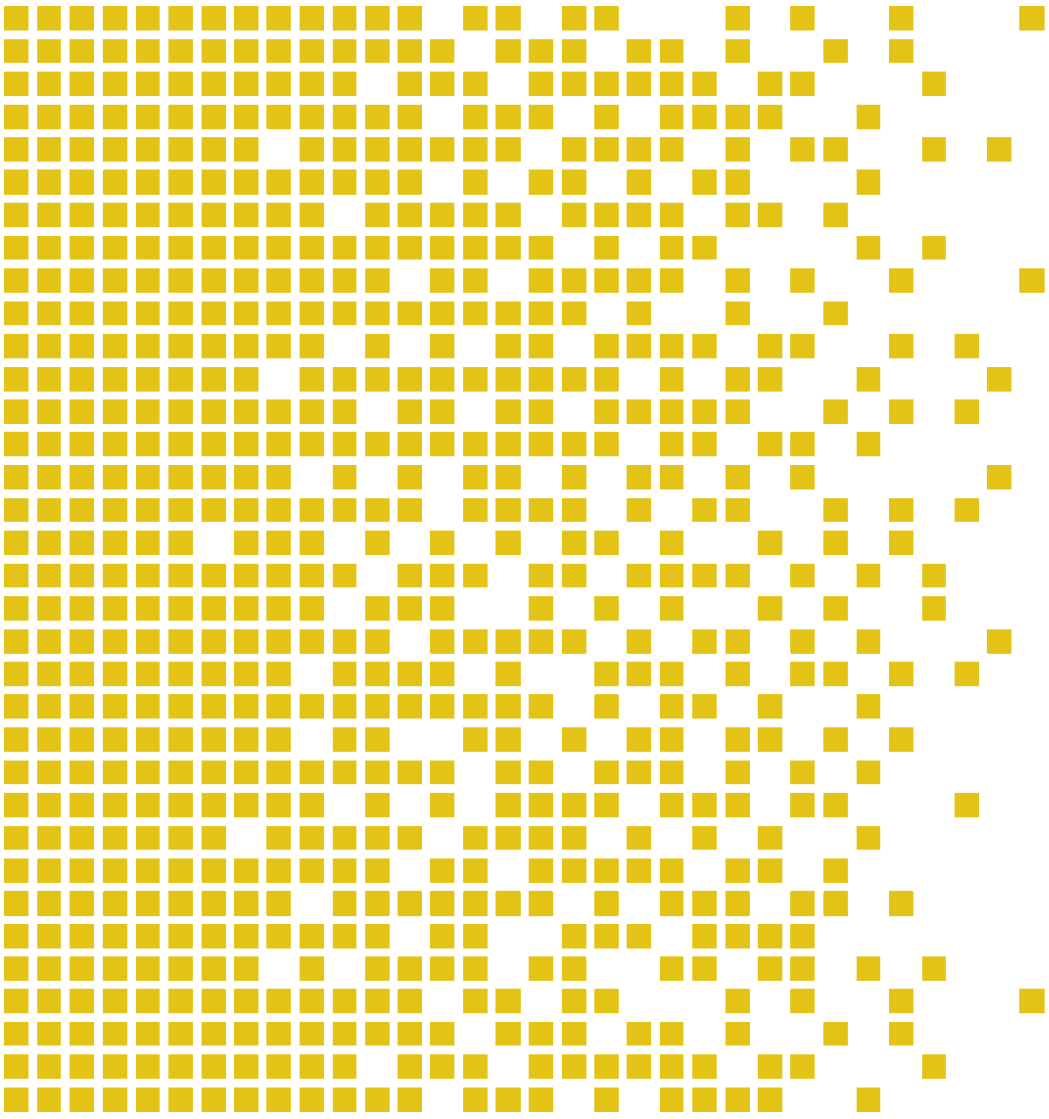
SERTIT-115 CR Certification Report

Issue 1.0 18 September 2018

Expiry date 18 September 2023

Hikvision Network Camera Series Firmware version V5.5.60



SERTIT, P.O. Box 814, N-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 (CCRA)

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 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 recognition under CCRA is limited to cPP related assurance packages or components up to EAL 2 with 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 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 5

2 Abbreviations 6

3 References 7

4 Executive Summary 8
4.1 Introduction 8
4.2 Evaluated Product 8
4.3 TOE scope 9
4.4 Protection Profile Conformance 9
4.5 Assurance Level 9
4.6 Security Policy 9
4.7 Security Claims 9
4.8 Threats Countered 9
4.9 Threats Countered by the TOE's environment 10
4.10 Threats and Attacks not Countered 10
4.11 Environmental Assumptions and Dependencies 10
4.12 IT Security Objectives 11
4.13 Non-IT Security Objectives 11
4.14 Security Functional Requirements 11
4.15 Evaluation Conduct 12
4.16 General Points 13

