Hikvision Network Camera Series

Security Target

Version 3.0

Document history

Version	Date	Comment	Author
0.5	2018-02-07	First draft	FGOM, XCAS
0.6	2018-02-08	Added out of the scope services Update according to Hikvision's comments Management functions added	XCAS
1.0	2018-03-13	First release	FGOM, XCAS
1.1	2018-04-05	Addressed the evaluator EORs	FGOM
1.2	2018-04-10	SDK removed ISAPI added	XCAS
2.0	2018-07-16	Updated guidance documentation versions Updated TOE firmware/software versions	FGOM
3.0	2018-08-02	Updated Guidance version and models features	Hikvision

Distribution list

- Hikvision
- SERTIT
- Brightsight

Contents

1 Security Target Introduction

1.1 Security Target Reference

ST Title	Hikvision Network Camera Series
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*
TOE Version	The TOE version is composed of the camera model, firmware version and firmware release date. Refer to Table 4 TOE series and models for details.
TOE Identification	The TOE unique identifier is composed of the camera model, firmware version and firmware release date. Refer to Table 4 TOE series and models for details.
TOE Type	Network Camera

Table 2 TOE reference

* The TOE name encompass all the camera models as listed in Table 4.

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.

The TOE provides the following functionality:

- Management interface.
- Video over IP.

The TOE consists of two series of Network cameras: DS-2CD3 and DS-2CD5. The following list details the models in scope for each family:

- **DS-2CD3 series:** DS-2CD3025G0-I, DS-2CD3125G0-IS, DS-2CD3325G0-I, DS-2CD3T25G0-I, DS-2CD3525G0-IS, DS-2CD3625G0-IZS, DS-2CD3725G0-IZS, DS-2CD3H25G0-IZS, DS-2CD3045G0-I, DS-2CD3145G0-IS, DS-2CD3345G0-I, DS-2CD3T45G0-I, DS-2CD3545G0-IS, DS-2CD3645G0-IZS, DS-2CD3745G0-IZS, DS-2CD3H45G0-IZS, DS-2CD3085G0-I, DS-2CD3185G0-IS, DS-2CD3385G0-I, DS-2CD3T85G0-I, DS-2CD3685G0-IZS, DS-2CD3785G0-IZS, DS-2CD3H85G0-IZS.
- **DS-2CD5 series:** DS-2CD5026G0-AP, DS-2CD5046G0-AP, DS-2CD5085G0-AP, DS-2CD5126G0-IZS, DS-2CD5146G0-IZS, DS-2CD5185G0-IZS, DS-2CD5A26G0-IZHS, DS-2CD5A46G0-IZHS, DS-2CD5A85G0-IZHS, DS-2CD5526G0-IZHS, DS-2CD5546G0-IZHS, DS-2CD5585G0-IZHS.

1.3.2 TOE Usage and Major Security Features

The environment consists of a LAN network which is totally isolated from other networks (e.g. other LANs or Internet). The TOE network may contain the following components: one or multiple TOEs, video recording devices (such as NVR) and management computers via ISAPI. Figure 1 illustrates the environment where the TOE is intended to be used:

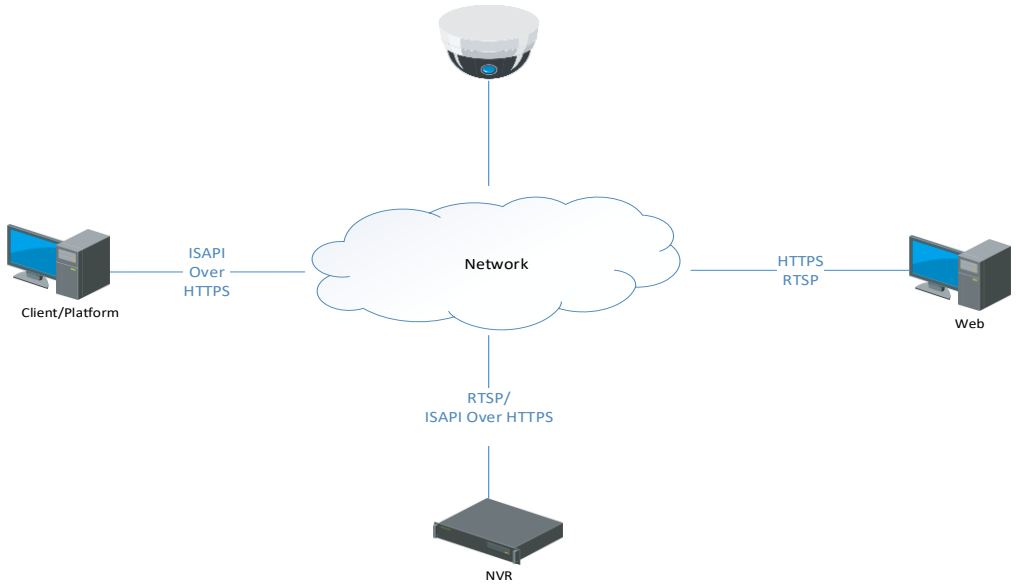


Figure 1 TOE usage scenario.

