CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

# C024 Certification Report

## RADIUSS Core version 2.0

File name: ISCB-5-RPT-C024-CR-v1a
Version: v1a
Date of document: 19 October 2012
Document classification: PUBLIC


For general inquiry about us or our services,
please email: mycc@cybersecurity.my



CyberSecurity Malaysia
(726630-U)
T +603 8946 0999
F +603 8946 0888

Corporate Office:
Level 8, Block A
Mines Waterfront Business Park
No 3 Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
www.cybersecurity.my

# C024 Certification Report

## RADIUSS Core version 2.0

19 October 2012

ISCB Department

**CyberSecurity Malaysia**

Level 8, Block A, Mines Waterfront Business Park,

No 3 Jalan Tasik, The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

Tel: +603 8946 0999 Fax: +603 8946 0888

http://www.cybersecurity.my

# Document Authorisation

| | |
|---|---|
| *DOCUMENT TITLE:* | C024 Certification Report - RADIUSS Core version 2.0 |
| *DOCUMENT REFERENCE:* | ISCB-5-RPT-C024-CR-v1a |
| *ISSUE:* | v1a |
| *DATE:* | 19 October 2012 |

| | |
|---|---|
| *DISTRIBUTION:* | UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION |

# Copyright Statement



Registered office:

Level 8, Block A,

Mines Waterfront Business Park,

No 3 JalanTasik, The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

*Printed in Malaysia*

# Forward

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 19 October 2012, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement at www.commoncriteriaportal.org).

# Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 3 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 3 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

# Document Change Log

| RELEASE | DATE | PAGES AFFECTED | REMARKS/CHANGE REFERENCE |
|---|---|---|---|
| v1 | 8 October 2012 | All | Final Released |
| v1a | 19 October 2012 | Page iv and Table 2 | Add the date of the certificate.<br>Rearranged the table rows. Disallow row to break across pages in Table 2 to cover all content of each rows in a page based on feedback from Scheme Certification Committee. |

# Executive Summary

RADIUSS Core version 2.0 (hereafter referred as RADIUSS Core) from Radmik Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

RADIUSS Core is a Java software module designed to be used as a core security module for RADIUSS (Radmik Intelligent Universal Surveillance System) framework. RADIUSS framework is a management of IP based solution for CCTV system that connect directly to preferred network and is manageable remotely via a local area network or the internet. It can handle simultaneous recording, allows remote access to live views and playback of recorded videos. It supports IP cameras and analogue video sources, and open system architecture to ensure integration with other third party systems.

The functions of the TOE that are within the scope of evaluation covering:

- the security audit logs,
- access control whereby only authorized users can view the video feeds and logs,
- identification and authentication of administrator and users before being allowed to perform any action in the TOE, and
- security management functions that include user management, log management, ACL (Access Control List) management and video camera management.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for RADIUSS Core, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with substances that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of RADIUSS Core to the Common Criteria (CC) evaluation assurance level EAL1. The report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by Stratsec.net Sdn Bhd (Stratsec) Security Evaluation Facility (Stratsec MySEF) and completed on 18 September 2012.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the RADIUSS Core evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that the RADIUSS Core meets their requirements and security needs. It is recommended that a potential user of the RADIUSS Core to refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

# Table of Contents

# Index of Tables



# Index of Figures

# 1 Target of Evaluation

## 1.1 TOE Description

1 The Target of Evaluation (TOE), RADIUSS Core version 2.0 (hereafter referred as RADIUSS Core) is a Java software module designed to be used as a core security module for RADIUSS (Radmik Intelligent Universal Surveillance System) framework.

2 RADIUSS framework is a management of IP based solution for CCTV system that connect directly to preferred network and is manageable remotely via a local area network or the internet. It can handle simultaneous recording, allows remote access to live views and playback of recorded videos. It supports IP cameras and analogue video sources and open system architecture to ensure integration with other third party systems.