5 Evaluation Findings 14
5.1 Introduction 14
5.2 Delivery 15
5.3 Installation and Guidance Documentation 15
5.4 Misuse 15
5.5 Vulnerability Analysis 15
5.6 Developer's Tests 15
5.7 Evaluators' Tests 16

6 Evaluation Outcome 17
6.1 Certification Result 17
6.2 Recommendations 17

Annex A: Evaluated Configuration 18
TOE Identification 18
TOE Documentation 19
TOE Configuration 19
Environmental Configuration 20

1 Certification Statement

Hikvision Digital Technology Co. Ltd. Hikvision Network Camera Series is a Network camera which comprises a hardware board and a specific firmware for the hardware.

Hikvision Network Camera Series version V5.5.60 has been evaluated under the terms of the Norwegian Certification Authority for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant to Evaluation Assurance Level EAL 2 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.

Certification team	Kjartan Jæger Kvassnes, SERTIT Arne Høye Rage, SERTIT
Date approved	18 September 2018
Expiry date	18 September 2023

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
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
POC	Point of Contact
PP	Protection Profile
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SOGIS MRA	SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] SERTIT (2018), *The Norwegian Certification Scheme*, SD001E, Version 10.4, SERTIT, 20 February 2018.

[2] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, CCMB-2017-04-001, Version 3.1 R5, CCRA, April 2017.

[3] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, CCMB-2017-04-002, Version 3.1 R5, CCRA, April 2017.

[4] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, CCMB- 2017-04-003, Version 3.1 R5, CCRA, April 2017.

[5] CCRA (2017), *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2017-04-004, Version 3.1 R5, CCRA, April 2017.

[6] SOGIS Management Committee (2010), *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, Version 3.0, SOGIS MC, January 8th 2010.

[7] CCRA (2014), *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, CCRA, July 2nd 2014.

[8] Hikvision (2018), *Hikvision Network Camera Series, Security Target,* Version 3.0.

[9] Brightsight (2018),*Evaluation Technical Report (ETR), Common Criteria EAL2+ALC_FLR.2 Evaluation of "Hikvision Network Camera Series"*, Issue 2.0.

[10] Hikvision (2018), *Hikvision Network Camera Series Security Guidance,* Version 0.7.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Hikvision Network Camera Series version V5.5.60 to the Sponsor, Hikvision Digital 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 ST[8] which specifies the functional, environmental and assurance evaluation components.

4.2 Evaluated Product

The version of the product evaluated was Hikvision Network Camera Series and version V5.5.60.

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

The TOE is a Network camera which comprises a hardware board and a specific firmware for the hardware. The TOE provides a management interface and video over IP functionalities with high security features such as security management, user identification and authentication, trusted path, audit logs, protection on the TSF, cryptographic support, TOE access and trusted firmware updates. Two series of IP cameras are included, namely DS-2CD3 series and DS-2CD5 series. The following list details the models in scope for each family:

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

The TOE environment consists of a LAN network which is totally isolated from other networks (e.g. other LANs or Internet). The TOE network may contain one or multiple TOEs, video recording devices (such as NVR) and management computers via ISAPI. There are two usage scenarios regarding the video distribution:

1. TOE's management interface being accessed from a browser or a client/platform software using ISAPI over HTTPS. ISAPI is an HTTP-based application programming interface that enables the TOE to communicate with IP media devices. Web application and client/platform programs must implement this API.
2. Video data distribution to a network recording device or to a web browser using the RTSP protocol.

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 [8] chapter 1.4.1 and 1.4.2.

4.4 Protection Profile Conformance

The ST[8] did not claim conformance to any protection profile.

4.5 Assurance Level

The ST[8] specified the assurance components for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 2, 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 ST[8] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional components 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.UNAUTHORISED_ACCESS
  Threat agents may try to gain access to TOE functionality without having the required permission such as bypassing user authentication, access to functionality without permissions, administration impersonation, or operation replay. Attackers may take advantage of poorly implemented security measures like authentication, cookie management, design of the communications, etc. By attacking this

functionality it could be possible to execute malicious operations without having the proper privileges.

- T.TRANSMISSION_DISCLOSURE
  Threat agents may be able to obtain credential of valid TOE users during the communication between the same TOE and the other device (e.g. management computer). Weak cryptography implementation like small key sizes or the usage of deprecated algorithms and protocols may allow an attacker to sniff communications, recover credentials or manipulate the traffic. Note that this threat is applicable only for the management interfaces: ISAPI.
- T.VIDEO_MANIPULATION
  Threat agents may try to modify the integrity of the video data sent to the recording devices (NVR). An attacker may try to manipulate video data by a man-in-the middle (MITM) attack intercepting the video data and modifying the content partially or totally or by circumventing the integrity mechanisms of the video data transmission. Successful attacks may allow attackers to manipulate the video image without being detected by the system.
- T.CAMERA_UNAVAILABLE
  Threat agents may try to subvert the availability of the TOE. An inadequate protection against Denial of Service (DOS) attacks or a badly chosen physical protection may allow an attacker to force the interruption of the video data transmission.
- T.UPDATE_COMPROMISE
  Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to alteration.