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 is an HTTP-based application programming interface that enables the TOE to communicate with IP media devices. Web application and client/platform programs must implement this API.
- Video data distribution to a network recording device or to a web browser using the following the RTSP protocol.

The TOE provides the following major security features:

- Security management.
- User identification and authentication.
- Trusted path.
- Audit logs.
- Protection of the TSF.
- Cryptographic support.
- TOE access.
- Trusted firmware updates.

The TOE does not provide confidentiality protection of the video data when distributing it to external entities through the TOE network.

The TOE also provide 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 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) and management devices via ISAPI over HTTPS.

Component	Required	Scope	Description
Management computer with a web browser	Mandatory	No	General purpose computer that is used to manage the TOE using a web interface implementing ISAPI over HTTPS and to receive video data through the RTSP protocol.
Network Video Recorder (NVR)	Optional	No	Physical device used to record and store video. The video is received via RTSP protocol.
Client/Platform	Optional	No	General purpose computer which implements a software solution to record and store video from the TOE and/or manage the same TOE through ISAPI over HTTPS.

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 consists of 2 different product series, each series containing different hardware models integrating the same firmware/software versions for the whole series. The full list of models is provided below:

Series	Models	Firmware/Software	Interfaces
DS-2CD3	DS-2CD3025G0-I	Firmware V5.5.60 build 180514 Web version V4.0.51 build 180425 Encoding version V7.3 build 180510 Plugin version V3.0.6.43	DC12V, SD, RJ45
	DS-2CD3125G0-IS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3325G0-I		DC12V, SD, RJ45
	DS-2CD3T25G0-I		DC12V, SD, RJ45
	DS-2CD3525G0-IS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3625G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3725G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3H25G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3045G0-I		DC12V, SD, RJ45
	DS-2CD3145G0-IS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3345G0-I		DC12V, SD, RJ45
	DS-2CD3T45G0-I		DC12V, SD, RJ45
	DS-2CD3545G0-IS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3645G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3745G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out

	DS-2CD3H45G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3085G0-I		DC12V, SD, RJ45
	DS-2CD3185G0-IS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3385G0-I		DC12V, SD, RJ45
	DS-2CD3T85G0-I		DC12V, SD, RJ45
	DS-2CD3685G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3785G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3H85G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
DS-2CD5	DS-2CD5026G0-AP	Firmware V5.5.60 build 180514 Web version V4.0.1 build 180502 Encoding version V7.3 build 180510 Plugin version V3.0.6.38	DC12V, SD, RJ45, RS485, audio 1in 1out, alarm 2in 2out
	DS-2CD5046G0-AP		DC12V, SD, RJ45, RS485, audio 1in 1out, alarm 2in 2out
	DS-2CD5085G0-AP		DC12V, SD, RJ45, RS485, audio 1in 1out, alarm 2in 2out
	DS-2CD5126G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD5146G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD5185G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD5A26G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 2in 2out
	DS-2CD5A46G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 2in 2out
	DS-2CD5A85G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 2in 2out
	DS-2CD5526G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD5546G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD5585G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out

Table 4 TOE series and models

Type	Name	Version
Security Guidance	Hikvision Network Camera Series Security Guidance	Version 0.7
User Manual	Hikvision Network Camera User Manual	UD09650B
ISAPI specification	Hikvision IP Surveillance API, Image Service Specification	v2.1 rev 1
	Hikvision IP Surveillance API, PTZ Service Specification	v2.2 rev 1
	Hikvision IP Surveillance API, (RaCM Part) User Guide	v2.0 rev 1
	Hikvision IP Surveillance API User Guide	v2.2 rev 1

Table 5 Guidance documentation

The delivery of the TOE hardware (the camera itself) to customers is performed through a courier company. The camera firmware and user guidance is available to the TOE users through Hikvision's web site.

