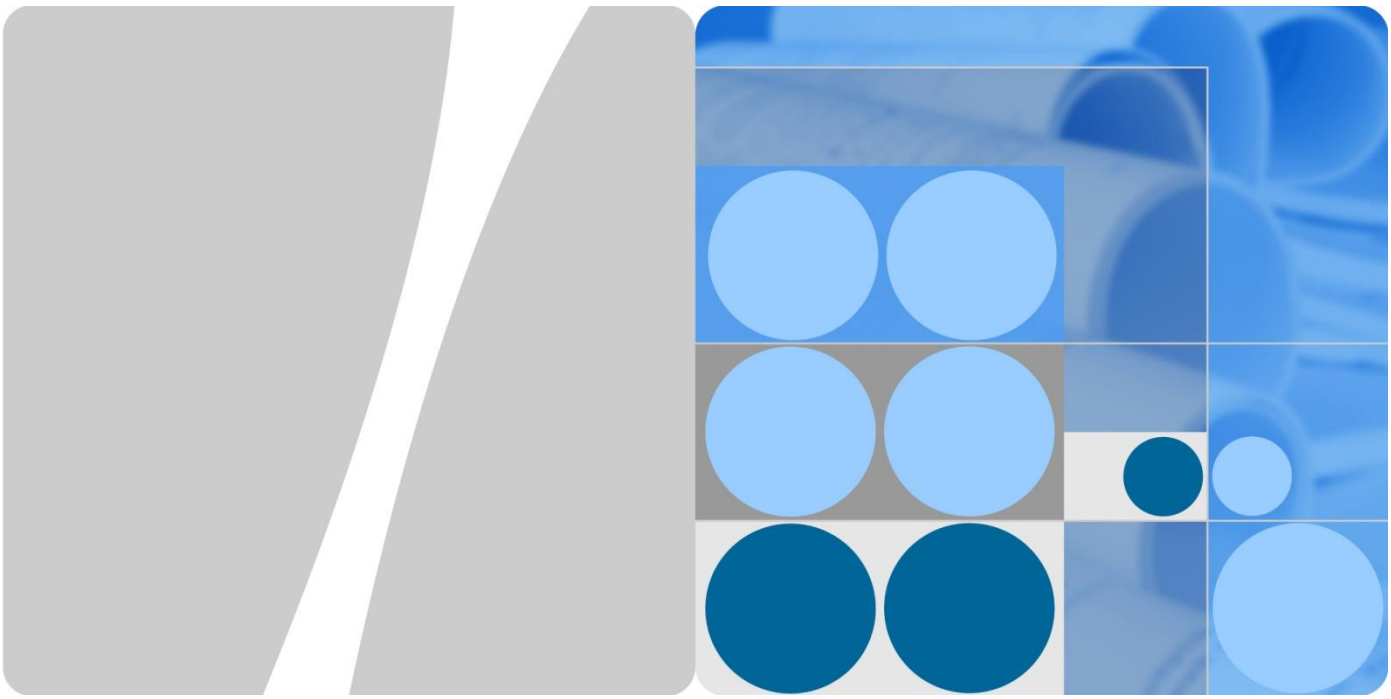


Huawei IP Camera Series products V200R003C20 Security Target

Issue 1.0

Date 2018-03-27

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 ST Introduction 1
1.1 ST Reference 1
1.2 TOE Reference 1
1.3 TOE Overview 1
1.3.1 TOE Type 1
1.3.2 TOE usage & Major Security Features 2
1.3.3 Non TOE Hardware/Software/Firmware 2
1.4 TOE Description 3
1.4.1 TOE Logical Scope 3
1.4.2 TOE Physical Scope 5
2 Conformance Claims 10
3 Security Problem Definition 11
3.1 Threats to Security 11
3.2 Assumptions 12
4 Security Objectives 14
4.1 Security Objectives for the Operational Environment 14
4.2 Security Objectives for the TOE 15
4.3 Security Objectives Rationale 15
4.3.1 Tracing of security objectives to SPD 15
4.3.2 Justification of tracing 16
5 Extended Components Definition 19
6 Security Requirements 20
6.1 Security Functional Requirements 20
6.1.1 SECURITY AUDIT (FAU) 20
6.1.2 CRYPTOGRAPHIC SUPPORT (FCS) 21
6.1.3 IDENTIFICATION AND AUTHENTICATION (FIA) 23
6.1.4 SECURITY MANAGEMENT (FMT) 23
6.1.5 PROTECTION OF THE TSF (FPT) 24
6.1.6 TOE ACCESS (FTA) 24
6.1.7 TRUSTED PATH/CHANNELS (FTP) 24
6.2 Security Assurance Requirements 24

6.3 Security Requirements Rationale 26
6.3.1 SFR Necessity and Sufficiency Analysis 26
6.3.2 SFR Dependency Analysis 29
6.3.3 SAR Rationale 32
6.3.4 SAR Dependency Analysis 32
7 TOE Summary Specification 34
8 Acronyms 38
9 Glossary of Terms 39
10 Document References 40

Figures

Figure 1-1 TOE Deployment Diagram 2

Tables

Table 1-1 IT Environment Components 3
Table 1-2 Excluded Functionality 4
Table 1-3 Physical Specifications 5
Table 3-1 Information Assets 11
Table 3-2 Threats 11
Table 3-3 Assumptions 12
Table 4-1 Security Objectives for the Operational Environment 14
Table 4-2 Security Objectives for the TOE 15
Table 4-3 Tracing of security objectives to SPD 16
Table 4-4 Threat Rationale 17
Table 4-5 Assumption Rationale 17
Table 6-1 Auditable Events 20
Table 6-2 Security Assurance Requirements 25
Table 6-3 Tracing of security SFR to Security Ojectives 26
Table 6-4 Justification of tracing 28
Table 6-5 SFR Missing dependencies justification 29
Table 6-6 SAR Missing dependencies justification 32
Table 7-1 Justification of tracing 34
Table 8-1 Acronyms 38
Table 9-1 Glossary of Terms 39
Table 10-1 Document References 40

1 ST Introduction

1.1 ST Reference

Title Huawei IP Camera Series products running V200R003C20 version Security Target

Version 1.0

Author Huawei Technologies Co., Ltd.

Date of publication 2018-03-27

1.2 TOE Reference

TOE Name Huawei IP Camera Series products

TOE Version V200R003C20

TOE Developer Huawei Technologies Co., Ltd.