4.9 Threats Countered by the TOE's environment

No threats or attacks that are countered by TOE's environment are described.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

- A.TRUSTED_USERS
  The administrator of the TOE is a trusted individual which must correctly configure and install the TOE in its operational environment by following the guidance documentation. The users of the TOE are considered trusted individuals which will not carry out any malicious action trying to compromise the availability of the TOE.
- A.TRUSTED_NETWORK_SYSTEMS

Attackers have no chance to connect any malicious devices into the local network of the TOE.

4.12 IT Security Objectives

- O.USER_AUTHENTICATION
  The TOE provides authentication mechanisms for users, of which there are 3 types: Administrator, Operator and User.
- O.USER_AUTHORISATION
  The TOE manages different access control to operations for different user roles.
- O.USER_MANAGEMENT
  The TOE provides management capabilities to the Administrator role for adding/removing users into the system (Operator and User roles) and to configure the access permissions to the TOE functionalities.
- O.AUDIT_LOGS
  The TOE supports logging of events and alarms.
- O.VIDEO_INTEGRITY
  The TOE provides means to ensure the integrity of the video data generated.
- O.FIRMWARE_LOAD_INTEGRITY
  The firmware image during firmware loading is verified by the TOE in terms of integrity and authenticity, to ensure that only valid firmware updates are accepted.
- O.TRUSTED_PATH
  The TOE provides the capacity to establish a trusted path before accessing the management functionality

4.13 Non-IT Security Objectives

- OE.TRUSTED_USERS
  The administrator of the TOE is a trusted individual which will correctly configure and install the TOE in its operational environment by following the guidance documentation. The users of the TOE are trusted individuals that will not perform any malicious action trying to compromise the availability of the TOE.
- OE.TRUSTED_NETWORK_SYSTEMS
  Attackers have no chance to connect any malicious devices into the local network of the TOE.
- OE.TOE_AVAILABILITY
  The operational environment shall protect the TOE against internal attacks trying to disrupt the availability.

4.14 Security Functional Requirements

- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

- FMT_MOF.1 Management of security functions behavior
- FIA_AFL.1 Authentication failure handling
- FIA_SOS.1 Verification of secrets
- FIA_UAU.1 Timing of authentication
- FIA_UID.1 Timing of identification
- FTP_TRP.1 Trusted path
- FAU_GEN.1 Audit data generation
- FAU_SAR.1 Audit review
- FPT_STM.1 Reliable time stamps
- FDP_DAU.1 Basic Data Authentication
- FCS_COP.1/AES Cryptographic operation (AES Data Encryption/Decryption)
- FCS_CKM.1/AES Cryptographic key generation
- FCS_CKM.1/AES_TLS Cryptographic key generation (for TLS)
- FCS_CKM.4/AES Cryptographic key destruction
- FCS_COP.1/Hash Cryptographic operation (Hash Algorithm)
- FCS_COP.1/Sign Cryptographic operation (Signature Generation and Verification)
- FCS_CKM.1/Sign Cryptographic key generation
- FCS_CKM.4/Sign Cryptographic key destruction
- FCS_COP.1/HMAC Cryptographic operation (Keyed Hash Algorithm)
- FCS_CKM.1/HMAC Cryptographic key generation
- FCS_CKM.4/HMAC Cryptographic key destruction
- FTA_MCS.1 Basic limitation on multiple concurrent sessions
- FTA_SSL.4 User-initiated termination
- FPT_TFU.1 Trusted Firmware Updates.

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 SD001E[1]. 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 both the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, CCRA[7], and the Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, SOGIS MRA[6] and the evaluation was conducted in accordance with the terms of these Arrangements.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its ST[8], which prospective consumers are advised to read. To ensure that the ST[8] 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)[5].

SERTIT monitored the evaluation in accordance with SD001E[1] which was carried out by the Name of EVIT Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the final ETR[9] to SERTIT in ETR date. SERTIT then produced this Certification Report.

4.16 General Points

The evaluation addressed the security functionality claimed in the ST[8] with reference to the assumed operating environment specified by the ST[8]. 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 2 assurance package augmented with ALC_FLR.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	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_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

5.1 Introduction

The evaluation addressed the requirements specified in the ST[8]. The results of this work were reported in the ETR[9] 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

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 in the Operational User Guidance documents [10] provided by the developer.