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. 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 7 (for the Administrator) or 5 (for the Operator and User) consecutive unsuccessful attempts, the TOE blocks the IP address from which the user is trying to connect.

1.4.2.3 Trusted path/channel

A trusted path implemented with HTTPS communication shall be established before accessing the TOE management functionality.

1.4.2.4 Audit Logs

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.

1.4.2.5 Protection of the TSF

The TOE provides reliable time stamps.

1.4.2.6 Cryptographic Support

The TOE provides cryptographic support for specific functionality:

- HTTPS secure communications to access the management functionality of the TOE.
- RTSP protocol authentication.
- RSA signature verification to verify the firmware.
- Video integrity watermarking.

1.4.2.7 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 a method to terminate an open session by an action of the user.

1.4.2.8 Trusted Firmware Updates

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

1.4.2.9 Excluded functionality

Following functionality is not included within the scope of the evaluation and shall therefore be disabled.

Services	**Rationale**
NTP	Services and functionalities are disabled in the evaluated configuration.
HTTP	
RS-232/RS-485	
DDNS	
PPPoE	
UPnP	
SNMP (v1, v2 and v3)	
FTP	
E-mail	
Platform access	

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 claim conformance to CC Part 2 extended and CC Part 3 conformant.

2.2 Package Claim

The Security Target claims conformance to assurance package EAL2 augmented by ALC_FLR.2.

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

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.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's 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	The administrator of the TOE is a trusted individual which must correctly configure and install the TOE in its operational environment by following the guidance documentation. The users of the TOE are considered trusted individuals which will not carry out any malicious action trying to compromise the availability of the TOE.
A.TRUSTED_NETWORK_SYSTEMS	Attackers have no chance to connect any malicious devices into the local network of the TOE.

Table 7 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	Threat agents 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.
T.TRANSMISSION_DISCLOSURE	Threat agents may be able to obtain credential 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.
T.VIDEO_MANIPULATION	Threat agents 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.

Threat	Definition
T.CAMERA_UNAVAILABLE	Threat agents may try to subvert the availability of the TOE An inadequate protection against Denial of Service (DOS) attacks or a badly chosen physical protection may allow an attacker to force the interruption of the video data transmission.
T.UPDATE_COMPROMISE	Threat agents 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 alteration.

Table 8 Threats

3.3 Organisational Security Policies

There are no Organizational Security Policies identified for this TOE.

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.
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.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 before accessing the management functionality

Table 9 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	Attackers have no chance to connect any malicious devices into the local network of the TOE.
OE.TOE_AVAILABILITY	The operational environment shall protect the TOE against internal attacks trying to disrupt the availability.

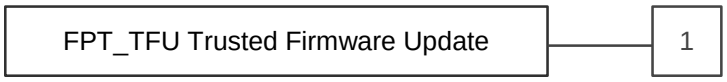
Table 10 Objectives for the operational environment

5 Extended Component Definition

5.1 Definition of the family FPT_TFU

Family Behaviour
Components in this family address the requirements for the verification of the integrity and authenticity of the TOE firmware before updating.

Component levelling



Management: FPT_TFU.1
There are no management activities foreseen.

Audit: FPT_TFU.1
There are no actions defined to be auditable.

FPT_TFU.1 Trusted Firmware Updates.

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation

FPT_TFU.1.1 The TSF shall provide [assignment: authorised users] the ability to query the currently executing version of the TOE firmware.

FPT_TFU.1.2 The TSF shall provide [assignment: authorised users] the ability to manually initiate updates to the TOE firmware and [selection: support automatic checking for updates, support automatic updates, no other update mechanism].

FPT_TFU.1.3 The TSF shall provide means to authenticate firmware updates to the TOE using a [assignment: digital signature mechanism, published hash, other mechanisms] prior to accepting and installing those updates.

FPT_TFU.1.4 The TSF shall provide means to verify the integrity of firmware images to the TOE using a [assignment: hashing algorithm, other mechanisms] prior to accepting and installing those updates.

6 Security Functional Requirements

Notes:

- Selections and assignments have been underlined.
- Various refinements have been made in the requirements (**in bold**).
- Iterations have been indicated by adding a "/ITERATION" to the SFR and by adding a part to the requirement name (in brackets).

6.1 Security Management

6.1.1 FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles Administrator, Operator and User.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.2 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.

6.1.3 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 User Identification and Authentication

6.2.1 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 7 (for the Administrator role) or 5 (for the Operator and User roles) 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 connecting IP address for 30 minutes.

