trusted path/channel
- Security Audit
- Protection of the TSF

- Limited TOE access
- Cryptographic operation

The TOE provides confidentiality protection of the video data when distributing it to external entities through the TOE network.

The TOE also provides additional features corresponding to a Network Camera TOE type. These features are considered only functional features; therefore they are not security related and not part of the evaluation scope. The supported features include (among others, and dependant on the TOE model):

- Image processing options such as face detection, intrusion detection, unattended baggage detection, privacy mask, etc.
- Support for different video resolutions and frame rates, image settings (saturation, brightness, contrast…) and multiple simultaneous video streams.
- Support for multiple video data encoding and compression standards.

1.3.3 Required Non-TOE Hardware/Software/Firmware

As illustrated in Figure 1, the TOE network may contain the following components: the TOE (one or multiple), video recording devices (e.g. NVR), management devices via ISAPI protocol over HTTPS and RTP/RTSP protocol over TLS, and the Syslog server for receiving the audit logs via syslog protocol over TLS.

Component	Required	Scope	Description
Management computer with a web browser	Mandatory	No	General purpose computer, based on Windows and/or macOS platforms, that is used to manage the TOE using a web interface implementing ISAPI protocol over HTTPS and to receive video data through the RTP/RTSP protocol over TLS.
Network Video Recorder (NVR)	Optional	No	Physical device used to record and store video. The video is received via RTP/RTSP protocol over TLS
Client/Platform	Optional	No	General purpose computer which implements a software solution to record and store video from the TOE using RTP/RTSP protocol over TLS and/or manage the same TOE through ISAPI protocol over HTTPS.
Syslog Server	Optional	No	General purpose computer running syslog service and receive audit log via syslog protocol over TLS.

Table 3 Components of the environment[1]

1.4 **TOE Description**

1.4.1 Physical Scope

1.4.1.1 List of TOE models

The TOE is provided in the following format: a network camera hardware (different for each camera model), a firmware binary image file and the user guidance documentation.

The TOE components are shown below:

[1] TOE environment components; NVR, web browser and Syslog Server belong to internal network.

Series	Models[1]	Version of Firmware/Software[2]	Interfaces
iDS-2CD7x	iDS-2CD7026G2-AP	Firmware: V5.9.22 Web: 5.2.46_R0101 Encoding: V7.3 Binary File: IPCG_OS_H11_EN_STD_5.9.22_250227.zip IPCG_SAP_H11_EN_STD_5.9.22_250227.zip *Note:* Web and Encoding are part of the firmware. *Note:* Binary files are used for firmware. IPCG_OS_H11_EN_STD_5.9.22_250227.zip used on non “/P” and “EP” models IPCG_SAP_H11_EN_STD_5.9.22_250227.zip used on /P and /EP models Binary files differs based on the hardware models which are specifically designed to read the vehicle number of cars. /P and /EP can recognize the vehicle plates & non /P and non /EP model cannot.	DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7046G2-AP		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7046G2/E-AP		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7086G2/E-AP		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7086G2-AP		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7126G2-IZ(H)S(Y)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7146G2-IZ(H)S(Y)(1T)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7186G2-IZ(H)S(Y)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A26G2-IZHS(Y)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A46G2-IZHS(Y)(1T)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A86G2-IZHS(Y)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A46G2-IZHS(Y)/5G		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A86G2-IZHS(Y)/5G		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7546G2-XZHS(Y)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7586G2-XZHS(Y)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A47G2-XZHS(Y)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A87G2-XZHS(Y)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A46G2-IZHS(Y)长焦		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A45G2-IZHS(Y)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD70C6G2-AP		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD70C6G2/E-IHSYR		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker

	iDS-2CD71C6G2-IZ(H)S(Y)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7AC6G2-IZHS(Y)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7547G2-ZHS/RC(eF)		DC12V, SD , audio 1in 1out, alarm 2in 2out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7547G2-XZHS(Y)(eF)		DC12V, SD , audio 1in 1out, alarm 2in 2out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	DS-2CD7587G2-XZHS(Y)(eF)		DC12V, SD , audio 1in 1out, alarm 2in 2out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7587G2-ZHS/RC(eF)		DC12V, SD , audio 1in 1out, alarm 2in 2out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A46G2-IZHS(Y)(4G)		DC12V, SD , audio 1in 1out, alarm 3in 3out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A86G2-IZHS(Y)(4G)		DC12V, SD , audio 1in 1out, alarm 3in 3out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7546G2/P-XZHS(Y)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7586G2/P-XZHS(Y)		DC12V, SD , audio 1in 1out, alarm 2in 2out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A46G2(/P)-IZHS(Y)(5G)		DC12V, SD , audio 1in 1out, alarm 2in 2out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A86G2(/P)-IZHS(Y)(5G)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A46G2/P-IZHS(Y)(长焦)		DC12V, SD , audio 1in 1out, alarm 2in 2out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A46G2/P-IZHS(Y)		DC12V, SD , audio 1in 1out, alarm 2in 2out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A86G2/P-IZHS(Y)		DC12V, SD , audio 1in 1out, alarm 1in 1out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A47G2/P-XZHS(Y)		DC12V, SD , audio 1in 1out, alarm 2in 2out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A87G2/P-XZHS(Y)		DC12V, SD , audio 1in 1out, alarm 2in 2out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A45G2/P-IZHS(Y)		DC12V, AC24V, SD , audio 1in 1out, alarm 3in 3out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7046G2/P-AP		DC12V, AC24V, SD , audio 1in 1out, alarm 3in 3out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7086G2/P-AP		DC12V, AC24V, SD , audio 1in 1out, alarm 3in 3out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7046G2/EP-IHSY		DC12V, AC24V, SD , audio 1in 1out, alarm 3in 3out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker

	iDS-2CD7086G2/EP-IHSY		DC12V, AC24V, SD , audio 1in 1out, alarm 3in 3out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7547G2/P-XZHS(Y)(2.8-12mm		DC12V, AC24V, SD , audio 1in 1out, alarm 3in 3out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7587G2/P-XZHS(Y)(2.8-12mm		DC12V, AC24V, SD , audio 1in 1out, alarm 3in 3out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A46G2/P-IZHS(Y)(4G)		DC12V, AC24V, SD , audio 1in 1out, alarm 3in 3out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker
	iDS-2CD7A86G2/P-IZHS(Y)(4G)		DC12V, AC24V, SD , audio 1in 1out, alarm 3in 3out，12 VDC, max. 100 mA，-U：build in Mic,/SL:Built-in Speaker

Table 4 TOE series and models[2]

Note: The difference between each hardware model is just the mechanical difference. There is no impact on the security features.

Type	**Name**	**Version**
Security Guidance	[AGD] Hikvision Security Guidance	Version 1.2
User Manual	UD38502B_Network Camera_User Manual_H11	V5.9.14

Table 5 Guidance documentation

The delivery of the TOE hardware (the camera itself) to customers is performed through a courier company. The TOE must be shipped in a carton box with tamper evident seal, in such a way that any tampering attempt would be visible. The firmware is shipped together with the TOE hardware. The new camera firmware can be downloaded from Hikvision's web site in zip file format. The user guidance is in PDF format and can be downloaded from Hikvision's web site in the following URL https://www.hikvision.com/en/support/download/firmware-with-cc.

1.4.2 Logical Scope

This section outlines the logical boundaries of the security functionality of the TOE.

1.4.2.1 Security Management

The TOE maintains three different roles which are assign to each user. Allowed management functions are different for each role.

1.4.2.2 User Identification and Authentication

The TOE management can be done either using a computer with a web browser supporting HTTPS or by a software platform implementing the ISAPI over HTTPS. In both cases the access to the TOE is protected by a user/password authentication. The access to the management functions implements security controls

[2] The hardware version is embedded in the model name. Note that the CPU is the same for all models, the only differences are on the image processing and memory size.

[2] The binary is the same for all models of each model series, e.g. IPCG_OS_H11_EN_STD_5.9.22_250227.zip is used on any model of the iDS-2CD7 series.

to detect unsuccessful authentication attempts and insufficient password complexity and length. In case of reaching the Administrator configurable positive integer (7 by default) consecutive unsuccessful attempts, the TOE blocks the account from which the user is trying to connect.

1.4.2.3 Trusted path/channel

A trusted path/channel implemented with HTTPS/TLS communication shall be established before accessing the TOE management functionality, video data and syslog transmission.

1.4.2.4 Security Audit

The TOE has the capability to generate audit records. TOE administrators have the ability to read the logs after establishing the trusted path and successfully log in.

The TOE has the capability to send the audit data to a trusted network entity (e.g., a syslog server).

1.4.2.5 Protection of the TSF

The TOE has self-tests during the initial start-up.

The TOE prevents reading of all TSF data.

1.4.2.6 Limited TOE Access

The TOE provides the capability to restrict the maximum number of concurrent session for a same user through the management interface. It also implements two different methods to terminate an open session: inactivity of the user or an action of the user. The session is locked after inactivity time the administrator configured and need re-authenticate.

1.4.2.7 Cryptographic Operation

TOE performs cryptographic operations such as encryption, decryption, hashing and digital signature.

1.4.2.8 Excluded functionality

Following functionality is not included within the scope of the evaluation and shall therefore be disabled or not used in the evaluated configuration as specified in the guidance.

Services	Rationale
NTP	Services and functionalities are either disabled or must not be used in the evaluated configuration, as stated in [AGD].
HTTP	
RS-232/RS-485	
External Devices	
DDNS	
PPPoE	
NAT	
SNMP (v1, v2 and v3)	
FTP	
E-mail	
Platform access	
Wireless Dial	
Self-signed certificates	

Integration Protocol	
Websocket	
SDK	
TLS1.1	

Table 6 Disabled services and functionality (Note: they are disabled in CC-mode by default)

2 Conformance claims

2.1 CC Conformance Claim

The TOE and ST claim conformance to the CC:2022 Revision 1 [1] [2] [3] [4] [5] [CEM] [Errata].

The ST claims conformance to CC Part 2 conformant and CC Part 3 conformant.

2.2 Package Claim

The Security Target claims conformance to assurance package EAL3 augmented with the following security assurance requirements:

Assurance class	Augmented assurance component
ALC	ALC_FLR.2 Flaw reporting procedures

Table 7 Augmented assurance components

2.3 Conformance Rationale

No conformance is claimed to any Protection Profile.

The assurance level was chosen to ensure that:

- The TOE has a moderate level of assurance in enforcing its security functions when instantiated in its intended environment which imposes no restrictions on assumed activity on applicable networks.
- Any remaining security flaws in the TOE that are brought to the notice of the Developer will be remediated.

3 Security Problem Definition

This chapter identifies the following:

- Significant assumptions about the TOE's operational environment.
- Threats that must be countered by the TOE or its environment
- Organisational Security Policies to be enforced

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name. OSPs are identified as P.OSP with "OSP" specifying a unique name.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumption	Definition
A.TRUSTED_USERS	It is assumed that the administrator of the TOE will correctly configure and install the TOE in its operational environment by following the provided guidance documentation. Additionally, it is assumed that the users are trustworthy and will not act in a manner harmful to the TOE.
A.TRUSTED_NETWORK_SYSTEMS	It is assumed that attackers have no chance to connect any malicious devices into the local network of the TOE.
A.NO_PHYSICAL_ACCESS	It is assumed that the following TOE environment components belong to internal network: • A management computer with a web browser • A network video recorder (NVR) client/platform • A syslog server

Table 8 Assumptions

3.2 Threats

The following table lists the threats addressed by the TOE and its environment. The assumed level of expertise of the attacker for all the threats identified below is Basic.

Threat	Definition
T.UNAUTHORISED_ACCESS	An attacker may try to gain access to TOE functionality without having the required permission. This threat includes: • Bypassing user authentication • Access to functionality without permissions, • Administrator impersonation, • Operation replay. Attackers may take advantage of poorly implemented security measures like authentication, cookie management, design of the communications, etc. By attacking this functionality, it could be possible to execute malicious operations without having the proper privileges.

Threat	Definition
T.TRANSMISSION_DISCLOSURE	An attacker may be able to obtain credentials of valid TOE users during communication between the same TOE and the other device (e.g. management computer). Weak cryptography implementation like small key sizes or the usage of deprecated algorithms and protocols may allow an attacker to sniff communications, recover credentials or manipulate the traffic. Note that this threat is applicable only for the management interfaces: ISAPI.
T.VIDEO_MANIPULATION	An attacker may try to modify the integrity of the video data sent to the recording devices (NVR). An attacker may try to manipulate video data by: • A man-in-the middle (MITM) attack intercepting the video data and modifying the content partially or totally. • Circumventing the integrity mechanisms of the video data transmission. Successful attacks may allow attackers to manipulate the video image without being detected by the system.
T.CAMERA_UNAVAIBLE	An attacker may aim to overwhelm the devices, services, and network of its intended target with fake internet traffic, rendering them inaccessible to or useless for legitimate users. • Distributed-denial-of-service (DDoS) attack may make the device lost functions in some time. • Uses invalid, unexpected, or random data as input on the network.
T.UPDATE_COMPROMISE	An attacker may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to alterations.

Table 9 Threats

3.3 Organisational Security Policies

The following table lists OSP to be enforced by security objectives.

OSP	Definition
P.FIRMWARE_RELEASE	All firmware releases must be signed across the organization.
P.KEY_SECRECY	To prevent disclosure of symmetric keys, procedures will exist to keep such keys confidential.
P.PASSWORDS	The password policy should be compliant by the following password policy: 1. Passwords have a minimum length of 8 characters. 2. Passwords have a maximum length of 16 characters. 3. Passwords contain at least 2 of the following types of characters: lower case, upper case, numbers and special characters.

Table 10 Organizational Security Policies

4 Security Objectives

4.1 Security Objectives for the TOE

Objective	Definition
O.USER_AUTHENTICATION	The TOE provides authentication mechanisms for users, of which there are 3 types: Administrator, Operator and User.
O.USER_AUTHORISATION	The TOE manages different access control to operations for different user roles, by means of a unique account and password.
O.USER_MANAGEMENT	The TOE provides management capabilities to the Administrator role for adding/removing users into the system (Operator and User roles) and to configure the access permissions to the TOE functionalities.
O.AUDIT_LOGS	The TOE supports logging of events and alarms.
O.AUDIT_VIEW	The TOE provides the authorized administrators the capability to review audit data and overwrite the oldest stored audit records if the audit trail is full. The administrators can delegate this capability to other roles.
O.AUDIT_EXPORT	The TOE is to be able to establish a secure link to an external audit server to enable external audit trail storage.
O.VIDEO_INTEGRITY	The TOE provides means to ensure the integrity of the video data generated.
O.TRUSTED_PATH	The TOE provides the capacity to establish a trusted path (using a unique operation ID) before accessing the management functionality.
O.VIDEO_PROTECTION	The TOE provides confidentiality protection of the video data when distributing it to external entities through the TOE network
O.SOFTWARE_VERIFIED	The TOE provides to self-verify executable code in the TSF.
O.KEY_SECRECY	The TOE ensures that symmetric keys are kept confidential in the TSF.

Table 11 Objectives for the TOE

4.2 Security Objectives for the Operational Environment

Objective	Definition
OE.TRUSTED_USERS	Administrator of the TOE will correctly configure and install the TOE in its operational environment by following the provided guidance documentation. Additionally, TOE users are trustworthy and will not act in a manner harmful to the TOE.
OE.TRUSTED_NETWORK_SYSTEMS	The operational environment shall prevent the attacker from performing a man-in-the-middle attack within the local network.
OE.TOE_AVAILABILITY	The operational environment shall protect the TOE against internal attacks trying to disrupt the availability of the TOE to intended users.
OE.NO_PHYSICAL_ACCESS	The following TOE environment components shall belong to internal network: • A management computer with a web browser • A network video recorder (NVR) client/platform • A syslog server
OE.PASSWORDS	The operational environment –more specifically the client or web service operating the TOE-, should comply with the password policy defined in **P.PASSWORDS**.

Table 12 Objectives for the operational environment

The rationale for the security objectives is shown in Table 15.

5 Extended Component Definition

There is no extended component definition.

6 Security Functional Requirements

Notes:

- Assignment operations have been underlined.
- Selection operations have been marked in *italics.*
    - in the case where a selection operation is contained in an assignment operation, or vice versa, then the contents are marked in *underlined italics*.
- Refinements (if any) are made in the requirements (**in bold**).
- Iterations (if any) have been indicated by adding a "/ITERATION" to the SFR and by adding a part to the requirement name (in brackets).

6.1 Cryptographic Operation

6.1.1 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access

FCS_COP.1.1/AESGCM The TSF shall perform data encryption and decryption in accordance with a specified cryptographic algorithm AES used in GCM mode and cryptographic key sizes 128 bits and 256 bits that meet the following: NIST SP 800-38D.

FCS_COP.1.1/SHA The TSF shall perform cryptographic hashing in accordance with a specified cryptographic algorithm SHA256, SHA384 and SHA512 and cryptographic key sizes 256, 384 and 512 bits that meet the following: FIPS PUB 180-4.

FCS_COP.1.1/RSA The TSF shall perform cryptographic signature services (authentication and verification) in accordance with a specified cryptographic algorithm RSA (digital signature) and cryptographic key sizes 2048 bits that meet the following: FIPS PUB 186-5.

6.1.2 FCS_CKM.6 Timing and event of cryptographic key destruction

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.6.1 The TSF shall destroy RSA and AES keys when *no longer needed*.

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method zeroization and free memory that meets the following: NIST SP 800-57

6.1.3 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_CKM.5 Cryptographic key derivation, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.3 Cryptographic key access

[FCS_RBG.1 Random bit generation, or

FCS_RNG.1 Generation of random numbers]

FCS_CKM.6 Timing and event of cryptographic key destruction]

FCS_CKM.1.1/RSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA cryptographic key pair generation and specified cryptographic key sizes 2048-bits that meet the following: FIPS PUB 186-5.

FCS_CKM.1.1/AES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm random number generation using AES and specified cryptographic key sizes 128-bits and 256-bits that meet the following: NIST SP800-90A

FCS_CKM.1.1/AESTLS The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm AES GCM mode key generation and specified cryptographic key sizes 128 bits and 256 bits that meet the following: RFC5288 and RFC5246.

6.1.4 FCS_RBG.1 Random bit generation

FCS_RBG.1	**Random bit generation**
Hierarchical to:	No other components.
Dependencies:	[FCS_RBG.2 Random bit generation (external seeding), or FCS_RBG.3 Random bit generation (internal seeding – single source)] FPT_FLS.1 Failure with preservation of secure state FPT_TST.1 TSF self-testing

FCS_RBG.1.1 The TSF shall perform deterministic random bit generation services using CTR DRBG (AES) in accordance with ISO/IEC 18031:2011 after initialization with a seed.

FCS_RBG.1.2 The TSF shall use a *TSF noise* for initialized seeding.

FCS_RBG.1.3 The TSF shall update the RBG state by *reseeding* using a *TSF noise source* in the following situations: *on demand*

6.1.5 FCS_RBG.3 Random bit generation (internal seeding – single source)

FCS_RBG.3	**Random bit generation (internal seeding – single source)**
Hierarchical to:	No other components.
Dependencies:	FCS_RBG.1 Random bit generation (RBG)

FCS_RBG.3.1 The TSF shall be able to seed the RBG using *TSF software-based noise source* CPU jitter time with a minimum of 256 bits of min-entropy.

Application note: Utilizing the inherent unpredictability of CPU timing fluctuations to generate entropy for random number generation. The CPU Jitter Random Number Generator (RNG) uses the `variations in CPU instruction execution times` to produce randomness. The RNG measures the execution time of the LFSR (Linear Feedback Shift Register) itself, as well as its supporting functions and memory access operations. These measured time differences are then incorporated into the LFSR-maintained entropy pool.

6.2 **Security Management**

6.2.1 FMT_SMR.2 Restrictions on security roles

Hierarchical to: FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.2.1 The TSF shall maintain the roles Administrator, Operator and User.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions:

The Administrator is the only role able to create, delete and modify users are satisfied.

6.2.2 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1) *Creation/deletion/modification of Operators and Users*;
2) Configuration of credentials and access permissions of existing Operators and Users;
3) Trusted path certificate management;
4) Initiate the firmware update operation.
5) Configure the authentication failure parameters
6) Configure the maximum number of concurrent sessions that belong to the same IP.
7) Configure the session inactivity time before session termination
8) *Export and import the configuration file*

6.2.3 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to *modify the behaviour of* the functions defined in FMT_SMF.1 to the Administrator.

6.2.4 FMT_MTD.1 Core Data Management

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to *manage* the TSF data (audit logs) to Administrator.

6.3 **User Identification and Authentication**

6.3.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when the *Administrator configurable positive integer within* *3 to 20* unsuccessful authentication attempts occur related to user authentication through all the interfaces.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall discard any authentication attempts originating from the account for 30 minutes.

Application note: the interfaces include only the ISAPI interface over HTTPS and RTP/RTSP interface over TLS. If the TOE is powered off and back on, the blocking of the account is reverted; however, for an attacker to exploit this scenario he would need to have physical access to the TOE, which is covered by OE.TRUSTED_NETWORK_SYSTEMS

Application Note 2: Administrator configurable positive integer is set to 7 by default (internal company policy).

6.3.2 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow the establishment of the trusted path (as defined in FTP_TRP.1) on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.3.3 FIA_UAU.7 Protected Authentication Feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only obscured feedback to the user while the authentication is in progress.

Application Note: "Obscured feedback" implies the TSF does not produce a visible display of any authentication data entered by a user (such as the echoing of a password), although an obscured indication of progress may be provided (such as an asterisk for each character). It also implies that the TSF does not return any information during the authentication process to the user that may provide any indication of the authentication data.

6.3.4 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow the establishment of the trusted path (as defined in FTP_TRP.1) on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.3.5 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

1. User ID
2. User level
3. SHA256 hash of password

6.4 **Trusted path/channels**

6.4.1 FTP_TRP.1 Trusted Path

Hierarchical to: No other components

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification,disclosure* .

FTP_TRP.1.2 The TSF shall permit *remote users* to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *initial user authentication through the ISAPI interface , and all subsequent operations performed on those interfaces after the user has been authenticated*.

Application Note: The TLS version used in trusted path/channels is only 1.2 and 1.3 , the used cipher suites:

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_AES_256_GCM_SHA384(TLS1.3)
TLS_AES_128_GCM_SHA256(TLS1.3)

Other cipher suites are available, but these are outside the evaluated configuration.

6.4.2 FTP_ITC .1 Inter -TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *another trusted IT product* [3] to initiate communication via the trusted channel.

[3] The subject to initiate communication is the **RTP/RTSP client**

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for syslog exporting.

Application Note: The TLS version used in trusted path/channels is only 1.2 and 1.3, the used cipher suites are:

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384(TLS1.3)
TLS_AES_128_GCM_SHA256(TLS1.3)

Other cipher suites are available, but these are outside the evaluated configuration.

6.5 **Security audit**

6.5.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate audit data of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the *not specified* level of audit;
c) Failed user authentication attempts;
Login/logout of users;
Creation/deletion of users and configuration of access permissions;
Initiation of firmware update operations
Generating/import of, changing or deleting of cryptographic keys
Discontinuous changes to system time
Establishment and termination of trusted path
The termination of a remote session by the session locking mechanism

FAU_GEN.1.2 The TSF shall record within the audit data at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, none.

6.5.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.5.3 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide the Administrator with the capability to read all the auditable events as defined in FAU_GEN.1 from the audit data.

FAU_SAR.1.2 The TSF shall provide the audit data in a manner suitable for the user to interpret the information.

6.6 **Time stamps(FPT_STM)**

6.6.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note: For selecting the option of transmission of generated audit data to an external IT entity the TOE relies on a non-TOE audit server for storage and review of audit records. The storage of these audit records and the ability to allow the Administrator to review these audit records is provided by the operational environment in that case. Since the external audit server is not part of the TOE, there are no requirements on it except the capabilities for ITC transport for audit data. No requirements are placed upon the format or underlying protocol of the audit data being transferred. The TOE must be capable of being configured to transfer audit data to an external IT entity without Administrator intervention. Manual transfer would not meet the requirements. Transmission could be done in real-time or periodically. If the transmission is not done in real-time then the TSS describes what event stimulates the transmission to be made and what range of frequencies the TOE supports for making transfers of audit data to the audit server; the TSS also suggests typical acceptable frequencies for the transfer.

6.6.2 FPT_TST.1 TSF self-testing

Hierarchical to: No other components.
Dependencies: No dependencies

FPT_TST.1.1 The TSF shall run a suite of the following self-tests *during initial start-up* to demonstrate the correct operation of *TSF.*

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *none*.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of *none*.

Application note: The self-tests consist of U-boot verification, kernel image verification and app verification.

6.7 **Limited TOE Access**

6.7.1 FTA_MCS.1 Basic limitation on multiple concurrent sessions

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of 50 sessions in total.

Application note: The limit can be configured by the administrator at max of 128. The limit of sessions is the limit of connections to the TOE for any type of user. This upper limit can only be with the web client through HTTPS protocol.

6.7.2 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FTA_SSL.3.1 The TSF shall terminate an interactive session after an administrator configurable time interval (1-60 minutes) of session inactivity.

Application Note: Administrator configurable positive integer is set to 15 by default.

6.7.3 FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's [4]own interactive session.

[4] All type of users

7 Security Assurance Requirements

This Security Target claims conformance to EAL3, augmented with the security assurance components listed in Table 7.

This assurance level was chosen to ensure that:

- The TOE has a moderate level of assurance in enforcing its security functions when instantiated in its intended environment which imposes no restrictions on assumed activity on applicable networks.
- Any remaining security flaws in the TOE that are brought to the notice of the Developer will be remediated.

The requirements are summarised in the following table:

Assurance Class	Component	Component Title
ADV: Development	ADV_TDS.2	Architectural design
	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC_ Life-cycle support	ALC_CMC.3	Authorization controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_TSS.1	TOE summary specification
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
	ATE_DPT.1	Testing: basic design
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

Table 13 Assurance requirements description extended with ALC_FLR

8 TOE Summary Specification

8.1 Security Management

FMT_SMR.2: the TOE supports the user types of Administrators, Operator and User. The Administrator is the only role able to create, delete and modify users.

FMT_SMF.1: the TOE supports the management functions:

- Creation, deletion and modification of Operators and Users. There is only one Administrator user, created by default.
- Configuration of credentials and access permissions of existing Operators and Users.
- Management of the certificate for the HTTPS trusted path.
- Perform firmware update operations.
- Configure the authentication failure parameters
- Configure the maximum number of concurrent sessions that belong to the same user
- Configure the session inactivity time before session termination

FMT_MOF.1: The Administrator is the only user able to perform the management functions supported by the TOE.

FMT_MTD.1: The TOE restricts the ability to manage the TSF data only to the Administrator.

8.2 User Identification and Authentication

FIA_AFL.1: the TSF allows the administrator to configure the authentication failure parameters (3 - 20). When this number is reached, the connecting user is blocked for a period of 30 minutes before being able to attempt any further login. If the TOE is powered off and back on, the blocking of the account is reverted; however, for an attacker to exploit this scenario he would need to have physical access to the TOE, which is assumed not possible.

FIA_UID.1 / FIA_UAU.1: Users must first establish the trusted path with the TOE and then login to the camera before being able to perform any operation.

FIA_UAU.7: during the authentication process, only obscured feedback is provided to the user.

FIA_ATD.1: the TOE maintains the user ID, user level, SHA256 hash of password and temporary blocking time for the connecting account after unsuccessful authentication attempts.

8.3 Trusted path/channels

FTP_TRP.1: this requirement is met by the implementation of the HTTPS protocol for the ISAPI interface. The HTTPS protocol is based on TLS 1.2 and TLS1.3 protocol.

Following table details the supported server ciphers.

TLS version	Cipher Suite supported	RFC
TLS1.2	DHE-RSA-AES256-GCM-SHA384 (DHE 2048 bits)	RFC5288
	DHE-RSA-AES128-GCM-SHA256 (DHE 2048 bits)	RFC5288
TLS1.3	AES_256_GCM_SHA384	RFC5288
	AES_128_GCM_SHA256	RFC5288

Table 14 Supported cipher suites

Following the recommendations of [NIST-SP-800-52r2], the ciphers using RSA key transport are discarded, keeping only those using ephemeral Diffie-Hellman key exchange instead. Therefore, the TOE ciphers in the scope of the evaluated configuration are:

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,

TLS_AES_256_GCM_SHA384(TLS1.3)
TLS_AES_128_GCM_SHA256(TLS1.3)

In summary, the following cryptographic means are employed when using the above ciphers:

Symmetric Cryptography	AES in GCM mode and key sizes 128bits, 256bits
Asymmetric Cryptography	RSA and 2048bits key size
Hashing	SHA-256, SHA-384

FTP_ITC.1: the TSF provides a communication channel based on TLS protocol between the TOE and another trusted IT product. The assured identification and protection of the channel data are provided. The TSF initiates the communication for syslog exporting over TLS protocol protection. While the video streaming client requests the video stream, the TSF provides the video data with RTP/RTSP over TLS protection using the ciphers of the evaluated configuration detailed in the TSS description for FTP_TRP.1.

8.4 **Security Audit**

FAU_GEN.1: the TSF generates audit logs by default and stores them in the flash. The audit logs can also be transmitted to the external audit server on the trust channel. The audit logs cover all the audit events as listed in this SFR, and includes details of date/time, user triggering the event and type of event.

FAU_GEN.2: the TSF associates each auditable event with the identity of the user.

FAU_SAR.1: the TSF allows the Administrator to view the audit logs.

8.5 Protection of the TSF

FPT_STM.1: the camera time settings are configurable by the Administrator and is used to provide reliable timestamps.

FCS_CKM.1/AES: the AES key used for protecting the keys above in flash memory is generated when the TOE is reset and first set up.

FCS_COP.1/SHA: the TSF stores the passwords in non-plaintext form and prevents the reading of plaintext passwords. The TSF stores the password using a SHA256 hash of the password according to [FIPS PUB 180-4] standard.

FPT_TST.1: the TSF runs self-tests during initial start-up to demonstrate the correct operation of the TSF.

8.6 TOE Access

FTA_MCS.1: the TSF limits the default number of user connections to 50. The TSF allows the administrator to configure the maximum number to 128.

FTA_SSL.3: The TSF session is terminated after inactive time administrator configured and need reauthentication.

FTA_SSL.4: the TSF allows manual logout of users on all interfaces.

8.7 Cryptographic Operation

FCS_COP.1/RSA: The TOE supports RSA 2048 bit signature generation and verification during TLS session establishment.

FCS_COP.1/SHA: The TOE provides SHA-256, SHA-384 and SHA-512 for TLS channel

FCS_COP.1/AESGCM: All pre-shared keys, symmetric keys and private keys are AES encrypted.

FCS_CKM.1.1/RSA: The TOE generates 2048-bit public and private key-pair for asymmetric RSA cryptography

FCS_CKM.1.1/AESTLS: The TOE generates MAC keys and symmetric keys according to RFC5246.

FCS_CKM.6: The TOE’s OpenSSL cryptographic module stores cryptographic keys and keying material in the TOE’s RAM during cryptographic operations. When these cryptographic keys and keying material are no longer needed, the OpenSSL cryptographic module destroys them by overwriting the corresponding RAM addresses with zeroes. The TOE shall subsequently deallocate the memory location.

FCS_RBG.1 and FCS_RBG.3: The random number generator is implemented through CTR_DRBG(AES).

9 Rationales

9.1 Security Objectives Rationale

This rationale consists of four parts:

- A table mapping all the threats and assumptions against security objectives
- A rationale that the security objectives uphold all assumptions
- A rationale that the security objectives enforce all OSPs
- A rationale that the security objectives counter all threats

9.1.1 Threats, Assumptions and OSPs to Security Objectives Mapping

Threats and assumptions Objectives	A.TRUSTED_USERS	A.TRUSTED_NETWORK_SYSTEMS	A.NO_PHYSICAL_ACCESS	P.FIRMWARE_RELEASE	P.KEY_SECRECY	P.PASSWORDS	T.UNAUTHORISED_ACCESS	T.TRANSMISSION_DISCLOSURE	T.VIDEO_MANIPULATION	T.CAMERA_UNAVAILABLE	T.UPDATE_COMPROMISE
O.USER_AUTHENTICATION							X				
O.USER_AUTHORISATION							X				
O.USER_MANAGEMENT							X				
O.AUDIT_LOGS							X			X	X
O.AUDIT_VIEW							X				
O.AUDIT_EXPORT								X			
O.VIDEO_INTEGRITY									X		
O.TRUSTED_PATH							X	X			
O.VIDEO_PROTECTION								X			
O.SOFTWARE_VERIFIED				X							
O.KEY_SECRECY					X						
OE.TRUSTED_USERS	X										
OE.TRUSTED_NETWORK_SYSTEMS		X									
OE.TOE_AVAILABILITY		X								X	
OE.NO_PHYSICAL_ACCESS			X								
OE.PASSWORDS						X					

Table 15 Threats and Assumptions to Security Objectives Mapping

9.1.2 Assumptions to security objectives rationale

Assumption	Rationale
A.TRUSTED_USERS	**OE.TRUSTED_USERS** makes sure that TOE users are trustworthy and will not act in a manner harmful to the TOE and the administrator of the TOE will correctly configure and install the TOE in its operational environment by following the provided guidance documentation.

Assumption	Rationale
A.TRUSTED_NETWORK_SYSTEMS	**OE.TRUSTED_NETWORK_SYSTEMS** ensures the operational environment prevents the attacker from performing a man-in-the-middle attack within the local network. **OE.TOE_AVAILABILITY** ensures that the operational environment protects the TOE against internal attacks aiming to disrupt the availability of the TOE.
A.NO_PHYSICAL_ACCESS	**OE.NO_PHYSICAL_ACCESS** ensures that attackers don't have access to the following TOE environment components since the following TOE environment components belong to internal network: • A management computer with a web browser • A network video recorder (NVR) client/platform • A syslog server

Table 16 Assumptions to security objectives rationale

9.1.3 Threats to security objectives rationale

Threat	Rationale
T.UNAUTHORISED_ACCESS	**O.USER_AUTHENTICATION** mitigates the threat requiring that all users have a mechanism to authenticate to the TOE to get access to the management interface. Each user has its own account and password. Therefore, impersonation is impossible. **O.USER_AUTHORISATION** requires the TOE to allow different operations depending on the role assigned to the user being authenticated. In addition, **O.USER_MANAGEMENT** assigns to the administrator the privileges of adding and removing users as well as the configuration of their privileges. **O. AUDIT_LOGS** contributes to the mitigation of the threat by generating and audit record for each user access event. **O.AUDIT_REVIEW** contributes to the mitigation of the threat by only allowing the administrator to review and edit audit data. **O.TRUSTED_PATH** mitigates the operation replay by using unique operation ID for each operation implemented in TLS protocol.
T.TRANSMISSION_DISCLOSURE	**O.TRUSTED_PATH** mitigates this threat by requiring a trusted path before performing any management action in order to protect users credentials. **O.VIDEO_PROTECTION** mitigates this threat by providing the confidentiality protection of the video data. **O.AUDIT_EXPORT** contributes to the mitigation of the threat by establishing a secure link for external audit trail storage.
T.VIDEO_MANIPULATION	**O.VIDEO_INTEGRITY** mitigates this threat by implementing an integrity protection mechanism of the video data transmitted.
T.CAMERA_UNAVAILABLE	**OE.TOE_AVAILABILITY** mitigates this threat ensuring that the operational environment protects the TOE against internal attacks aiming to disrupt the availability of the TOE. In addition, **O.AUDIT_LOGS** also contributes to the mitigation of the threat by generating and audit records each time the video data is unavailable.
T.UPDATE_COMPROMISE	**O.AUDIT_LOGS** also contributes to the mitigation of the threat by generating and audit record each time there is a firmware loading attempt either successful or unsuccessful.

Table 17 Threats to security objectives rationale

9.1.4 OSPs to security objectives rationale

OSP	Rationale
P.FIRMWARE_RELEASE	**O.SOFTWARE_VERIFIED** makes sure that self-tests are run by the TSF in order to detect corruption of software.
P.KEY_SECRECY	**O.KEY_SECRECY** ensures that symmetric keys are kept confidential and prevents users to read such keys.
P.PASSWORDS	**OE.PASSWORDS** ensures that the operational environment checks that passwords of a minimum complexity are used.

Table 18 OSPs to security objectives rationale

9.2 Security Requirements Rationale

This rationale shows that all security objectives for the TOE are upheld by the security functional requirements.

Objective	Rationale
O.USER_AUTHENTICATION	This objective is met by FIA_AFL.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FIA_ATD.1, FTA_MCS.1, FTA_SSL.3, and FTA_SSL.4 • requiring user authentication and identification before gaining TOE access (FIA_UAU.1, FIA_UID.1) • protecting user credentials via obscured password feedback (FIA_UAU.7) • associating attributes to each user (FIA_ATD.1) • enforcing authentication failure handling (FIA_AFL.1) • limiting multiple concurrent sessions connected to the TOE (FTA_MCS.1), • enforcing termination after defined period of inactivity (FTA_SSL.3), • enabling users to initiate session termination (FTA_SSL.4)
O.USER_AUTHORISATION	This objective is met by FIA_AFL.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FIA_ATD.1, FTA_MCS.1, FTA_SSL.3, and FTA_SSL.4 • requiring user authentication and identification before gaining TOE access (FIA_UAU.1, FIA_UID.1) • protecting user credentials via obscured password feedback (FIA_UAU.7) • associating attributes to each user (FIA_ATD.1) • enforcing authentication failure handling (FIA_AFL.1) • limiting multiple concurrent sessions connected to the TOE (FTA_MCS.1), • enforcing termination after defined period of inactivity (FTA_SSL.3), • enabling users to initiate session termination (FTA_SSL.4)
O.USER_MANAGEMENT	This objective is met by FMT_SMR.2, FMT_SMF.1, FMT_MOF.1 and FMT_MTD.1 • specifies the security management functions that the TOE can perform (FMT_SMF.1) • enforces the restrictions on security roles (FMT_SMR.2) • restricting security management functions to Administrator and Operator roles (FMT_MOF.1). • Core Data Management(FMT_MTD.1)
O.AUDIT_LOGS	This objective is met by FAU_GEN.1, FAU_GEN.2, FPT_STM.1 and FCS_RBG.1. • generating audit log according to the defined conditions (FAU_GEN.1). • associating each log with user identity (FAU_GEN.2) • ensuring a reliable time stamp (FPT_STM.1) • Random bit generation (FCS_RBG.1)
O.AUDIT_VIEW	This objective is met by FAU_GEN.1, FAU_GEN.2, FMT_SMR.2 and FAU_SAR.1. • generating audit log according to the defined conditions (FAU_GEN.1). • associating each log with user identity (FAU_GEN.2) • allowing authorized TOE users to review audit logs (FAU_SAR.1)
O.AUDIT_EXPORT	This objective is met by FTP_ITC.1

Objective	Rationale
	• ensures by providing a communication channel between TSF and another trusted IT product that is logically distinct from other communication channels and provides assured identification of TSF end points and protection of the channel data from modification or disclosure. (FTP_ITC .1)
O.VIDEO_INTEGRITY	This objective is met by FTP_ITC.1. • ensures by providing a communication channel between TSF and another trusted IT product that is logically distinct from other communication channels and provides assured identification of TSF end points and protection of the channel data from modification or disclosure. (FTP_ITC .1)
O.TRUSTED_PATH	This objective is met by FTP_TRP.1 • provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification, disclosure* (FTP_TRP.1)
O.VIDEO_PROTECTION	This objective is met by FTP_ITC.1 • ensures by providing a communication channel between TSF and another trusted IT product that is logically distinct from other communication channels and provides assured identification of TSF end points and protection of the channel data from modification or disclosure.
O.SOFTWARE_VERIFIED	This objective is met by FPT_TST.1 • conducting self-test to verify the correctness of TSF (FPT_TST.1)
O.KEY_SECRECY	This objective is met by FPT_SKP.1

Table 19 SFR to security objectives rationale

9.3 Dependency Rationale

This rationale shows that all dependencies of all security requirements have been addressed:

Requirement	Dependency	Rationale
FMT_SMR.2	FIA_UID.1 Timing of identification	Met by FIA_UID.1
FMT_SMF.1	No dependencies	n/a
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Met by FMT_SMR.2 since it is hierarchical to FMT_SMR.1 FMT_SMF.1
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Met by FMT_SMR.2 since it is hierarchical to FMT_SMR.1 FMT_SMF.1
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Met by FIA_UAU.1
FIA_UAU.1	FIA_UID.1 Timing of identification	Met by FIA_UID.1
FIA_UAU.7	FIA_UAU.1 Timing of authentication	Met by FIA_UAU.1
FIA_UID.1	No dependencies	n/a
FIA_ATD.1	No dependencies	n/a
FTP_TRP.1	No dependencies	n/a
FTP_ITC.1	No dependencies	n/a
FAU_GEN.1	FPT_STM.1 Reliable time stamps	Met by FPT_STM.1
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	Met by FAU_GEN.1 and FIA_UID.1
FAU_SAR.1	FAU_GEN.1 Audit data generation	Met by FAU_GEN.1

FPT_STM.1	No dependencies	n/a
FPT_TST.1	No dependencies	n/a
FTA_MCS.1	FIA_UID.1 Timing of identification	Met by FIA_UID.1
FTA_SSL.3	FMT_SMR.1 Security roles	Met by FMT_SMR.2 since it is hierarchical to FMT_SMR.1
FTA_SSL.4	No dependencies	n/a
FCS_COP.1	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	Met by FCS_CKM.1 TOE does not support any key access method. Therefore, FCS_CKM.3 is not included in the ST.
FCS_CKM.6	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Met by FCS_CKM.1
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction]	Met by FCS_COP.1 TOE does not support any key access method. Therefore, FCS_CKM.3 is not included in the ST. FCS_CKM.6 FCS_RBG.1
FCS_RBG.1	[FCS_RBG.2 Random bit generation (external seeding), or FCS_RBG.3 Random bit generation (internal seeding – single source)] FPT_FLS.1 Failure with preservation of secure state FPT_TST.1 TSF self-testing	FCS_RBG.3 There is no secure state in case of any failure. Therefore, FPT_FLS.1 is not included in the ST. FPT_TST.1
FCS_RBG.3	FCS_RBG.1 Random bit generation (RBG)	FCS_RBG.1

Table 20 SFR dependencies rationale

10 Abbreviations and glossary

CC	Common Criteria
CIFS	Common Internet File System
DDNS	Dynamic DNS
DNS	Domain Name server
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
IP	Internet Protocol
IPC	IP Camera
ISAPI	IP Surveillance Application Programming Interface
LAN	Local Area Network
NFS	Network File System
NTP	Network Time Protocol
NVR	Network Video Recorder
OS	Operating System
PPPoE	Point-to-Point Protocol over Ethernet
SDK	Software Development Kit
SNMP	Simple Network Management Protocol
ST	Security Target
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
UPNP	Universal Plug and Play
U-boot	Universal Boot Loader

11 References

[1] Common Criteria for Information Technology Security Evaluation.

Part 1: Introduction to General Model, CC:2022, Revision 1, November 2022.

[2] Common Criteria for Information Technology Security Evaluation.

Part 2: Security functional components, CC:2022, Revision 1, November 2022.

[3] Common Criteria for Information Technology Security Evaluation.

Part 3: Security assurance components, CC:2022, Revision 1, November 2022.

[4] Common Criteria for Information Technology Security Evaluation.

Part 4: Framework for the specification of evaluation methods and activities, CC:2022, Revision 1, November 2022.

[5] Common Criteria for Information Technology Security Evaluation.

Part 5: Pre-defined packages of security requirements, CC:2022, Revision 1, November 2022.

[6] Common Methodology for Information Technology Security Evaluation. Evaluation methodology, November 2022, CEM:2022 Revision 1

[FIPS PUB 180-4] Secure Hash Standard (SHS)

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[FIPS PUB 186-4] Digital Signature Standard (DSS),

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[NIST-SP-800-52r2] Guidelines for the Selection, Configuration, and Use of TLS Implementations, NIST SP 800-52Rev.2, August 2019

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

[AGD] Hikvision Network Camera Series Security Guidance Version 1.2

[User Manual] UD38502B_Network Camera_User Manual_H11 V5.9.14

[Errata] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1) Version: 1.1