Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-106 CR Certification Report

Issue 1.0 19 April 2018

Huawei IP Camera Series v200R003C20

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.1 11.11.2011

SERTIT, Postboks 814, 1306 Sandvika, NORWAY

Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. The Common Cr iteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognized under the terms of the CCRA July 2nd 2014.

The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.

Contents

1 Certification Statement

Huawei Technology Co. Ltd. Huawei IP Camera Series Products is a series of IP cameras used to send video over an IP network such as a local area network or the Internet.

Huawei IP Camera Series Products version V200R003C20 have been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) augmented requirements of Evaluation Assurance Level EAL 3 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality in the specified environment when running on the platforms specified in Annex A.

Author	Kjartan Jæger Kvassnes Certifier K Kvassnes
Quality Assurance	Arne Høye Rage Quality Assurance Arne H. Rage
Approved	Jørn Arnesen Head of SERTIT
Date approved	19 April 2018

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
IPC	IP Camera
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Huawei IP Camera Series Products V200R003C20 Security Target, Huawei Technology Co. Ltd., version 1.0, 27 March 2018.

[2] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] The Norwegian Certification Scheme, SD001E, Version 10.4, 20 February 2018.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] Evaluation Technical Report Common Criteria EAL3+ALC_FLR.2 Evaluation of "Huawei IP Camera Series V200R003C20", v3.0, 26 March 2018.

[8] CC Huawei IP Camera Series products V200R003C20 AGD_PRE V04.

[9] CC Huawei IP Camera Series products V200R003C20 AGD_OPE V03.

[10] IPC V200R003C20 Product Documentation V01.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Huawei IP Camera Series Products version V200R003C20 to the Sponsor, Huawei Technology Co. Ltd., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was Huawei IP Camera Series Products and version V200R003C20.

These products are also described in this report as the Target of Evaluation (TOE). The developer was Huawei Technology Co. Ltd.

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. 8 IP Cameras are included, namely, IPC6125-WDL-FA, IPC6225-VRZ, IPC6285- VRZ, IPC6325-WD-VRZ, IPC6385-VRZ, IPC6525-Z30, IPC6625-Z30, IPC6681-Z20. 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.

The TOE 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.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The TOE scope is described in the ST [1] chapter 1.4.1 and 1.4.2.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 3, augmented by ALC_FLR.2. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

There are no Organizational Security Policies or rules with which the TOE must comply.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

- 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 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.

4.9 Threats Countered by the TOE's environment

- 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.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

- 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 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.

4.12 IT Security Objectives

- 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.

4.13 Non-IT Security Objectives

- 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..

4.14 Security Functional Requirements

- FAU_GEN.1 Audit data generation
- FAU_GEN.2 User identity association
- FAU_SAR.1 Audit review
- FCS_CKM.1/RSA Cryptographic key generation
- FCS_CKM.1/DATA_AES Cryptographic key generation
- FCS_CKM.1/TLS_AES Cryptographic key generation
- FCS_CKM.1/ KeyedHash Cryptographic key generation
- FCS_CKM.4/RSA Cryptographic key destruction
- FCS_CKM.4/DATA_AES Cryptographic key destruction
- FCS_CKM.4/TLS_AES Cryptographic key destruction
- FCS_CKM.4/ KeyedHash Cryptographic key destruction
- FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)

- FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)
- FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)
- FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)
- FIA_AFL.1 Authentication failure handling
- FIA_ATD.1 User attribute definition
- FIA_UAU.2 User authentication before any action
- FIA_UID.2 User identification before any action
- FMT_MOF.1 Management of security functions behaviour
- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security roles
- FPT_STM.1 Reliable time stamps
- FTA_MCS.1 Basic limitation on multiple concurrent sessions
- FTA_SSL.3 TSF-initiated termination
- FTA_SSL.4 User-initiated termination
- FTP_TRP.1 Trusted path

4.15 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V. Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT in 26 March 2018. SERTIT then produced this Certification Report.

4.16 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 3 assurance package augmented with ALC_FLR.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
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
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

The TOE delivery procedures are outlined for the consumer in [8].

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance listed in the ST[1] chapter 1.4.2. The Common Criteria Security Evaluation - Certified Configuration preparative guidance [8] describes all necessary steps to configure the TOE in the certified configuration. These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

Based on all possible attack paths and threat agents, the evaluator analysed all possible attack scenarios aiming at compromising the assets defined in the ST [1]. Furthermore the evaluator analysed public domain vulnerabilities related to 3rd party libraries such as the OS kernel, the webserver, and the TLS libraries, to check if there are known exploitable vulnerabilities. The evaluator also searched the public domain vulnerabilities for the generic IP camera.

The evaluators assessed all possible vulnerabilities found during evaluation. Potential vulnerabilities were found but only one of them turned out to be possibly exploitable. The developer has updated the guidance to enhance the secure configuration of the TOE, and as a result this issue has become moot.

5.6 Developer's Tests

The Developer Test Plan consists of 15 tests. The categories are based on major groupings of security functionality, and in combination cover all SFRs and TSFIs.

5.7 Evaluators' Tests

For independent testing it was decided to repeat 9 out of the 15 developer tests, which provided a good coverage of the SFRs. The evaluator has also made sure that there is no overlap between these tests and the tests in the ATE IND, thereby maximizing coverage.

The evaluator also analysed the Developer Test Plan to see where additional ATE tests could be performed, and devised 10 additional tests.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Huawei IP Camera Series Products version V200R003C20 meet the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL 3 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of Huawei IP Camera Series Products version V200R003C20 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 4.3 "TOE Scope" and Section 5 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

The above "Evaluation Findings" include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE. In particular the user must not use the Huawei root CA that comes together with the TOE. The user must use their own trusted PKI instead.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of the 8 models. The details of their hardware specification and firmware version are listed below:

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 alarm output • Analog video: 1-channel CVBS output, BNC connector • Audio： 1-channel audio input and 1-channel audio port ,3.5mm mono

Model	Feature	Interface
		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 slot.
IPC6385-VRZ  firmware version：	• Up to 4K(3840×2160) UHD • H.265, H.264 and MJPEG video compression • Wide dynamic range 120dB • Intelligent behavior	• 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

Model	Feature	Interface
V200R003C20	analytics, color recognition, vehicle and pedestrian classification, exception audio detection • IP66 protection class	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 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	• 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

Model	Feature	Interface
	• Intelligent analytics • IK10 Vandal-proof class • IP66 protection class • Ultra wide operating temperature range -40°C ~ 60°C	• 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

TOE Documentation

The supporting guidance documents evaluated were:

[a] CC Huawei IP Camera Series products V200R003C20 AGD_PRE V04

[b] CC Huawei IP Camera Series products V200R003C20 AGD_OPE V03

[c] IPC V200R003C20 Product Documentation 01

Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".

TOE Configuration

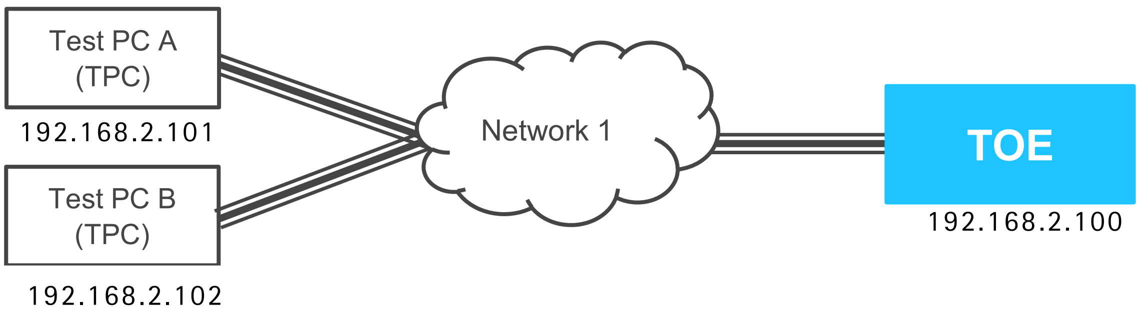
The following configuration was used for testing:

ITEM	IDENTIFIER
HARDWARE	IPC6125-WDL-FA IPC6385-VRZ IPC6525-Z30
SOFTWARE	V200R003C20
MANUALS	CC Huawei IP Camera Series products V200R003C20 AGD_PRE V04 CC Huawei IP Camera Series products V200R003C20 AGD_OPE V03 IPC V200R003C20 Product Documentation 01

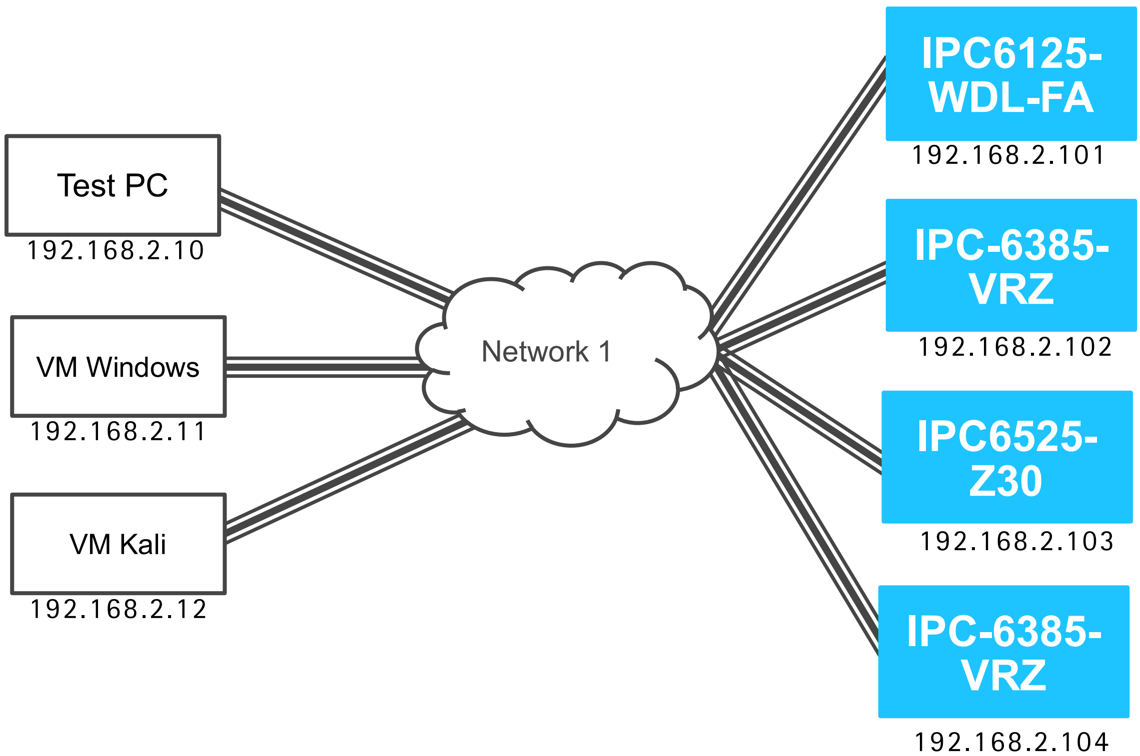
Environmental Configuration

The TOE is tested in the following two different test setups.

Test setup 1



Test setup 2



Certificate

The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunctionwith the complete Certification report. The evaluation has been conducted in accordance with the provisions of The Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced. Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown of this certificate. This certificate is not an endorsement of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Product Manufacturer: Huawei Technologies

Product Name: Huawei IP Camera Series Products

Type of Product: IP Camera

Version and Release Numbers: V200R003C20

Assurance Package: EAL 3 augmented with ALC_FLR.2

Evaluation Criteria: Common Criteria v. 3.1 R4

Name of IT Security Evaluation Facility: Brightsight B.V.

Name of Certification Body: SERTIT

Certification Report Identifier: SERTIT-106 CR Issue 1.0, 19. April 2018

Certificate Identifier: SERTIT-106 C

Date Issued: 19. April 2018

K. Kvassnes

Kjartan Jæger Kvassnes
Certifier

Arne H. Rage

Arne Høye Rage
Quality Assurance

Jørn Arnesen
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security

CCRA recognition for components up EAL 2 and ALC_FLR only.

SOGIS MRA recognition for components up to EAL 4.