Application note: the interfaces include only the ISAPI interface implementing the protocols HTTPS and RTSP. If the TOE is powered off and back on, the blocking of the IP address 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.

6.2.2 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet the following:

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.

6.2.3 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.

6.2.4 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 **Trusted path/channels**

6.3.1 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.

6.4 **Audit Logs**

6.4.1 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.

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.

6.4.2 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, Operator and User roles 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 Protection of the TSF

6.5.1 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.

6.5.2 FDP_DAU.1 Basic Data Authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of the video data.

FDP_DAU.1.2 The TSF shall provide **external entities accessing the video data** with the ability to verify evidence of the validity of the indicated information.

Refinement: there are no defined subjects on the TOE which can verify the validity evidence, therefore the [assignment: *list of subjects*] operation of FDP_DAU.1.2 has been refined to replace "subjects" with "external entities" to correctly define which entities can perform this operation.

Application note: the validity evidence of the video data is provided through the "watermarking" feature of the TOE. The watermarking data is provided together with the video data when video is requested and sent to an external entity, and it's generated with AES using the video data and other camera data such as model, serial number, time and date.

6.6 Cryptographic support

6.6.1 AES Data Encryption/Decryption

6.6.1.1 FCS_COP.1/AES Cryptographic operation (AES Data Encryption/Decryption)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1/AES Cryptographic key generation
FCS_CKM.4/AES Cryptographic key destruction

FCS_COP.1.1/AES The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES in CBC mode and cryptographic key sizes 128 and 256 bits that meet the following: [FIPS197].

6.6.1.2 FCS_CKM.1/AES Cryptographic key generation

Hierarchical to: No other components.

Dependencies: FCS_CKM.4/AES Cryptographic key destruction

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

6.6.1.3 FCS_CKM.1/AES_TLS Cryptographic key generation (for TLS)

Hierarchical to: No other components.

Dependencies: FCS_CKM.4/AES Cryptographic key destruction

FCS_CKM.1.1/AES_TLS The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm TLS protocol and specified cryptographic key sizes 128 and 256 bits that meet the following: [RFC5246].

6.6.1.4 FCS_CKM.4/AES Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: FCS_CKM.1/AES Cryptographic key generation

FCS_CKM.4.1/AES The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key value with zeros that meets the following: none.

6.6.2 Hash Algorithm

6.6.2.1 FCS_COP.1/Hash Cryptographic operation (Hash Algorithm)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1/Hash Cryptographic key generation
FCS_CKM.4/Hash Cryptographic key destruction

FCS_COP.1.1/Hash The TSF shall perform cryptographic hashing in accordance with a specified cryptographic algorithm SHA1, SHA-256, SHA-384, SHA-512, MD5 and cryptographic key sizes none that meet the following: [FIPS 180-4], [RFC1321].

Application note: the dependencies with FCS_CKM.1 and FCS_CKM.4 are not met for Hash operations, as no cryptographic keys are required for this operation (see rationale in 9.3).

6.6.3 Signature Generation and Verification

6.6.3.1 FCS_COP.1/Sign Cryptographic operation (Signature Generation and Verification)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1/Sign Cryptographic key generation
FCS_CKM.4/Sign Cryptographic key destruction

FCS_COP.1.1/Sign The TSF shall perform digital signature generation and verification in accordance with a specified cryptographic algorithm RSA with SHA1, RSA with SHA-256, RSA with SHA-384, RSA with SHA-512 and cryptographic key sizes 1024 and 2048 bits that meet the following: [FIPS PUB 186-4].

6.6.3.2 FCS_CKM.1/Sign Cryptographic key generation

Hierarchical to: No other components.

Dependencies: FCS_CKM.4/Sign Cryptographic key destruction

FCS_CKM.1.1/Sign The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA key generation and specified cryptographic key sizes 1024 and 2048 bits that meet the following: [FIPS PUB 186-4].

6.6.3.3 FCS_CKM.4/Sign Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: FCS_CKM.1/Sign Cryptographic key generation

FCS_CKM.4.1/Sign The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key value with zeros that meets the following: none.

6.6.4 HMAC

6.6.4.1 FCS_COP.1/HMAC Cryptographic operation (Keyed Hash Algorithm)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1/HMAC Cryptographic key generation
FCS_CKM.4/HMAC Cryptographic key destruction

FCS_COP.1.1/HMAC The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-MD5, HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384 and cryptographic key sizes 128 and 256 bits that meet the following: [FIPS 198].

6.6.4.2 FCS_CKM.1/HMAC Cryptographic key generation

Hierarchical to: No other components.

Dependencies: FCS_CKM.4/HMAC Cryptographic key destruction

FCS_CKM.1.1/HMAC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm key derivation function and specified cryptographic key sizes 128 and 256 bits that meet the following: [FIPS 198].

6.6.4.3 FCS_CKM.4/HMAC Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: FCS_CKM.1/HMAC Cryptographic key generation

FCS_CKM.4.1/HMAC The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key value with zeros that meets the following: none.

6.7 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 128 sessions per user.

Application note: the limit of sessions is the limit of connections to the TOE for any type of user. For some of the TOE models this limit is lower.

6.7.2 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.

6.8 Trusted Firmware Updates

6.8.1 FPT_TFU.1 Trusted Firmware Updates.

Hierarchical to: No other components.
Dependencies: FCS_COP.1/Sign Cryptographic operation (Signature Generation and Verification)

FPT_TFU.1.1 The TSF shall provide Administrator the ability to query the currently executing version of the TOE firmware.

FPT_TFU.1.2 The TSF shall provide Administrator the ability to manually initiate updates to the TOE firmware and no other update mechanism.

FPT_TFU.1.3 The TSF shall provide means to authenticate firmware updates to the TOE using a RSA2048 with SHA-512 digital signature mechanism as defined in FCS_COP.1/Sign prior to accepting and installing those updates.

FPT_TFU.1.4 The TSF shall provide means to verify the integrity of firmware images to the TOE using a RSA2048 with SHA-512 digital signature mechanism as defined in FCS_COP.1/Sign prior to accepting and installing those updates.

7 Security Assurance Requirements

This Security Target claims conformance to EAL2, augmented with ALC_FLR.2. 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 11 EAL2 requirements description extended with ALC_FLR

8 TOE Summary Specification

8.1 Security Management

FMT_SMR.1: the TOE supports the user types Administrator, Operator and User.

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.

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).

8.2 User Identification and Authentication

FIA_AFL.1: the TSF allows 7 failed authentication attempts for the Administrator and 5 for the Operators and Users. When this number is reached, the IP address of 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 IP address 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_SOS.1: the TSF enforces that passwords have a length between 8-16 characters and include at least 2 different types of characters between lowercase, uppercase, numbers and special characters.

FIA_UAU.1: users must login into the camera before being able to perform any operation.

FIA_UID.1: users must login into the camera before being able to perform any operation.

8.3 Trusted path/channels

FTP_TRP.1: this requirement is met by the implementation of the HTTPS/TLS protocol for the ISAPI interface and the RTS^P protocol.

8.4 Audit Logs

FAU_GEN.1: the TSF generates audit logs by default and stores them in the SD card. 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_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.

FDP_DAU.1: the TSF provides integrity and validity evidence of the video data through the watermarking feature. The watermarking data is provided together with the video data when video is requested and sent to an external entity, and it's generated with AES using the video data and other camera data such as model, serial number, time and date.

8.6 Cryptographic support

FCS_COP.1: the TSF provides cryptographic services to support the trusted path, user authentication protocols and the video watermarking feature.

FCS_CKM.1: the TSF provides key generation services to support the cryptographic services.

FCS_CKM.4: the TSF provides key destruction services to support the cryptographic services.

8.7 TOE Access

FTA_MCS.1: the TSF limits the maximum number of user connections to 128.

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

8.8 Trusted Firmware Updates

FPT_TFU.1: the TSF allows the Administrator user to initiate firmware update operations. The firmware image is validated through RSA signature verification.

9 Rationales

9.1 Security Objectives Rationale

This rationale consists of three 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 counter all threats

9.1.1 Threats and Assumptions to Security Objectives Mapping

Objectives \ Threats and assumptions	A.TRUSTED_USERS	A.TRUSTED_NETWORK_SYSTEMS	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.TRUSTED_PATH				X			
O.VIDEO_INTEGRITY					X		
O.FIRMWARE_LOAD_INTEGRITY							X
OE.TRUSTED_USERS	X						
OE.TRUSTED_NETWORK_SYSTEMS		X					
OE.TOE_AVAILABILITY						X	

Table 12 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.
A.TRUSTED_NETWORK_SYSTEMS	**OE.TRUSTED_NETWORK_SYSTEMS** addresses the assumption that attackers have no chance to connect any malicious devices into the local network of the TOE.

Table 13 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. This objective is completed with **O.USER_AUTHORISATION** which 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.
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.
T.VIDEO_MANIPULATION	**O.VIDEO_INTEGRITY** mitigates this threat by implementing an integrity protection mechanisms 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 record each time the video data is unavailable.
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 14 Threats 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_SOS.1, FIA_UAU.1, FIA_UID.1, FTA_MCS.1 and FTA_SSL.4.
O.USER_AUTHORISATION	This objective is met by FIA_AFL.1, FIA_SOS.1, FIA_UAU.1, FIA_UID.1, FTA_MCS.1 and FTA_SSL.4.
O.USER_MANAGEMENT	This objective is met by FMT_SMR.1, FMT_SMF.1 and FMT_MOF.1.
O.AUDIT_LOGS	This objective is met by FAU_GEN.1, FAU_SAR.1 and FPT_STM.1.
O.TRUSTED_PATH	This objective is met by FTP_TRP.1, FCS_COP.1/AES, FCS_CKM.1/AES_TLS, FCS_CKM.1/AES, FCS_CKM.4/AES, FCS_COP.1/Sign, FCS_CKM.1/Sign, FCS_CKM.4/Sign, FCS_COP.1/Hash, FCS_COP.1/HMAC, FCS_CKM.1/HMAC and FCS_CKM.4/HMAC.
O.VIDEO_INTEGRITY	This objective is met by FDP_DAU.1, FCS_COP.1/AES, FCS_CKM.1/AES and FCS_CKM.4/AES.
O.FIRMWARE_LOAD_INTEGRITY	This objective is met by FPT_TFU.1, FCS_COP.1/Sign, FCS_CKM.1/Sign, FCS_CKM.4/Sign and FCS_COP.1/Hash.

Table 15 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.1	FIA_UID.1	Met by FIA_UID.1
FMT_SMF.1	None	n/a
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	Met by FMT_SMR.1 and FMT_SMF.1
FIA_AFL.1	FIA_UAU.1	Met by FIA_UAU.1
FIA_SOS.1	None	n/a
FIA_UAU.1	FIA_UID.1	Met by FIA_UID.1
FIA_UID.1	None	n/a
FTP_TRP.1	None	n/a
FAU_GEN.1	FPT_STM.1	Met by FPT_STM.1
FAU_SAR.1	FAU_GEN.1	Met by FAU_GEN.1
FPT_STM.1	None	n/a
FCS_COP.1/AES	FCS_CKM.1 and FCS_CKM.4	Met by FCS_CKM.1/AES and FCS_CKM.4/AES
FCS_CKM.1/AES	FCS_CKM.4 and FCS_COP.1	Met by FCS_CKM.4/AES and FCS_COP.1/AES
FCS_CKM.1/AES_TLS	FCS_CKM.4 and FCS_COP.1	Met by FCS_CKM.4/AES and FCS_COP.1/AES
FCS_CKM.4/AES	FCS_CKM.1	Met by FCS_CKM.1/AES
FCS_COP.1/Hash	FCS_CKM.1 and FCS_CKM.4	Dependencies with FCS_CKM.1 and FCS_CKM.4 are not met. Hashing operations do not require a cryptographic key, so the creation/destruction operations from FCS_CKM.1 and FCS_CKM.4 are not required.
FCS_COP.1/Sign	FCS_CKM.1 and FCS_CKM.4	Met by FCS_CKM.1/Sign and FCS_CKM.4/Sign
FCS_CKM.1/Sign	FCS_CKM.4 and FCS_COP.1	Met by FCS_CKM.4/Sign and FCS_COP.1/Sign
FCS_CKM.4/Sign	FCS_CKM.1	Met by FCS_CKM.1/Sign
FCS_COP.1/HMAC	FCS_CKM.1 and FCS_CKM.4	Met by FCS_CKM.1/HMAC and FCS_CKM.4/HMAC
FCS_CKM.1/HMAC	FCS_CKM.4 and FCS_COP.1	Met by FCS_CKM.4/HMAC and FCS_COP.1/HMAC
FCS_CKM.4/HMAC	FCS_CKM.1	Met by FCS_CKM.1/HMAC
FTA_MCS.1	FIA_UID.1	Met by FIA_UID.1
FTA_SSL.4	None.	n/a
FDP_DAU.1	None.	n/a
FPT_TFU.1	FCS_COP.1	Met by FCS_COP.1/Sign

Table 16 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
[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
[RTSP]	Real Time Streaming Protocol
[TOE]	Target of Evaluation
[TSF]	TOE Security Functionality
[UPNP]	Universal Plug and Play

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.