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 [8]. Furthermore, the evaluator analysed public domain vulnerabilities on other versions of the firmware on similar products to check if there are known exploitable vulnerabilities. The evaluator also searched the public domain vulnerabilities for the generic IP camera.

All penetration tests showed that the possible vulnerabilities resulting from the vulnerability analysis could not be exploited.

5.6 Developer's Tests

The Developer Test Plan consists of 22 tests for the TOE DS-2CD3 series and 22 tests for the TOE DS-2CD5 series.. The tests 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 16 (8 for DS-2CD3 series and 8 for DS-2CD5 series) out of the 44 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 analyzed the Developer Test Plan to see where additional ATE tests could be performed, and devised 7 additional tests (see further below), focusing in verification of the TLS implementation, known weaknesses in the web interface and IP cameras specific vulnerabilities.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[9], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Hikvision Network Camera Series version V5.5.60 meet the specified Common Criteria Part 3 conformant components of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 extended functionality in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of Hikvision Network Camera Series version V5.5.60 should understand the specific scope of the certification by reading this report in conjunction with the ST[8]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST.

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

The TOE should be used in accordance with the supporting guidance [10] 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 evaluators consider important to highlight that the TOE must never be configured with self-signed certificates.

Annex A: Evaluated Configuration

TOE Identification

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

Series	Models	Firmware/Software	Interfaces
DS-2CD3	DS-2CD3025G0-I	Firmware V5.5.60 build 180514 Web version V4.0.51 build 180425 Encoding version V7.3 build 180510 Plugin version V3.0.6.43	DC12V, SD, RJ45
	DS-2CD3125G0-IS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3325G0-I		DC12V, SD, RJ45
	DS-2CD3T25G0-I		DC12V, SD, RJ45
	DS-2CD3525G0-IS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3625G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3725G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3H25G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3045G0-I		DC12V, SD, RJ45
	DS-2CD3145G0-IS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3345G0-I		DC12V, SD, RJ45
	DS-2CD3T45G0-I		DC12V, SD, RJ45
	DS-2CD3545G0-IS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3645G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3745G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3H45G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3085G0-I		DC12V, SD, RJ45
	DS-2CD3185G0-IS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3385G0-I		DC12V, SD, RJ45
	DS-2CD3T85G0-I		DC12V, SD, RJ45
	DS-2CD3685G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3785G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD3H85G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
DS-2CD5	DS-2CD5026G0-AP	Firmware V5.5.60 build 180514 Web version V4.0.1 build 180502 Encoding version V7.3 build 180510 Plugin version V3.0.6.38	DC12V, SD, RJ45, RS485, audio 1in 1out, alarm 2in 2out
	DS-2CD5046G0-AP		DC12V, SD, RJ45, RS485, audio 1in 1out, alarm 2in 2out
	DS-2CD5085G0-AP		DC12V, SD, RJ45, RS485, audio 1in 1out, alarm 2in 2out
	DS-2CD5126G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD5146G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD5185G0-IZS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD5A26G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 2in 2out
	DS-2CD5A46G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 2in 2out

	DS-2CD5A85G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 2in 2out
	DS-2CD5526G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD5546G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	DS-2CD5585G0-IZHS		DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out

TOE Documentation

The supporting guidance documents evaluated were:

[a] CC AGD_UM Network Camera User Manual

[b] CC AGD_PRE-OPE Hikvision Network Camenra Series Security Guidance version 0.7

[c] CC AGD_OPE Hikvision ISAPI 2.0 – Image Service

[d] CC AGD_OPE Hikvision ISAPI 2.0 – IPMD Service

[e] CC AGD_OPE Hikvision ISAPI 2.0 – PTZ Service

[f] CC AGD_OPE Hikvision ISAPI 2.0 – RaCM Service

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	DS-2CD5526G0-IZHS, DS-2CD5046G0-AP), B0046-5 (DS-2CD3725G0-IZS), B0046-6 (DS-2CD3025G0-I).
SOFTWARE	Firmware package identified as IPC_H3_EN_STD_5.5.60_180514 for DS-2CD5526G0-IZHS and DS-2CD5046G0-AP and firmware package identified as IPC_G1_EN_STD_5.5.60_180514 for DS-2CD3725G0-IZS and DS-2CD3025G0-I. All the devices were configured according the Security Guidance [10].
MANUAL	CC AGD_UM Network Camera User Manual CC AGD_PRE-OPE Hikvision Network Camenra Series Security Guidance version 0.7 CC AGD_OPE Hikvision ISAPI 2.0 – Image Service CC AGD_OPE Hikvision ISAPI 2.0 – IPMD Service CC AGD_OPE Hikvision ISAPI 2.0 – PTZ Service CC AGD_OPE Hikvision ISAPI 2.0 – RaCM Service

Environmental Configuration

The following network diagram describes the scenario used to perform testing: