



Hikvision Network Camera Series
iDS-2CD7

Security Target
Version 2.1

Document history

Version	Date	Comment	Author
1.0	2022-04-18	First Release	ZhuZhenyu
2.1	2022-11-23	Second Release with minor update	ZhuZhenyu

Contents

1	Security Target Introduction.....	6
1.1	Security Target Reference	6
1.2	TOE Reference	6
1.3	TOE Overview.....	6
1.3.1	TOE Type.....	6
1.3.2	TOE Usage and Major Security Features.....	7
1.3.3	Required Non-TOE Hardware/Software/Firmware	8
1.4	TOE Description.....	9
1.4.1	Physical Scope	9
1.4.1.1	List of TOE models	9
1.4.2	Logical Scope	10
1.4.2.1	Security Management	10
1.4.2.2	User Identification and Authentication	10
1.4.2.3	Trusted path/channel	10
1.4.2.4	Security Audit	10
1.4.2.5	Protection of the TSF	10
1.4.2.6	Limited TOE Access	10
1.4.2.7	Trusted Firmware Updates	11
1.4.2.8	Excluded functionality	11
2	Conformance claims.....	12
2.1	CC Conformance Claim	12
2.2	Package Claim	12
2.3	Conformance Rationale	12
3	Security Problem Definition.....	13
3.1	Assumptions.....	13
3.2	Threats	13
3.3	Organisational Security Policies	14
4	Security Objectives.....	15
4.1	Security Objectives for the TOE.....	15
4.2	Security Objectives for the Operational Environment.....	15

5	Extended Component Definition	16
6	Security Functional Requirements	17
6.1	Cryptographic Operation	17
6.1.1	FCS_COP.1 Cryptographic operation	17
6.1.2	FCS_CKM.4 Cryptographic key destruction	17
6.1.3	FCS_CKM.1 Cryptographic key generation.....	18
6.2	Security Management	18
6.2.1	FMT_SMR.2 Restrictions on security roles	18
6.2.2	FMT_SMF.1 Specification of Management Functions.....	18
6.2.3	FMT_MOF.1 Management of security functions behaviour.....	19
6.2.4	FMT_MTD.1 Core Data Management	19
6.3	User Identification and Authentication	19
6.3.1	FIA_AFL.1 Authentication failure handling	19
6.3.2	FIA_UAU.1 Timing of authentication	20
6.3.3	FIA_UAU.7 Protected Authentication Feedback.....	20
6.3.4	FIA_UID.1 Timing of identification	20
6.3.5	FIA_ATD.1 User attribute definition	21
6.4	Trusted path/channels	21
6.4.1	FTP_TRP.1 Trusted path.....	21
6.4.2	FTP_ITC.1 Inter-TSF trusted channel	22
6.5	Security audit	22
6.5.1	FAU_GEN.1 Audit data generation.....	22
6.5.2	FAU_GEN.2 User identity association.....	23
6.5.3	FAU_SAR.1 Audit review	23
6.5.4	FPT_STM.1 Reliable time stamps	23
6.5.5	FPT_TST.1 TSF testing	24
6.6	FTA_MCS.1 Limited TOE Access.....	24
6.6.1	FTA_MCS.1 Basic limitation on multiple concurrent sessions	24
6.6.2	FTA_SSL.3 TSF-initiated termination	25
6.6.3	FTA_SSL.4 User-initiated termination	25
7	Security Assurance Requirements	26

8	TOE Summary Specification	27
8.1	Security Management	27
8.2	User Identification and Authentication	27
8.3	Trusted path/channels	28
8.4	Security Audit	29
8.5	Protection of the TSF	29
8.6	TOE Access	29
8.7	Trusted Firmware and Key Update	30
9	Rationales	31
9.1	Security Objectives Rationale	31
9.1.1	Threats, Assumptions and OSPs to Security Objectives Mapping.....	31
9.1.2	Assumptions to security objectives rationale	31
9.1.3	Threats to security objectives rationale	32
9.1.4	OSPs to security objectives rationale	32
9.2	Security Requirements Rationale	32
9.3	Dependency Rationale.....	33
10	Abbreviations and glossary	35
11	References	36

1 Security Target Introduction

1.1 Security Target Reference

ST Title	Hikvision Network Camera Series iDS-2CD7x Security Target
ST Version	See Document History
ST Date	See Document History
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	1.0
TOE Components	The TOE is Hikvision Network Camera series consisting of the network camera models, firmware, OS and the guidance. The name of the camera models, the version of firmware and OS are listed in <i>Table 4</i> The version of user guidance is listed in <i>Table 5</i> .
Developer	Hikvision
TOE Type	Network Camera

Table 2 TOE reference

1.3 TOE Overview

1.3.1 TOE Type

The Target of Evaluation (TOE) is a Network Camera 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 three series of Network cameras : iDS-2CD7 series . The following list details the models in scope for each family:

iDS-2CD7 series:

- iDS-2CD7046G0-AP
- iDS-2CD7086G0-AP
- iDS-2CD7046G0/E-IHSY
- iDS-2CD7086G0/E-IHSY
- iDS-2CD7146G0-IZS
- iDS-2CD7186G0-IZS
- iDS-2CD7146G0-IZHSY

- iDS-2CD7186G0-IZHSY
- iDS-2CD7546G0-IZHS
- iDS-2CD7546G0-IZHSY
- iDS-2CD7586G0-IZHS
- iDS-2CD7586G0-IZHSY
- iDS-2CD7A46G0-IZHS
- iDS-2CD7A46G0-IZHSY
- iDS-2CD7A86G0-IZHS
- iDS-2CD7A86G0-IZHSY

1.3.2 TOE Usage and Major Security Features

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

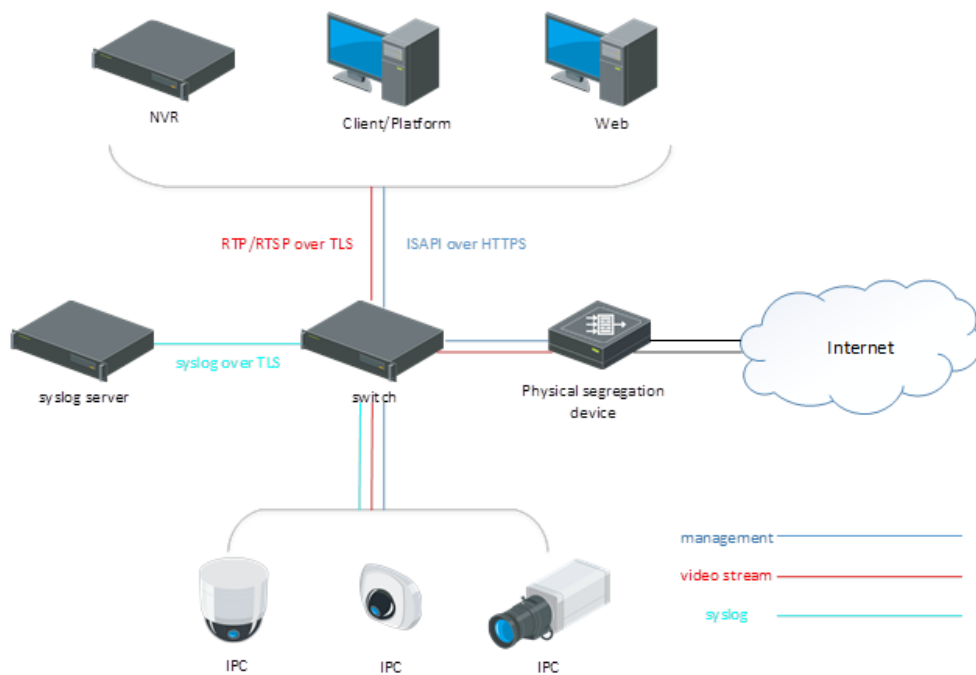


Figure 1 TOE usage scenario.

Note that neither the management nor the video stream are accessible from the internet. The “Physical segregation 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:

- 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.

- Video data distribution to a network recording device or to a web browser and a client/platform using the following the RTP/RTSP protocol over TLS.
- Exporting audit logs to a trusted syslog server through syslog protocol over TLS.

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
- Trusted firmware updates

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

1.4 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:

Series	Models ¹	Version of Firmware/Software ²	Interfaces
iDS-2CD7	iDS-2CD7046G0-AP	Firmware: v5.7.73 build 221111 Web: v4.0.1.0 build 211109 Encoding: v7.3 build 220325 Plugin: 3.0.7.45 (The 5 series) Binary file: IPCG_H8_EN_NEU_5.7.73_20402.zip Interfaces	DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7086G0-AP		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7046G0/E-IHSY		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7086G0/E-IHSY		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7146G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7186G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7146G0-IZHSY		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7186G0-IZHSY		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7546G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7546G0-IZHSY		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7586G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7586G0-IZHSY		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7A46G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7A46G0-IZHSY		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7A86G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
iDS-2CD7A86G0-IZHSY	DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out		

Table 4 TOE series and models¹

Type	Name	SHA256 value	Version
Security Guidance	Hikvision Network Camera Series Security Guidance	21F92278E1CD0CEFCB906056CF62EC45B C52EB2B3CEB6A8222AE96EC519173A8	Version 1.0
User Manual	Hikvision Network Camera User Manual	A980EC19EEE473BB075DC100BB1FB12F5 AAAB0942041FAF1AE59399B1227A72C	UD14456B
ISAPI specification	Hikvision Intelligent Security API (General Application) Developer guide	775C3E2420FF3440333775F131929E429BF 73D66BD53980BF919F58372ADAF71	Version 2.7
ISAPI additional	Hikvision Intelligent Security API (Additional)	7EB6B3C5FB29B00543E20C36FDF9AB4D5 64B0C746569064864FAA0150005702B	Version 2.7

¹ 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_H8_EN_NEU_5.7.73_220402.zip is used on any model of the 7 series.

Table 5 Guidance documentation

The delivery of the TOE hardware (the camera itself) to customers is performed through a courier company. The firmware is shipped together with the TOE hardware. The new camera firmware can be downloaded from Hikvision's web site.

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 users. 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 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 provides reliable time stamps.

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

The TOE prevents reading of all secure 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 Trusted Firmware Updates

The trusted firmware update functionality is implemented and enforced using signature verification of the signed firmware.

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_PRE].
HTTP	
RS-232/RS-485	
External Devices	
IPv6	
DDNS	
PPPoE	
NAT	
SNMP (v1, v2 and v3)	
FTP	
E-mail	
Platform access	
Wireless Dial	
Self-signed certificates	
QoS	
802.1X	
Integration Protocol	
Websocket	
SDK	
TLS1.1	

Table 6 Disabled services and functionality

2 Conformance claims

2.1 CC Conformance Claim

The TOE and ST claim conformance to the CC Version 3.1 revision 5 [2] [3].

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 EAL2 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.

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 guidance documentation. It is assumed that the users of the TOE will not carry out any malicious action trying to compromise the availability of 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 TOE will not be physically accessible.

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	A hacker may try to gain access to TOE functionality without having the required permission. This threat includes: <ul style="list-style-type: none"> • 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.
T.TRANSMISSION_DISCLOSURE	A hacker may be able to obtain credentials of valid TOE users during the 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.

Threat	Definition
T.VIDEO_MANIPULATION	<p>A hacker 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:</p> <ul style="list-style-type: none"> • 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. <p>Successful attacks may allow attackers to manipulate the video image without being detected by the system.</p>
T.UPDATE_COMPROMISE	<p>A hacker 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.</p>

Table 9 Threats

3.3 Organisational Security Policies

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

OSP	Definition
P.SOFTWARE_VERIFIED	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.KEY_SECRETACY	To prevent disclosure of symmetric keys, procedures will exist to keep such keys confidential.
P.PASSWORDS	<p>The password policy should be compliant by the following password policy:</p> <ol style="list-style-type: none"> 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 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.FIRMWARE_LOAD_INTEGRITY	The firmware image during firmware loading is verified by the TOE in terms of integrity and authenticity, to ensure that only valid firmware updates are accepted.
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	The administrator of the TOE is a trusted individual which will correctly configure and install the TOE in its operational environment by following the guidance documentation. The users of the TOE are trusted individuals that will not perform any malicious action trying to compromise the availability of the TOE.
OE.TRUSTED_NETWORK_SYSTEMS	The operational environment shall prevent the hacker from connecting any malicious devices into the local network of the TOE.
OE.NO_PHYSICAL_ACCESS	The operational environment shall protect the TOE preventing its physical access.
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 19.

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]
FCS_CKM.4 Cryptographic key destruction

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

FCS_COP.1.1/A ESGCM 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/S HA 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/R SA 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 180-4.

6.1.2 *FCS_CKM.4 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.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method zeroization and free memory that meets the following: NIST SP 800-88.

6.1.3 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1
Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/R SA 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 180-4.

FCS_CKM.1.1/A ES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm random number generation and specified cryptographic key sizes 128-bits and 256-bits that meet the following: none

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

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 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.2 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.2 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to manage the TSF data 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

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 are:

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384 (ECDH256) TLS1.3
TLS_AES_128_GCM_SHA256 (ECDH256) 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*² to initiate communication via the trusted channel.
- 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 (ECDH 256)
TLS_AES_128_GCM_SHA256 (ECDH256)

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 an audit record 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; and
- c) Failed user authentication attempts;
- d) Login/logout of users;
- e) Creation/deletion of users and configuration of access permissions;
- f) Initiation of firmware update operations.
- g) Generating/import of, changing or deleting of cryptographic keys
- h) Discontinuous changes to system time

² The subject to initiate communication is the ~~RTP/RTSP client~~

- i) Establishment and termination of trusted path
- j) The termination of a remote session by the session locking mechanism

FAU_GEN.1.2 The TSF shall record within each audit record 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/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 records.

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

6.5.4 *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.

6.5.5 *FPT_TST.1 TSF testing*

Hierarchical to: No other components.

Dependencies: No other components.

- | | |
|-------------|---|
| FPT_TST.1.1 | The TSF shall run a suite of self-tests <u>during initial start-up</u> to demonstrate the correct operation of <i>TSF</i> . |
| FPT_TST.1.2 | The TSF shall provide authorised users with the capability to verify the integrity of <i>none</i> . |
| FPT_TST.1.3 | The TSF shall provide authorised users with the capability to verify the integrity of <i>none</i> . |

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

6.6 **FTA_MCS.1 Limited TOE Access**

6.6.1 *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 <u>50</u> 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.

6.6.2 *FTA_SSL.3 TSF-initiated termination*

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after an administrator-configurable time interval of session inactivity.

6.6.3 *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 own interactive session.

7 Security Assurance Requirements

This Security Target claims conformance to EAL2, 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.1	Basic design
	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Functional specification
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC_ Life-cycle support	ALC_CMC.2	CM capabilities
	ALC_CMS.2	CM scope
	ALC_DEL.1	Delivery
	ALC_FLR.2	Flaw reporting procedures
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.1	Coverage
	ATE_FUN.1	Functional tests
	ATE_IND.2	Independent testing
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: Administrator, 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 and deletion 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 (as defined in FMT_SMF.1).

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 protocol.

FCS_CKM.1/RSA: the TOE will generate a self-signed RSA2048 certificate for initial secure communication with the TOE after a reset of the TOE.

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-AES256-SHA256 (DHE 2048 bits)	RFC5246
	DHE-RSA-AES256-SHA (DHE 2048 bits)	RFC3268
	AES256-GCM-SHA384	RFC5288
	AES256-SHA256	RFC5246
	AES256-SHA	RFC5246
	DHE-RSA-AES128-GCM-SHA256 (DHE 2048 bits)	RFC5288
	DHE-RSA-AES128-SHA256 (DHE 2048 bits)	RFC5246
	DHE-RSA-AES128-SHA (DHE 2048 bits)	RFC3268
	AES128-GCM-SHA256	RFC5288
	AES128-SHA256	RFC3268
	AES128-SHA	RFC3268

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. AES key is generated from the DH key exchange (FCS_CKM.1/AESTLS) and all keys will be deleted after use (FCS_CKM.4). 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 (ECDH256) (TLS1.3)
 TLS_AES_128_GCM_SHA256 (ECDH256) (TLS1.3)

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

Symmetric Cryptography FCS_COP.1/AESCBC, FCS_COP.1/AESGCM: AES in CBC, GCM mode and key sizes 128bits, 256bits

Asymmetric Cryptography FCS_COP.1/RSA: RSA and 2048bits key size

Hashing FCS_COP.1/SHA: 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, the Operators and Users 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_COP.1/AESCBC: All pre-shared keys, symmetric keys and private keys are AES encrypted.

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 re-authentication.

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

8.7 Trusted Firmware and Key Update

FCS_COP.1/RSA, FCS_COP.1/SHA: The firmware image with RSA public key is validated through signature verification using RSA 2048 with SHA-512 according to [FIPS PUB 186-4] standard.

FMT_SMF.1: The TSF allows the Administrator user to initiate firmware update operation.

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

Objectives \ Threats and assumptions	A.TRUSTED_USERS	A.TRUSTED_NETWORK_SYSTEMS	A.NO_PHYSICAL_ACCESS	P.SOFTWARE_VERIFIED	P.KEY_SECRETY	P.PASSWORDS	T.UNAUTHORISED_ACCESS	T.TRANSMISSION_DISCLOSURE	T.VIDEO_MANIPULATION	T.UPDATE_COMPROMISE
O.USER_AUTHENTICATION							X			
O.USER_AUTHORISATION							X			
O.USER_MANAGEMENT							X			
O.AUDIT_LOGS							X			X
O.AUDIT_VIEW							X			
O.AUDIT_EXPORT								X		
O.VIDEO_INTEGRITY									X	
O.FIRMWARE_LOAD_INTEGRITY										X
O.TRUSTED_PATH							X	X		
O.VIDEO_PROTECTION								X		
O.SOFTWARE_VERIFIED				X						
O.KEY_SECRETY					X					
OE.TRUSTED_USERS	X									
OE.TRUSTED_NETWORK_SYSTEMS		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 the users with access to the TOE are trusted and that the administrator will correctly configure and install the TOE in its operational environment by following the guidance documentation. The user of the TOE will not perform any malicious action trying to compromise the availability of the TOE.

Assumption	Rationale
A.TRUSTED_NETWORK_SYSTEMS	OE.TRUSTED_NETWORK_SYSTEMS ensures the operation environment prevents attackers connecting any malicious devices into the local network of the TOE.
A.NO_PHYSICAL_ACCESS	OE.NO_PHYSICAL_ACCESS ensures that attackers will by no means have physical access to the TOE.

Table 16 Assumptions to security objectives rationale

9.1.3 Threats to security objectives rationale

Threat	Rationale
T.UNAUTHORISED_ACCESS	<p>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, the impersonation is impossible.</p> <p>O.USER_AUTHORISATION requires the TOE to allow different operations depending on the role assigned to the user being authenticated.</p> <p>In addition, O.USER_MANAGEMENT assigns to the administrator the privileges of adding and removing users as well as the configuration of their privileges.</p> <p>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.</p> <p>O.TRUSTED_PATH mitigates the operation replay by using unique operation ID for each operation implemented in TLS protocol.</p>
T.TRANSMISSION_DISCLOSURE	<p>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.</p> <p>O.AUDIT_EXPORT contributes to the mitigation of the threat by establishing a secure link for external audit trail storage.</p>
T.VIDEO_MANIPULATION	O.VIDEO_INTEGRITY mitigates this threat by implementing an integrity protection mechanisms of the video data transmitted.
T.UPDATE_COMPROMISE	O.FIRMWARE_LOAD_INTEGRITY mitigates this threat making sure that the TOE verifies the signature of the loaded firmware before installing it. 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.SOFTWARE_VERIFIED	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, FTA_SSL.4 and FCS_COP.1/SHA
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, FTA_SSL.4 and FCS_COP.1/SHA

Objective	Rationale
O.USER_MANAGEMENT	This objective is met by FMT_SMR.2, FMT_SMF.1, FMT_MOF.1 and FMT_MTD.1
O.AUDIT_LOGS	This objective is met by FAU_GEN.1, FAU_GEN.2 and FPT_STM.1.
O.AUDIT_VIEW	This objective is met by FAU_GEN.1, FAU_GEN.2, FMT_SMR.2 and FAU_SAR.1 and FCS_COP.1/SHA.
O.AUDIT_EXPORT	This objective is met by FTP_ITC.1, FCS_COP.1/RSA, FCS_COP.1/SHA, FCS_COP.1/AESCBC, FCS_COP.1/AESGCM, FCS_CKM.1/AESTLS, FCS_CKM.1/RSA, FCS_CKM.4
O.VIDEO_INTEGRITY	This objective is met by FTP_ITC.1, FCS_COP.1/RSA, FCS_COP.1/SHA, FCS_COP.1/AESCBC, FCS_COP.1/AESGCM, FCS_CKM.1/AESTLS, FCS_CKM.1/RSA, FCS_CKM.4
O.FIRMWARE_LOAD_INTEGRITY	This objective is met by FCS_COP.1/RSA, FCS_COP.1/SHA, FCS_CKM.4
O.TRUSTED_PATH	This objective is met by FTP_TRP.1, FCS_COP.1/RSA, FCS_COP.1/SHA, FCS_COP.1/AESCBC, FCS_COP.1/AESGCM, FCS_CKM.1/AESTLS, FCS_CKM.1/RSA, FCS_CKM.4
O.VIDEO_PROTECTION	This objective is met by FTP_ITC.1, FCS_COP.1/RSA, FCS_COP.1/SHA, FCS_COP.1/AESCBC, FCS_COP.1/AESGCM, FCS_CKM.1/AESTLS, FCS_CKM.1/RSA, FCS_CKM.
O.SOFTWARE_VERIFIED	This objective is met by FPT_TST.1
O.KEY_SECRETY	This objective is met by FCS_COP.1/AESCBC and FCS_CKM.1/AES, FCS_CKM/4

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	Met by FIA_UID.1
FMT_SMF.1	None	n/a
FMT_MOF.1	FMT_SMR.2 and FMT_SMF.1	Met by FMT_SMR.2 and FMT_SMF.1
FMT_MTD.1	FMT_SMR.2 and FMT_SMF.1	Met by FMT_SMR.2 and FMT_SMF.1
FIA_AFL.1	FIA_UAU.1	Met by FIA_UAU.1
FIA_UAU.1	FIA_UID.1	Met by FIA_UID.1
FIA_UAU.7	FIA_UAU.1	Met by FIA_UAU.1
FIA_UID.1	None	n/a
FIA_ATD.1	None	n/a
FTP_TRP.1	None	n/a
FTP_ITC.1	None	n/a
FAU_GEN.1	FPT_STM.1	Met by FPT_STM.1
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	Met by FAU_GEN.1 and FIA_UID.1
FAU_SAR.1	FAU_GEN.1	Met by FAU_GEN.1
FPT_STM.1	None	n/a
FPT_TST.1	None	n/a
FTA_MCS.1	FIA_UID.1	Met by FIA_UID.1
FTA_SSL.3	None	n/a
FTA_SSL.4	None.	n/a
FCS_COP.1/AESCBC	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1 and FCS_CKM.4	Met by FCS_CKM.4 and FCS_CKM.1/AESTLS or FCS_CKM.1/AES

FCS_COP.1/AESGCM	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1 and FCS_CKM.4	Met by FCS_CKM.4 and FCS_CKM.1/AESTLS
FCS_COP.1/RSA	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1 and FCS_CKM.4	Met by FCS_CKM.4 and FCS_CKM.1/RSA
FCS_COP.1/SHA	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1 and FCS_CKM.4	NA
FCS_CKM.4	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1	Met by FCS_CKM.1.1/RSA or FCS_CKM.1.1/AES or FCS_CKM.1.1/AESTLS
FCS_CKM.1.1/RSA	FCS_CKM.2, or FCS_COP.1 and FCS_CKM.4 Cryptographic key destruction	Met by FCS_COP.1/RSA and FCS_CKM.4
FCS_CKM.1.1/AES	FCS_CKM.2, or FCS_COP.1 and FCS_CKM.4 Cryptographic key destruction	Met by FCS_COP.1/AES and FCS_CKM.4
FCS_CKM.1.1/AESTLS	FCS_CKM.2, or FCS_COP.1 and FCS_CKM.4 Cryptographic key destruction	Met by FCS_COP.1/AESTLS and FCS_CKM.4

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
HikSSL	Hikvision cryptographic library.
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, Version 3.1, Revision 5, April 2017.
- [2] Common Criteria for Information Technology Security Evaluation.
Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- [3] Common Criteria for Information Technology Security Evaluation.
Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
- [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>