1.3 TOE Overview

1.3.1 TOE Type

The TOE is an IP Camera system composed of a hardware platform and a firmware running within the platform as a whole system. This TOE provides video over IP networks with some security features such as Security Audit, Cryptographic support, Identification and Authentication, Security Management, Protection of the TSF, TOE access, Trusted Path. We provide 8 IP Cameras include IPC6125-WDL-FA, IPC6225-VRZ, IPC6285- VRZ, IPC6325-WD-VRZ, IPC6385-VRZ, IPC6525-Z30, IPC6625-Z30, IPC6681-Z20 (more details in 1.4.2),Some can be used in indoors, such as IPC6125-WDL-FA, IPC6325-WD-VRZ. Some can be used in outdoors, such as IPC6225-VRZ, IPC6285- VRZ, IPC6681-Z20.

.

1.3.2 TOE usage & Major Security Features

A network camera, often known as an IP camera, is used to send video over an IP network such as a local area network (LAN) or the Internet. A network camera enables live viewing and/or recording, either continuously, at scheduled times, on request or when triggered by an event. there are two usage scenarios regarding the video distribution:

1.The video data distribution is only accessed using the web interface .

2.The video data is sent and stored in a server using a different interface than https used for the web access.

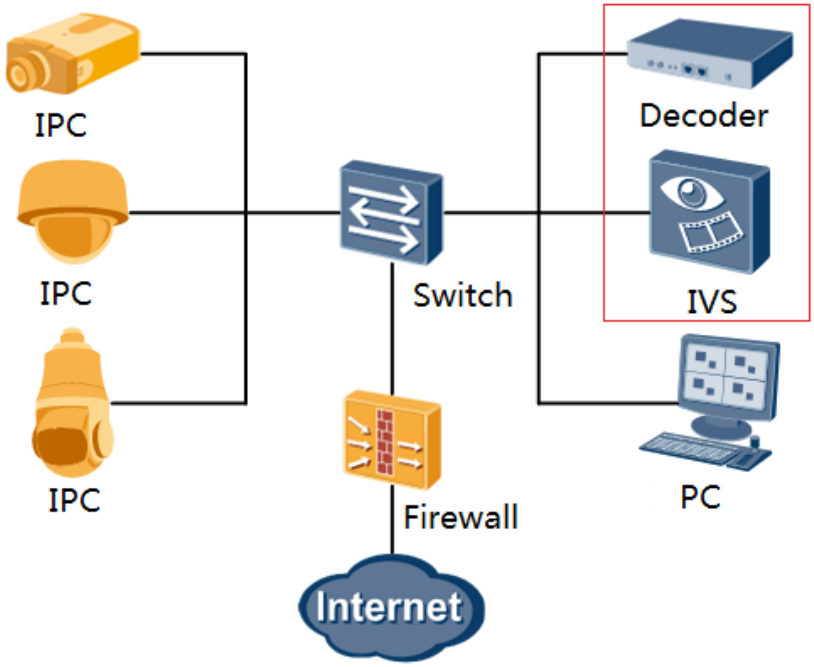
This certification is only about the first scenarios.

The major security features include: Security Audit, Cryptographic support, Identification and Authentication, Security Management, Protection of the TSF, TOE access, Trusted Path.

1.3.3 Non TOE Hardware/Software/Firmware

The Figure 1-1 shows a sample TOE deployment, and the logical interconnections to/from TOE components.

Figure 1-1 TOE Deployment Diagram



The figure above shows a sample TOE deployment, and the logical interconnections to/from TOE components. This certification does not include decoder and IVS

This environment includes one network which is separated from external networks (e.g. other LANs or Internet) by a Firewall/Gateway/Physical segregation device. In the TOE network there are only the following components: IP cameras, one (or a very limited number of) computer for cameras management and the video recording equipment (e.g. IVS and decoders). Furthermore the TOE network shall be setup so connection of any other devices is not possible.

The Firewall/Gateway/Physical segregation blocks all the traffic except for TOE management and video distribution from the specific external equipment intended for such purpose, by using NAT and IP source white list and protect the TOE network from attacks from the outside (e.g. DDOS). A more restrictive firewall configuration is also valid (e.g. complete network isolation).

Table 1-1 IT Environment Components

Component	Required	Usage/purpose Description for TOE performance
PC	Yes	This includes any IT Environment Management workstation with TLS-enabled browser installed that is used by the TOE administrator for remote administration of the TOE. The browser must support HTTPS.
Switch	Yes	Switch means a local area network (LAN)，which composed of one or more swatches.
Firewall/Gateway/Physical segregation	Yes	The Firewall/Gateway/Physical segregation must be deployed to prevent the any attacks if the TOE is used from the Internet.

1.4 TOE Description

1.4.1 TOE Logical Scope

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below:

1. Security Audit
2. Cryptographic support
3. Identification and Authentication
4. Security Management
5. Protection of the TSF
6. TOE access
7. Trusted Path

These features are described in more details in the subsections below.

Security Audit

The TOE generates the audit data and provides authorised users with the capability to read audit information from the audit records.

Cryptographic support

The TOE provides cryptography support for secure communications. The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; digital signature using RSA; Hash Algorithm using SHA-256,SHA-1; and keyed-hash

message authentication using HMAC-SHA-256,HMAC-SHA-1. The TOE also implements HTTPS for secure remote administration, also include video data transfer.

Identification and Authentication

The TOE provides authentication services for administrative users of the TOE who connect remotely by HTTPS. The TOE requires administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length and to enforce mandatory password complexity rules. When the defined number of unsuccessful authentication attempts has been surpassed, the TOE will terminate the session of the user trying to authenticate and block the user account for authentication for default 5 minutes.

Security Management

The TOE provides security management for users of the TOE who can manage the different roles and security functions.

Protection of the TSF

The TOE can be able to provide reliable time stamps.

TOE access

Administrative sessions can be set to terminate after a configurable idle-time limit. The TOE can restrict the maximum number of concurrent sessions that belong to the same user. Once a session has been terminated the TOE requires administrators to re-authenticate to establish a new session. The TOE can allow user-initiated termination of the user's own interactive session.

Trusted Path

Remote administrators or users can establish trusted communication paths to the TOE using HTTPS.

The following Table 1-2 is excluded from the evaluation.

Table 1-2 Excluded Functionality

Excluded Functionality	Exclusion Rationale
SSH	SSH will be disabled in the evaluated configuration.
SNMP	SNMP will be disabled in the evaluated configuration.
SDK	SDK will be disabled in the evaluated configuration.
SOAP	SOAP will be disabled in the evaluated configuration.
T28181	T28181 will be disabled in the evaluated configuration.
Genetec	Genetec will be disabled in the evaluated configuration.

1.4.2 TOE Physical Scope

The TOE is comprised of the following physical specifications as described in Table 1-3 documents below:

AGD_PRE (CC Huawei IP Camera Series products V200R003C20 AGD_PRE V04.doc)

AGD_OPE (CC Huawei IP Camera Series products V200R003C20 AGD_OPE V03.doc.)

IPC V200R003C20 Product Documentation01.

Table 1-3 Physical Specifications

Model	Feature	Interface
IPC6125-WDL-FA  firmware version：V200R003C20	• H.265, H.264 and MJPEG video compression standard • Dual-channel 1080p HD video encoding • Intelligent analytics • Auto Back Focus(-FA) • 1x SFP slot for SFP fiber optic modules(-FA)	• Ethernet: 1x RJ-45 10/100/1000Base-T self-adaptive Ethernet port • SFP slot: 1x SFP slot • Opto-electronic cascade(OEC): Supporting cascade connection of two cameras via opto-electronic Eth ports • Serial: 1x RS-485 port ,supporting PELCO-P/D protocol • Alarm : 1-channel alarm input and 1-channel alarm output • Analog video: 1-channel CVBS output • Audio: 1-channel audio input and 1-channel audio port • Memory card slot: 1x Micro SD/SDHC/SDXC slot • Lens interface: C- or CS-mount interface
IPC6225-VRZ  firmware version：V200R003C20	• H.265, H.264 and MJPEG video compression standard • Invisible IR(-SP) • Built-in motorized zoom and focus lens • Intelligent analytics	• Ethernet: 1x RJ-45 10/100Base-T self-adaptive Ethernet port • Serial: 1x RS-485 port (PELCO-P/D protocol) • Alarm: 2-channel alarm input and 2-channel

Model	Feature	Interface
		alarm output • Analog video: 1-channel CVBS output, BNC connector • Audio： 1-channel audio input and 1-channel audio port ,3.5mm mono connector • Memory card slot：1x MicroSD/SDHC/SDXC slot
IPC6285- VRZ  firmware version：V200R003C20	• Up to 4K(3840×2160) UHD • H.265, H.264 and MJPEG video compression • Wide dynamic range 120dB • Intelligent behavior analytics, color recognition, vehicle and pedestrian classification, exception audio detection • IP67 protection class	• Ethernet: 1x RJ-45 10/100、1000Base-T self-adaptive Ethernet port • Serial: 1x RS-485 port (PELCO-P/D protocol) • Alarm: 2-channel alarm input and 2-channel alarm output • Analog video: 1-channel CVBS output, BNC connector • Audio： 1-channel audio input and 1-channel audio port • Memory card slot：1x MicroSD/SDHC/SDXC slot
IPC6325-WD-VRZ  firmware version：V200R003C20	• H.265, H.264 and MJPEG video compression standard • Wide dynamic range 120dB • 2.8-12 mm Motorized and smart focus • Intelligent analytics • Intelligent IR control(-VRZ) • IP66 protection class • IK10 Vandal-proof class • Railway application standards	• Ethernet interface: 1x RJ-45 10/100Base-T self-adaptive Ethernet port • Serial interface: 1x RS-485 port • Alarm interface: 1-channel alarm input and 1-channel alarm output • Analog video interface: 1-channel CVBS output • Audio interface: 1-channel audio input and 1-channel audio port (3.5mm mono connector) • Memory card slot: 1x MicroSD/SDHC/SDXC

Model	Feature	Interface
		slot.
IPC6385-VRZ  firmware version：V200R003C20	• Up to 4K(3840×2160) UHD • H.265, H.264 and MJPEG video compression • Wide dynamic range 120dB • Intelligent behavior analytics, color recognition, vehicle and pedestrian classification, exception audio detection • IP66 protection class	• Ethernet interface: 1x RJ-45 10/100Base-T self-adaptive Ethernet port • Alarm interface: 1-channel alarm input and 1-channel alarm output • Audio interface: 1-channel audio input and 1-channel audio port (3.5mm mono connector) • The power input interface. supports DC12V±25% and AC24V±24.9% power input.
IPC6525-Z30  firmware version：V200R003C20	• H.265, H.264 and MJPEG video compression standard • Dual-channel 1080p HD video encoding • Ultra WDR 120dB • Auto defogging • Gyroscopic image stabilization • Intelligent analytics • SFP slot for SFP fiber optic modules • Opto-electronic cascade(OEC) • Railway applications	• Ethernet interface:1x RJ-45 10/100/1000Base-T self-adaptive Ethernet port • SFP slot:1x SFP slot for SFP fiber optic modules • Opto-electronic cascade(OEC):Supporting cascade connection of two cameras via opto-electronic Eth ports • Serial interface:1x RS-485 port (PELCO-P/D protocol) • Alarm interface:8-channel alarm input and 2-channel alarm output • Analog video interface:1-channel analog video output through the CVBS interface, BNC connector • Audio interface:1-channel audio input and 1-channel audio port • Memory card slot:1x

Model	Feature	Interface
		MicroSD/SDHC/SDXC slot
IPC6625-Z30  firmware version：V200R003C20	• H.265, H.264 and MJPEG video compression standard • Dual-channel 1080p HD video encoding • Intelligent IR • Ultra WDR 120dB • Highlight suppression • Auto defogging • Gyroscopic image stabilization • Intelligent analytics • IK10 Vandal-proof class • IP66 protection class • Ultra wide operating temperature range -40℃ ~ 60℃	• Ethernet interface:1x RJ-45 10/100Base-T self-adaptive Ethernet port • Serial interface:1x RS-485 port (PELCO-P/D protocol) • Memory card slot:1x MicroSD/SDHC/SDXC slot, up to 64 GB • Alarm interface:8-channel alarm input and 2-channel alarm output • Analog video interface:1-channel analog video output through the CVBS interface, BNC connector
IPC6681-Z20  firmware version：V200R003C20	• Up to 4K(3840×2160) UHD • H.265, H.264 and MJPEG video compression • Wide dynamic range 120dB • Intelligent behavior analytics, color recognition, vehicle and pedestrian classification, exception audio detection • IP66 protection class	• Ethernet interface：1x RJ-45 10/100/1000Base-T self-adaptive Ethernet port • Serial interface：1x RS-485 port (PELCO-P/D protocol) • Alarm interface：4-channel alarm input and 2-channel alarm output • Analog video interface：1-channel analog video output through the CVBS interface,BNC connector • Audio interface：1-channel audio input and 1-channel audio port,RCA connector • Memory card slot：1x MicroSD/SDHC/SDXC slot

2 Conformance Claims

This Security Target and the TOE described are in accordance with the requirements of Common Criteria 3.1R4.

This Security Target claims conformance with the following parts of Common Criteria:

- Conformance with [CC31R4P2].
- Conformance with [CC31R4P3].

The methodology to be used for the evaluation is described in the "Common Evaluation Methodology" of the Common Criteria standard of September 2012, version 3.1 revision 4 with an evaluation assurance level of EAL3 + ALC_FLR.2.

This Security Target does not claim conformance with any protection profile.

3 Security Problem Definition

3.1 Threats to Security

The information assets to be protected are the information stored, processed or generated by the TOE. Configuration data for the TOE, TSF data (such as user account information and passwords, etc.) and other information that the TOE facilitates access to (such as system software, patches) are all considered part of information assets.

Table 3-1 Information Assets

	Confidentiality	Integrity	Availability
Log data	X	X	
Configuration data	X	X	
Video data	X		X
User interaction traffic	X	X	X

This section identifies the threats to assets that require protection by the TOE. The threats are defined in terms of assets concerned, attackers and the adverse action that materializes the threat.

Table 3-2 Threats

Threat	Description
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on

Threat	Description
	which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give the unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.NETWORK_ATTACKS	Threat agents may attempt to attack TOE from internet or external networks with flooding, malformed packages or other means intended to subvert the TOE TSF. Successful attacks will result in loss of availability of the TOE, such as losing of control or device restarting.

3.2 Assumptions

The assumptions when using the TOE are the following:

Table 3-3 Assumptions

Assumption	Description
A.PHYSICAL_PROTECTION	The TOE is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the ST will not include any requirements on physical tamper protection or other physical attack mitigations. The ST will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The TOE is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to

Assumption	Description
	networking functionality).
A.TRUSTED_USERS	The Security Administrator(s) for the TOE are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and to lack malicious intent when administering the device. The TOE is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. All users of the TOE having access to the TOE management computers or the TOE network are trusted in the sense that they will not perform malicious actions intended to subvert the availability of the TOE assets.
A. NETWORK_SEGREGATION	The network environment of TOE (the LAN where the TOE is connected) is assumed to be trusted and to prevent attacks from internet. This environment includes one network which is separated from external networks (e.g. other LANs or Internet). In the TOE network there are only the following components: cameras, one (or a very limited number of) computer for cameras management and the video recording equipment (e.g. IVS and decoders). Connection of any other devices is not possible If access from Internet is necessary, a boundary protection device such as Firewall/Gateway/Physical segregation device is required to prevent attacks from the internet.

4 Security Objectives

4.1 Security Objectives for the Operational Environment

The security objectives for the Operational Environment determine the responsibility of the environment in countering the threats, enforcing upholding the assumptions. Each objective must be traced back to aspects of identified threats to be countered by the environment.

Table 4-1 Security Objectives for the Operational Environment

Security Objective	Description
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.TRUSTED_USERS	Users are trusted to follow and apply all guidance documentation in a trusted manner. Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. All users of the TOE having access to the TOE network are trusted in the sense that they will not perform malicious actions intended to subvert the availability of the TOE assets.
OE.NETWORK_SEGREGATION	The operational environment shall provide segregation from Internet by deploying TOE into a LAN with a firewall or gateway, and it shall restrict the physical access to the TOE network to TOE authorized users..

4.2 Security Objectives for the TOE

The security objectives for the TOE must determine (to the desired extent) the responsibility of the TOE in countering the threats. Each objective must be traced back to aspects of identified threats to be countered by the TOE.

Table 4-2 Security Objectives for the TOE

Security Objective	Description
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data.
O.AUDIT_VIEW	The TOE will provide only the authorized administrators the capability to review audit data, and overwrite the oldest stored audit records if the audit trail is full.
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE shall provide cryptographic functions (i.e.,encryption/decryption and digital signature operations) to maintain the confidentiality.
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators.
O.SESSION_ACCESS	The TOE shall provide mechanisms that can set basic limitation on multiple concurrent sessions and initiated termination.
O.ID_AUTH	The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting management access.
O.SECURITY_MANAGE	The TOE will provide management tools/applications to allow authorized administrators to manage its security functions.
O.ADMIN_ROLE	The TOE will provide administrator levels to isolate administrative actions, and to make the administrative functions available remotely.

4.3 Security Objectives Rationale

4.3.1 Tracing of security objectives to SPD

The following table provides a mapping of security objectives tracing each security objective for the TOE back to threats countered by that security objective enforced by that security objective, and each security objective for the operational environment back to threats countered by that security objective, and assumptions upheld by that security objective. This illustrates that the security objectives counter all threats, the security objectives for the operational environment uphold all assumptions.

Table 4-3 Tracing of security objectives to SPD

	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	**T.WEAK_CRYPTOGRAPHY**	**T.UNTRUSTED_COMMUNICATION_CHANNELS**	**T.UNDETECTED_ACTIVITY**	**T.NETWORK_ATTACKS**	**A.PHYSICAL_PROTECTION**	**A.LIMITED_FUNCTIONALITY**	**A.TRUSTED_USERS**	**A.NETWORK_SEGREGATION**
O.SYSTEM_MONITORING				X					
O.AUDIT_VIEW				X					
O.CRYPTOGRAPHIC_FUNCTIONS		X							
O.PROTECTED_COMMUNICATIONS		X	X						
O.SESSION_ACCESS	X								
O.ID_AUTH	X								
O.SECURITY_MANAGE	X	X	X	X					
O.ADMIN_ROLE	X								
OE.PHYSICAL						X			
OE.NO_GENERAL_PURPOSE							X		
OE.TRUSTED_USERS					X			X	
OE.NETWORK_SEGREGATION					X			X	X

4.3.2 Justification of tracing

The following table maps the threats of the security problem established to the security objectives of the TOE and the security objectives of the operational environment.

Table 4-4 Threat Rationale

Threat	Security Objectives
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	The **O.SESSION_ACCESS** objective requires that the TOE can provide the lock of session. The **O.ID_AUTH** objective requires the users to enter a qnique identifier and authentication before management access is granted. The **O.ADMIN_ROLE** objective ensures that only authorized administrator, with the proper privilege level have access to the TOE management functions. The **O.SECURITY_MANAGE** objective requires that the TOE can manage the above functions.
T.WEAK_CRYPTOGRAPHY	The **O.CRYPTOGRAPHIC_FUNCTIONS** objective requires that the TOE can provide the security cryptographic functions. The **O.PROTECTED_COMMUNICATIONS** objective requires to use the security cryptographic functions. The **O.SECURITY_MANAGE** objective requires that the TOE can manage the cryptographic functions.
T.UNTRUSTED_COMMUNICATION_CHANNELS	The **O.PROTECTED_COMMUNICATIONS** objective requires that the TOE can use the secure protocols for identified communication channels. The **O.SECURITY_MANAGE** objective requires that the TOE can manage the communication channels.
T.UNDETECTED_ACTIVITY	The **O.SYSTEM_MONITORING** objective requires that the TOE can generate audits records. The **O.AUDIT_VIEW** requires the TOE to provide the capability to prevent the unauthorized users from reviewing audit data, and overwrite the oldest stored audit records if the audit trail is full. The **O.SECURITY_MANAGE** objective requires that the TOE can manage the audit functions.
T.NETWORK_ATTACKS	The **OE.TRUSTED_USERS** objective requires that users having access to the TOE network are trusted. The **OE.NETWORK_SEGREGATION** requires protects the TOE network against attacks from external networks and prevents physical access to the TOE network.

The following table maps the assumptions of the problem established to the security objectives of the TOE and the security objectives of the operational environment.

Table 4-5 Assumption Rationale

Assumption	Security Objectives
A.PHYSICAL_PROTECTION	The **OE.PHYSICAL** objective ensures that the TOE should be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation.
A.LIMITED_FUNCTIONALITY	The **OE.NO_GENERAL_PURPOSE** objective ensures that the TOE provides networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing.
A.TRUSTED_USERS	The **OE.TRUSTED_USER** objective ensures that the TOE users should be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and

Assumption	Security Objectives
	adhering to guidance documentation. The **OE.NETWORK_SEGREGATION** objective ensures that access to non-authorized personnel is prevented.
A. NETWORK_SEGREGATION	The **OE.NETWORK_SEGREGATION** objective ensures that any Internet attacks are prevented by LAN which the TOE is connected to, which is also protected against unauthorized access.

5 Extended Components Definition

No extended components have been defined for this ST.

6 Security Requirements

6.1 Security Functional Requirements

6.1.1 SECURITY AUDIT (FAU)

FAU_GEN.1 Audit data generation

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

- Start-up and shutdown of the audit functions;

- All auditable events for the ***[selection, choose one of: not specified]*** level of audit; and

- ***[assignment: Specifically defined auditable events listed in*** Table 6-1***]***

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

- For each audit event type, based on the auditable event definitions of the functional components included in the ~~PP/~~ST, ***[assignment:none]*** .

Table 6-1 Auditable Events

Requirement	Auditable Events
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.
FMT_MOF.1	Configure the management function
FPT_STM.1	Configure the timestamp
FTA_MCS.1	Unsuccessful login attempts limit is met or exceeded.
FTA_SSL.4	The termination of an interactive session.

Requirement	Auditable Events
FTP_TRP.1	1. Initiation of the trusted path. 2. Termination of the trusted path. 3. Failure of the trusted path functions.

FAU_GEN.2 User identity association

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.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide ***[assignment: System administrator and Advanced Operator]*** with the capability to read ***[assignment: all audit information]*** 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.

6.1.2 CRYPTOGRAPHIC SUPPORT (FCS)

FCS_CKM.1/RSA Cryptographic key generation

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

FCS_CKM.1/DATA_AES Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[*[assignment: random number generation*]** and specified cryptographic key sizes [***assignment: 256 bits***] that meet the following: **[*assignment: NONE*].**

Application Note:

The algorithm used to encrypt the video stream is directly uses the random number as the AES256 KEY.

FCS_CKM.1/TLS_AES Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[*[assignment: Key derivation function*]** and specified cryptographic key sizes [***assignment: 128, 256 bits***] that meet the following: **[*assignment: RFC5246*].**

Application Note:

The Key of the AES256 algorithm using in TLS1.2 is generated by Key derivation function of RFC5246.

FCS_CKM.1/ KeyedHash Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[*[assignment: Key derivation function*** and specified

cryptographic key sizes [***assignment: 160, 256 bits***] that meet the following: [***assignment: RFC5246***].

FCS_CKM.4/RSA Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[assignment: full flash erase by overwriting with 0]*** that meets the following:***[assignment: NONE]***.

FCS_CKM.4/DATA_AES Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[assignment: full flash erase by overwriting with 0]*** that meets the following:***[assignment: NONE]***.

FCS_CKM.4/TLS_AES Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[assignment: full flash erase by overwriting with 0]*** that meets the following:***[assignment: NONE]***.

FCS_CKM.4/ KeyedHash Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[assignment: full flash erase by overwriting with 0]*** that meets the following:***[assignment: NONE]***.

FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)

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

FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1 The TSF shall perform ***[assignment: cryptographic signature services (generation and verification)]*** in accordance with a specified cryptographic algorithm ***[assignment: RSA Digital Signature Algorithm]*** and cryptographic key sizes ***[assignment: 2048 bits bits]*** that meet the following:***[assignment: U.S. NIST FIPS PUB 186-4]***.

FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1 The TSF shall perform ***[assignment: cryptographic hashing services]*** in accordance with a specified cryptographic algorithm ***[assignment: SHA-256，SHA1]*** ~~and cryptographic key sizes ***[assignment: : cryptographic key sizes]***~~ ***and message digest sizes [assignment: 256，160]*** that meet the following:***[assignment: FIPS180-4]***.

Application NOTE:SHA256 is only one used in Signature Generation and Verification.

FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1 The TSF shall perform ***[assignment: keyed-hash message authentication]*** in accordance with a specified cryptographic algorithm ***[assignment: HMAC-SHA-1,HMAC-SHA-256]*** and cryptographic key sizes ***[assignment: 160 bits used in HMAC-SHA-1, 256 bits used in HMAC-SHA-256] and message digest sizes [selection: 160,256 bits]*** that meet the following:***[assignment: FIPS198]***.

6.1.3 IDENTIFICATION AND AUTHENTICATION (FIA)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***[selection: an administrator configurable positive integer within [assignment: 5]]*** unsuccessful authentication attempts occur related to ***[assignment: Administrators attempting to authenticate remotely.]***.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***[selection: surpassed], the TSF shall [assignment: terminate the session of the user trying to authenticate and block the user account for authentication for default 5 minutes]***.

* Max. incorrect password inputs shall be at least set to 1.

FIA_ATD.1 User attribute definition

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

1. **user ID**
2. **user level**
3. **SHA256 hashes of passwords**
4. **temporary blocking time for user accounts after unsuccessful authentication attempts**
5. **time when users are logging in and logging off**

].

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4 SECURITY MANAGEMENT (FMT)

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to ***[selection: determine the behaviour of]*** the functions ***[assignment: defined in FMT_SMF.1]*** to ***[assignment: System administrator and Advanced Operator]***.

Application Note

Just the System Administrator has the ability to configure the authentication failure parameters for FIA_AFL.1.

FMT_SMF.1 Specification of Management Functions

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

1. ***Ability to administer the TOE remotely;***
2. ***Ability to configure the maximum number of concurrent sessions that belong to the same user;***

3. ***Ability to configure the authentication failure parameters for FIA_AFL.1;***
4. ***No other capabilities.]***.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles ***[assignment:***

1. ***System Administrator***
2. **Advanced Operator**
3. **Common Operator*]***.

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

6.1.5 PROTECTION OF THE TSF (FPT)

FPT_STM.1 Reliable time stamps

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

6.1.6 TOE ACCESS (FTA)

FTA_MCS.1 Basic limitation on multiple concurrent sessions

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 ***[assignment: 10]*** sessions per user.

FTA_SSL.3 TSF-initiated termination

The TSF shall terminate an interactive session after a ***[assignment: 10 mins]***.

FTA_SSL.4 User-initiated termination

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

6.1.7 TRUSTED PATH/CHANNELS (FTP)

FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***selection: 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 ***[selection: modification, disclosure]***.

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for ***[selection: initial user authentication]***.

6.2 Security Assurance Requirements

ASE_REQ.2.1C: *The statement of security requirements shall describe the SFRs and the SARs.*

ASE_REQ.2.2C: *All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.*

ASE_REQ.2.3C: *The statement of security requirements shall identify all operations on the security requirements.*

ASE_REQ.2.4C: *All operations shall be performed correctly.*

ASE_REQ.2.9C: *The statement of security requirements shall be internally consistent.*

The development and the evaluation of the TOE shall be done in accordance to the following security assurance requirements: **EAL3 + ALC_FLR.2**

The following table shows the assurance requirements by reference the individual components in [CC31R4P3]

Table 6-2 Security Assurance Requirements

Assurance Class	Assurance Components
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
ALC: Life-cycle support	ALC_CMC.3: Authorisation controls ALC_CMS.3: Implementation representation CM coverage ALC_DEL.1: Delivery procedures ALC_DVS.1: Identification of security measures ALC_LCD.1: Developer defined life-cycle model ALC_FLR.2: Flaw reporting procedures
ADV: Development	ADV_ARC.1: Security architecture description ADV_FSP.3: Functional specification with complete summary ADV_TDS.2: Architectural design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance AGD_PRE.1: Preparative procedures
ATE: Tests	ATE_COV.2: Analysis of coverage ATE_DPT.1: Testing: basic design ATE_FUN.1: Functional testing ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

6.3 Security Requirements Rationale

6.3.1 SFR Necessity and Sufficiency Analysis

Table 6-3 Tracing of security SFR to Security Ojectives

	O.SYSTEM_MONITORING	**O.AUDIT_VIEW**	**O.CRYPTOGRAPHIC_FUNCTIONS**	**O.PROTECTED_COMMUNICATIONS**	**O.SESSION_ACCESS**	**O.ID_AUTH**	**O.SECURITY_MANAGE**	**O.ADMIN_ROLE**
FAU_GEN.1	X							
FAU_GEN.2	X							
FAU_SAR.1		X						
FCS_CKM.1/RSA			X					
FCS_CKM.1/DADA_AES			X					
FCS_CKM.1/TLS_AES			X					
FCS_CKM.1/Keyed Hash			X					
FCS_CKM.4/RSA			X					
FCS_CKM.4/DADA_AES			X					
FCS_CKM.4/TLS_AES			X					

	O.SYSTEM_MONITORING	**O.AUDIT_VIEW**	**O.CRYPTOGRAPHIC_FUNCTIONS**	**O.PROTECTED_COMMUNICATIONS**	**O.SESSION_ACCESS**	**O.ID_AUTH**	**O.SECURITY_MANAGE**	**O.ADMIN_ROLE**
FCS_CKM.4/ KeyedHash								
FCS_COP.1/DataEncryption			X					
FCS_COP.1/SigGen			X					
FCS_COP.1/Hash			X					
FCS_COP.1/KeyedHash			X					
FIA_AFL.1						X		
FIA_ATD.1						X		
FIA_UAU.2						X		
FIA_UID.2						X		
FMT_MOF.1							X	
FMT_SMF.1							X	
FMT_SMR.1							X	X
FPT_STM.1	X							
FTA_MCS.1					X			

	O.SYSTEM_MONITORING	O.AUDIT_VIEW	O.CRYPTOGRAPHIC_FUNCTIONS	O.PROTECTED_COMMUNICATIONS	O.SESSION_ACCESS	O.ID_AUTH	O.SECURITY_MANAGE	O.ADMIN_ROLE
FTA_SSL.3					X			
FTA_SSL.4					X			
FTP_TRP.1				X				

Table 6-4 Justification of tracing

Security Objective	Rationale
O.SYSTEM_MONITORING	This objective is satisfied by: **FAU_GEN.1**-specifying the audit events generated by the TOE **FAU_GEN.2**-recording within each audit record information. **FPT_STM.1**-Timestamps associated with the audit record must be reliable.
O.AUDIT_VIEW	This objective is satisfied by: **FAU_SAR.1**-specifying a mechanism for authorized users to review all audit records.
O.CRYPTOGRAPHIC_FUNCTIONS	This objective is satisfied by: **FCS_CKM.1/RSA**-specifying cryptographic key generation by RSA. **FCS_CKM.4/RSA**-specifying cryptographic key destruction by RSA. **FCS_COP.1/DataEncryption**-specifying encryption and decryption by AES. **FCS_COP.1/SigGen**-specifying cryptographic signature services by RSA Digital Signature Algorithm. **FCS_COP.1/Hash**-specifying Hash Cryptographic Operation by SHA***. **FCS_COP.1/KeyedHash**-specifying KeyedHash Cryptographic Operation by HMAC-SHA***.
O.PROTECTED_COMMUNICATIONS	This objective is satisfied by: **FTP_TRP.1**-specifying the security trusted path by HTTPS.
O.SESSION_ACCESS	This objective is satisfied by: **FTA_MCS.1**-specifying basic limitation on multiple concurrent

Security Objective	Rationale
	sessions by same user. **FTA_SSL.3**-specifying terminate an interactive session after a configurable time. **FTA_SSL.4**-specifying user-initiated termination of the user's own interactive session.
O.ID_AUTH	This objective is satisfied by: **FIA_AFL.1**-specifying that an account is locked after a specified number of unsuccessful authentication attempts on the account. **FIA_ATD.1**-specifying the user security attributes associated with users. **FIA_UAU.2**-specifying the authentication of TOE administrators. **FIA_UID.2**-specifying the identification of TOE administrators.
O.SECURITY_MANAGE	This objective is satisfied by: **FMT_MOF.1**-specifying management of security functions behaviour. **FMT_SMF.1**-specifying the management of security functions. **FMT_SMR.1**-specifying the user roles supported by the TOE.
O.ADMIN_ROLE	This objective is satisfied by: **FMT_SMR.1**-specifying the user roles supported by the TOE.

6.3.2 SFR Dependency Analysis

Table 6-5 SFR Missing dependencies justification

SFR	Required	Fulfilled
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FIA_UID.2 FAU_GEN.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1/RSA	FCS_CKM.4/RSA [FCS_CKM.2/RSA or FCS_COP.1/RSA]	FCS_CKM.4/RSA FCS_COP.1/RSA
FCS_CKM.1/DATA_AES	FCS_CKM.4/ DATA_AES [FCS_CKM.2/	FCS_CKM.4/ DATA_AES FCS_COP.1/ DataEncryption

SFR	Required	Fulfilled
	DATA_AES or FCS_COP.1/ DataEncryption]	
FCS_CKM.1/TLS _AES	FCS_CKM.4/ TLS _AES [FCS_CKM.2/ TLS _AES or FCS_COP.1/ DataEncryption]	FCS_CKM.4/ TLS _AES FCS_COP.1/ DataEncryption
FCS_CKM.1/Keyed Hash	FCS_CKM.4/ KeyedHash [FCS_CKM.2/ KeyedHash or FCS_COP.1/ KeyedHash]	FCS_CKM.4/ KeyedHash FCS_COP.1/ KeyedHash
FCS_CKM.4/RSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/RSA]	FCS_CKM.1/RSA
FCS_CKM.4/ DATA_AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/ DATA_AES]	FCS_CKM.1/ DATA_AES
FCS_CKM.4/ TLS_AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/ TLS _AES]	FCS_CKM.1/ TLS _AES
FCS_CKM.4/ KeyedHash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/	FCS_CKM.1/ KeyedHash

SFR	Required	Fulfilled
	KeyedHash _AES]	
FCS_COP.1/DataEncryption	FCS_CKM.4/AES [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/AES]	FCS_CKM.4/DATA_AES FCS_CKM.4/TLS_AES FCS_CKM.4/DATA_AES FCS_CKM.4/TLS_AES
FCS_COP.1/SigGen	FCS_CKM.4/RSA [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/RSA]	FCS_CKM.4/RSA FCS_CKM.1/RSA
FCS_COP.1/Hash	FCS_CKM.4 [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	This SFR specifies keyless hashing operations, so initialisation and destruction of keys are not relevant
FCS_COP.1/KeyedHash	FCS_CKM.4/ KeyedHash [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/ KeyedHash]	FCS_CKM.4/ KeyedHash FCS_CKM.1/ KeyedHash
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	None	None
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2

SFR	Required	Fulfilled
FPT_STM.1	None	None
FTA_MCS.1	FIA_UID.1	FIA_UID.2
FTA_SSL.3	None	None
FTA_SSL.4	None	None
FTP_TRP.1	None	None

6.3.3 SAR Rationale

ASE_REQ.2.8C *The security requirements rationale shall explain why the SARs were chosen.*

The Evaluation Assurance Level 3+ has been chosen to commensurate with the threat environment that is experienced by typical consumers of the TOE.

6.3.4 SAR Dependency Analysis

ASE_REQ.2.5C: *Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.*

Table 6-6 SAR Missing dependencies justification

SAR	Required	Fulfilled	Missing
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	None
ASE_ECD.1	None	None	None
ASE_INT.1	None	None	None
ASE_TSS.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	None
AGD_OPE.1	ADV_FSP.1	ADV_FSP.1	None
AGD_PRE.1	None	None	None
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1	None
ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1	ASE_OBJ.2, ASE_ECD.1	None
ASE_SPD.1	None	None	None
ALC_CMC.3	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1	None
ALC_CMS.3	None	None	None

SAR	Required	Fulfilled	Missing
ALC_DEL.1	None	None	None
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	ADV_FSP.1, ADV_TDS.2 (hierarchically above ADV_TDS.1)	None
ADV_FSP.3	ADV_TDS.1	ADV_TDS.2 (hierarchically above ADV_TDS.1)	None
ADV_TDS.2	ADV_FSP.3	ADV_FSP.3	None
ALC_DVS.1	None	None	None
ALC_LCD.1	None	None	None
ATE_COV.2	ADV_FSP.2, ATE_FUN.1	ADV_FSP.3 (hierarchically above ADV_FSP.2), ATE_FUN.1	None
ATE_DPT.1	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1	None
ATE_FUN.1	ATE_COV.1	ATE_COV.2 (hierarchically above ATE_COV.1)	None
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	ADV_FSP.3 (hierarchically above ADV_FSP.2), AGD_OPE.1, AGD_PRE.1, ATE_COV.2 (hierarchically above ATE_COV.1), ATE_FUN.1	None
AVA_VAN.2	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1	ADV_ARC.1, ADV_FSP.3 (hierarchically above ADV_FSP.2), ADV_TDS.2 (hierarchically above ADV_TDS.1), AGD_OPE.1, AGD_PRE.1	None
ALC_FLR.2	None	None	None

7 TOE Summary Specification

Table 7-1 Justification of tracing

TSF	Rationale
Security Audit	This TSF is designed to satisfy the following security functional requirements: **FAU_GEN.1**- The TOE generates an audit record that is stored internally within the TOE whenever an audited event occurs. The TOE is able to generate the audit record of the following auditable events: • Start-up and shutdown of the audit functions, automatically operating with the restarting process. • Unsuccessful login attempts limit is met or exceeded. • Configure the management function • Configure the timestamp • Unsuccessful login attempts limit is met or exceeded. • The termination of an interactive session • The function of the TLS session, which involve the initiation, termination and failure. And for all the audited event, the TOE will generate the log with the following information: • Date and time of the event • type of event • subject identity • and the outcome (success or failure) of the event With these log information, Each of the events is specified in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. **FAU_GEN.2-** The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result they are traceable to a specific user. **FAU_SAR.1**-the TOE fulfills this requirement by providing admin user, And admin user has the privilege to review the audit log.

TSF	Rationale
Cryptographic support	The TOE provides cryptographic support for the following security functionality: **FCS_CKM.1/RSA Cryptographic key generation-** The TOE shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA2048. RSA is implemented in the following protocols: TLS/HTTPS **FCS_CKM.4/RSA Cryptographic key destruction-**The TOE shall destroy cryptographic keys by overwriting the flash with zero . RSA is implemented in the following protocols: TLS/HTTPS **FCS_CKM.1/DATA_AES Cryptographic key generation-** The TOE shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm random number generation with specified cryptographic key sizes 256 bits. **FCS_CKM.4/DATA_AES Cryptographic key destruction-** The TOE shall destroy cryptographic keys by overwriting the flash with zero . **FCS_CKM.1/TLS_AES Cryptographic key generation-** The TOE shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Key derivation function n with specified cryptographic key sizes 128,256 bits. TLS_AES is implemented in the following protocols: TLS1.2 **FCS_CKM.4/TLS_AES Cryptographic key destruction-** The TOE shall destroy cryptographic keys by overwriting the flash with zero . **FCS_CKM.1/KeyedHash Cryptographic key generation -** The TOE shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Key derivation function n with specified cryptographic key sizes 160,256 bits. KeyedHash is implemented in the following protocols: TLS1.2 **FCS_CKM.4/TLS_AES Cryptographic key destruction-** The TOE shall destroy cryptographic keys by overwriting the flash with zero . **FCS_COP.1/DataEncryption-**The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode (128, 256bits).AES is implemented in the following protocols: TLS/HTTPS **FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)-**The TOE shall perform in accordance with a specified cryptographic algorithm RSA2048 with SHA 256. RSA is implemented in the following protocols: TLS/HTTPS **FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)-**The TSF provides a specified cryptographic algorithm SHA256，SHA1 for digest. SHA256 and SHA1-160 is implemented in the following protocols: TLS/HTTPS **FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)-**The TOE provides HMAC-SHA-1 and HMAC-SHA256 for digest. HMAC-SHA256 is implemented in the following protocols: TLS/HTTPS
Identification and Authentication	The Identification and Authentication function is designed to satisfy the following security functional requirements: **FIA_AFL.1**-the TOE fulfills this requirement by preventing login of

TSF	Rationale
	administrators who have reached a defined threshold of unsuccessful authentication attempt. The TOE provides the authorized administrator the ability to specify the maximum number (default to 5 times) of unsuccessful authentication attempts through remote administrative interface (login unsuccessfully by 3 times, and Verified code is required), before an offending account will be locked out for an administratively defined time period. When an account attempting to log into an administrative interface reaches the administratively set maximum number of failed authentication attempts, the account will not be granted access to the administrative functionality of the TOE until the time period has elapsed(default to 5 min). **FIA_ATD.1**-the TOE fulfills this requirement by maintaining individual accounts with the following attributes: • user name • user level • SHA256 hashes of passwords • temporary blocking time for user accounts after unsuccessful authentication attempts • time when users are logging in and logging off With these user attributes, the TOE could identify, authenticate, authorize all users, and manage the authentication process. **FIA_UID.2 and FIA_UAU.2**-the TOE fulfills these requirements by preventing user access to the TOE until the user is successfully identified and authenticated, even the the least privilege role account which is the common operator.
Security Management	The **admin** user creates all initial users uniformly. When creating users, the **admin** user can bind roles to the users and assign rights to the roles. The Security Management function is designed to satisfy the following security functional requirements: **FMT_MOF.1** and **FMT_SMF.1**- The system can log in remotely through the admin account and password. The passwords can also be changed. All access attempts to systems or data must be authenticated, authorized, and recorded in logs. You can change the maximum number of multipoint logins (default to 10) of a user. The system administrator can specify the maximum number (5times) of incorrect password attempts for an account. If the maximum number of incorrect password attempts is reached, the account is locked. **FMT_SMR.1**- The system administrator can audit logs and use log records to detect potential risks in the system. The system must record the operations on major services in logs. Access to log files must be controlled to ensure log file security. The system administrator must maintain logs as follows: Assign the rights to query logs to dedicated personnel.
Protection of	The protection of the TSF function is designed to satisfy the following

TSF	Rationale
the TSF	security functional requirements: **FPT_STM.1**-The TOE provides a source of date and time information used in audit event timestamps. User can optionally be set to receive clock updates from website.
TOE access	The TOE access function is designed to satisfy the following security functional requirement: **FTA_MCS.1**-the TOE fulfills this requirement by restricting the maximum number of concurrent sessions that belong to the same user. And the maximum number of defaults is 10, supported configurable. **FTA_SSL.3**- Authorized administrators can configure maximum inactivity time-out values for remote administrative sessions. When the idle time limit has been reached, the session will be terminated, and any administrator who was using the session will be required to initiate and authenticate a new session. **FTA_SSL.4**-Administrators are able to initiate termination (logout) of their own authenticated interactive sessions.
Trusted Path	The trusted path function is designed to satisfy the following security functional requirement: **FTP_TRP.1**-the TOE fulfills this requirement by providing secure channels (via TLS) when a remote user communicates with the TOE.

8 Acronyms

The following table shows the acronyms used in this Security Target

Table 8-1 Acronyms

Acronym	Meaning
ST	Security Target
PP	Protection Profile
CC	Common Criteria
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFi	TSF Interface
IT	Information Technology
OSP	Organisational Security Policies
EAL	Evaluation Assurance Level
TSC	TSF Scope of Control
TSS	TOE Summary Specification
IPC	IP Camera

9 Glossary of Terms

Table 9-1 Glossary of Terms

Term	Meaning
Augmentation	Addition of one or more requirement(s) to a package
Evaluation Assurance Level	Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package
Operational Environment	Environment in which the TOE is operated
Protection Profile	Implementation-independent statement of security needs for a TOE type
Security Target	Implementation-dependent statement of security needs for a specific identified TOE
Target Of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance

10 Document References

The following table shows the documents referenced in this Security Target

Table 10-1 Document References

Reference	Document
CC31R4P1	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, Part 1: Introduction and general model
CC31R4P2	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, Part 2: Security functional components
CC31R4P3	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, Part 3: Security assurance components
CEM31R4	Common Criteria Evaluation methodology, Version 3.1, Revision 4