3 The evaluated security functionalities of the TOE includes:

a) **Auditing –** The TOE generates logs for video feeds such as recording time, cameras IP address, motion detection, success/failure of user authentication, change of passwords for users and other information.

b) **Access Control** – Data (video feeds and logs) can only be viewed by authorized users. Administrator can configure the access to the functionalities and data based on users' role.

c) **Identification and Authentication** – Administrators and users will need to identify and authenticate themselves before they are allowed to perform any action.

d) **Security Management** – Administrators are able to execute security management functions through the web interface provided by the TOE. The management functions include:

i) User management

ii) Log management

iii) ACL (Access Control List) Management

iv) Video camera management

## 1.2 TOE Identification

4 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

| | |
|---|---|
| **Evaluation Scheme** | Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme |
| **Project Identifier** | C024 |
| **TOE Name** | RADIUSS Core |

| | |
|---|---|
| **TOE Version** | Version 2.0 |
| **Security Target Title** | Radmik Solution RADIUSS Core EAL1 Security Target |
| **Security Target Version** | Version 1.1 |
| **Security Target Date** | 9 July 2012 |
| **Assurance Level** | Evaluation Assurance Level 1 (EAL1) |
| **Criteria** | Common Criteria for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3 (Ref [2]) |
| **Methodology** | Common Evaluation Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3 (Ref [3]) |
| **Protection Profile Conformance** | None |
| **Common Criteria Conformance** | CC Part 2 Conformant<br>CC Part 3 Conformant<br>Package conformant to EAL1 |
| **Sponsor and Developer** | Radmik Sdn Bhd,<br>Suite 6-5, Main Tower Sunsuria Avenue,<br>Persiaran Mahogani, Kota Damansara,<br>47810 Petaling Jaya,<br>Selangor Darul Ehsan, MALAYSIA.<br>Tel: +603-6150 0156 |
| **Evaluation Facility** | Stratsec MySEF |

## 1.3 Security Policy

5 RADIUSS Core implements Access Control Policy on video feeds that are stored in the database. Users need to be identified and authenticated before being able to access the video feeds. The TOE will permit a user to access the protected resources only if a user ID or user role has permission to view the video from a particular camera.

6 The details of the security policy are described in Section 5.1.2 of the Security Target (Ref [6]).

## 1.4 TOE Architecture

7 RADIUSS Core includes both logical and physical boundaries which are described in Section 1.4 and Section 1.5 of the Security Target (Ref [6]).

### 1.4.1 Logical Boundaries

8 The TOE security functions comprises of the following:

a) **Auditing –** The TOE generates audit data that comprises of security relevant events such as user login, camera service interruptions, video feeds accessed, and other information which is described in Section 5.1.1 of the Security Target (Ref [6]). Upon detection of movements from motion sensor cameras, an alert will be sent to the TOE and trigger SMS/email to be sent to users by the TOE.

b) **Access Control** – User data (video feeds, logs) can only be viewed by authorized users. Users will have to identify and authenticate themselves before they are allowed to perform any action. A pre-defined role set by the administrator will be allocated to the successful users. Depending on their roles and user ID, they can only view the video feeds of those cameras that are allocated to them.

c) **Identification and Authentication** – The TOE requires users to provide unique identification and authentication data before any administrative access to the TOE is granted. The TOE provides an authentication mechanism for users through a web interface. The only authentication mechanism supported by the TOE is passwords.

d) **Security Management** – Administrators are able to execute security management functions through the web interface provided by the TOE. This includes modifying the behaviour of the data collection and review, query audit data, and restrict access and/or the ability to query and modify all other TOE data to the appropriate authorized user/authorized role. The management functions include:

i) User management

ii) Log management

iii) ACL (Access Control List) Management

iv) Video camera management

### 1.4.2 Physical Boundaries

9 Figure 1 below describes the typical installation of RADIUSS framework which consists of the TOE.

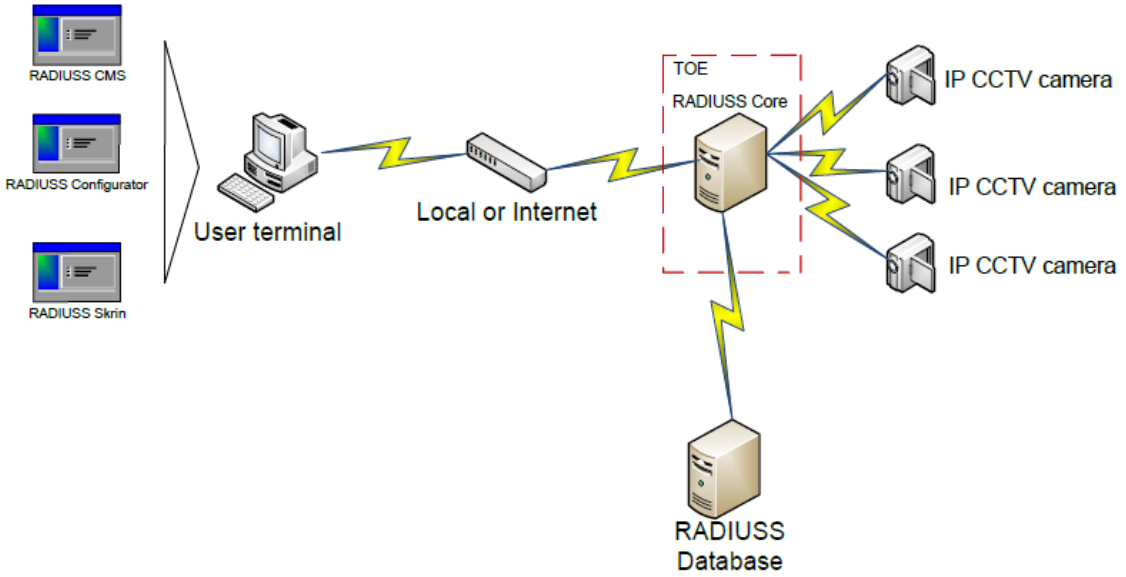


Figure 1: TOE Physical Scope

10 The main components of the RADIUSS framework includes:

a) **RADIUSS Core (TOE) –** provides core security functionalities for the RADIUSS framework.

b) **IP CCTV cameras** – CCTV cameras with IP based that are being used to record or monitor a specific location.

c) **RADIUSS Database –** use to store user information, stores video feeds from the camera, and other information needed by RADIUSS.

d) **User terminal** – use by the users to access the RADIUSS Core features from several GUI interfaces (RADIUSS Clients) installed in the user terminal which consist of RADIUSS Skrin (monitoring video feeds), RADIUSS Configurator (use by the administrator to manage the TOE) and RADIUSS CMS (Centralized Monitoring System use by all users based on their role).

11 The TOE is a Java software module that relies on supporting hardware and software as described in Section 1.3.3 of the Security Target (Ref [6]).

12 The Security Target assumes that environment provides appropriate physical security for the TOE. This would restrict direct access to the TOE.

## 1.5 Clarification of Scope

13 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel and communication security in accordance with administrator guidance that is supplied with the product.

14 Section 1.4.1 of this document described the scope of the evaluation. The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

a) **Audit** – The TOE records video camera-related events and user-related events that comprises security relevant events such as user logging, camera service interruptions, video feeds accessed, and other information. The events are listed in Section 5.1.1 of the Security Target (Ref [6]).

Events are identified by the user ID or the capture devices IP address that caused the events. The TOE allows only Administrator to view the audit records.

If an alert is received from the motion sensor cameras, the TOE will log this event and will send the alert to the user via SMS or email.

b) **Access Control** – User data (video feeds, logs) can only be viewed by authorized users. Users will have to identify and authenticate themselves and will be allocated a pre-defined role set by the administrator. Depending on their roles and user ID, they can only view the video feeds of those cameras that are allocated to them.

The TOE maintains access control lists (ACLs) for each object within an organisation. Each ACL maps users and roles to the operations that they are permitted to perform on the object.

There are 2 users maintained by the TOE: custom user, and Administrator. Each type of user will have different access rights to a user data and functionalities of the TOE. All users will have a unique user ID.

c) **Identification and Authentication** – The TOE requires users to provide unique identification and authentication data before any administrative access to the TOE is granted through a web interface. To login to the TOE, the user provides user ID and password. The TOE will hash the password and compares it to the stored user credential in the database. If either the login name or the password is incorrect, the login request will fail and no access to any functions will be made available. As result of a successful login, the session is established and authenticated user can access the TOE functionalities according to the role that is assigned to that particular user.

d) **Security Management** – The TOE contains various management functions to ensure efficient and secure management of the TOE:

i) User management – creation/deletion/modification of users and assigning each user to a role.

ii) Log Management – to allow certain users to view certain event logs.

iii) ACL Management – manage the actions that can be done by certain roles.

iv) Video camera management – allows users to enrol/remove camera.

Only Administrator and specific custom user role can modify the access control list, mapping of users to roles, registering/removing cameras, viewing certain event logs as well as modifying the user accounts.

The TOE maintains 2 roles to ensure that the functions are restricted to only those users that need to have access to privileged functions. The roles maintained by the TOE are: custom user, and Administrator. The functions above, and indeed, aspects of these functions, are restricted based on these roles.

The TOE allows no one to change the default values of the TSF data and security attributes of the TOE.

15 Potential consumers of the TOE are advised that some functions and services may not have been evaluated as part of the evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

16 Functions and services which are not included as part of the evaluated configuration are as follows:

a) A Hardware Server;

b) An Operating System on which the TOE is installed on;

c) A Database Software on which the TOE is dependent on as its database, MySQL 5;

d) User terminal/computer;

e) Other supporting software;

i) A web server software with PHP5 module (Apache 2.0).

ii) Monitoring software – Monit.

iii) Video player – VLC 0.9.

## 1.6 Assumptions

17 There is no assumption declared by developer.

## 1.7 Evaluated Configuration

18 This section describes the configurations of the TOE that are included within the scope of the evaluation.

19 The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented preparative user guidance (Ref 24) and defined in Section 1.3 of the Security Target (Ref [6]).

## 1.8 Delivery Procedures

20 The TOE is delivered to the customer by trusted staff from Radmik Sdn Bhd. Once the customer has accepted the delivery, installation of the TOE will proceed. The TOE shall be installed, configured, and set up by the trusted staff from Radmik Sdn Bhd.

21 However, for this EAL1 evaluation, TOE Delivery (ALC_DEL) is not included in the scope of the evaluation. Thus, developer did not provide any documentation on TOE delivery and the evaluators did not verify any TOE delivery process.

## 1.9 Documentation

22 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

23 The following documentation is provided by the developer to the end user as guidance to ensure secure operation of the product:

a) Radmik Solution RADIUSS Core EAL1 Guidance Documentation (Ref [8]).

b) Radiuss CMS, Centralized Monitoring System User Guide Version 1.0.10, 23 September 2010.

c) Radiuss Configurator 2.1 User Guide version 2.1, 23 September 2010.

d) Radiuss SKRIN User Guide Version 1.0.10, 23 September 2010.

24 The following documentation is used by the developer's authorised personnel as guidance to ensure secure installation of the product:

a) Radmik Solution RADIUSS Core EAL1 Guidance Documentation (Ref [8]).

b) Radiuss Core Installation Guide Rev 2, 7 September 2011.

# 2 Evaluation

25 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 1 (EAL1). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

## 2.1 Evaluation Analysis Activities

26 The evaluation activities involved a structured evaluation of RADIUSS Core, including the following components:

### 2.1.1 Life-cycle support

27 An analysis of the RADIUSS Core configuration management system and associated documentation was performed. The evaluators confirmed that the configuration list which includes the TOE and the evaluation evidence were clearly and uniquely labelled.

### 2.1.2 Development

28 The evaluators analysed the RADIUSS Core functional specification; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces (TSFIs), and how the TSF implements the security functional requirements (SFRs).

### 2.1.3 Guidance documents

29 The evaluators examined the RADIUSS Core preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

### 2.1.4 IT Product Testing

30 Testing at EAL1 consists of performing independent function test, and performing penetration tests. The RADIUSS Core testing was conducted at Stratsec MySEF lab in Plaza Sentral, Kuala Lumpur. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

#### 2.1.4.1 Independent Functional Testing

31 At EAL1, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining functional and guidance documentation, and creating test cases to verify the behaviour of the TOE.

32 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The result of the independent tests developed and performed by the evaluators to verify the TOE functionality as follows:

Table 2: Independent Functional Testing

| DESCRIPTION | SECURITY FUNCTION | TSFI | RESULTS |
|---|---|---|---|
| To test that the TSF shall perform hashing in accordance with a specified cryptographic algorithm (MD5) and meet the following: (FIPS 180-2). | FCS_COP.1 (Cryptographic operation) | • Web Interface<br>• Authentication Database Interface | **PASS**. Password MD5 value for 'radiuss' which was stored in the TOE is the same even though using different MD5 tool. |
| To test that the TOE shall send an alert to Radiuss CAS upon detection of a potential security violation. | FAU_ARP.1 (Security alarms) | Capturing Device Interface | **PASS.** Each alert triggered based on event defined in the capture device interface has properly mitigate to the correct channel such as email or SMS. |

| | | | |
|---|---|---|---|
| 1) The TSF shall be able to generate an audit record of the following auditable events:<br>a) Start-up and shutdown of the audit functions;<br>b) All auditable events for the level of audit; and<br>c) the following auditable events:<br>- user identification and authentication<br>- receiving of camera feeds and data<br>- user management<br>- video device management<br>2) The TSF shall record within each audit record at least the following information:<br>a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and<br>b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [date, time, camera's IP, user ID]. | FAU_GEN.1 (Audit data generation) | • Web Interface<br>• Capturing Device Interface<br>• Authentication Database Interface<br>• Storage Database Interface | **PASS.** Each auditable event able to generate audit records based on the claims. |

| | | | |
|---|---|---|---|
| To test that 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_GEN.2 (User identity association) | • Web Interface<br>• Capturing Device Interface<br>• Authentication Database Interface<br>• Storage Interface | **PASS.** The audit record has display the responsible person that causes the audit events. |
| 1) To test that the TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.<br>2) To test that the TSF shall enforce the following rules for monitoring audited events:<br>a) Accumulation or combination of (an alert sent by the motion-sensor cameras) known to indicate a potential security violation. | FAU_SAA.1 (Potential violation analysis) | Capturing Device Interface | **PASS.** Capturing device interface is able to identify potential security violation based on events defined in test step. |
| To test that the TSF shall enforce the User Access Control SFP on<br>Subjects:<br>a) Administrator<br>Objects:<br>b) Video Feeds<br>Operations:<br>c) Viewing of video feeds | FDP_ACC.1 (Subset access control) | • Web Interface<br>• Authentication Database Interface<br>• Storage Database Interface | **PASS.** Database has identified the right person to login and each user has been defined with different role by administrator. |

| | | | |
|---|---|---|---|
| 1) To test that the TSF shall enforce the User Access Control SFP to objects based on the following:<br>Subject attribute:<br>a) ID of the user<br>b) corresponding user role<br>Object attributes:<br>Access Control List<br>2) To test that the TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [<br>The operation is allowed, if:<br>a) The Access Control List for an object permits the user ID to access that object; OR<br>b) The Access Control List for an object permits the User Role to access that Object.].<br>3) To test that the TSF shall explicitly authorise access of subjects to objects based on the following additional rules: the Administrator role can access all records and functions. | FDP_ACF.1 (Security attribute based access control) | • Web Interface<br>• Authentication Database Interface<br>• Storage Database Interface | **PASS**. The TOE is able to perform access control and allow operation based on ID, roles, access control list. |
| To test that the TSF shall maintain the following list of security attributes belonging to individual users: [<br>- User ID<br>- Role<br>- Password | FIA_ATD.1 (User attribute definition) | • Web Interface<br>• Authentication Database Interface | **PASS**. The testing proved that the TOE is able to maintain ID, password and role for each user. |

| | | | |
|---|---|---|---|
| To test that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. | FIA_UAU.2 (User authentication before any action) | • Web Interface<br>• Authentication Database Interface | **PASS.** The testing proved that the user is able to login without any other TSF intermediate action. |
| To test that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. | FIA_UID.2 (User identification before any action) | • Web Interface<br>• Authentication Database Interface | **PASS.** User is able to login without any other TSF intermediate action and TOE has shown the record for respective user. |
| To test that the TSF shall enforce the User Access Control SFP to restrict the ability to (*delete,* write) the security attributes to only administrator. | FMT_MSA.1 (Management of security attributes) | • Web Interface<br>• Authentication Database Interface | **PASS.** The testing has proved that only administrator will be able to delete/write security attributes. |
| 1) To test the TSF shall enforce the User Access Control SFP to provide restrictive default values for security attributes that are used to enforce the SFP.<br>2) To test that the TSF shall allow specifying alternative initial values to override the default values when an object or information is created. | FMT_MSA.3 (Static attribute initialisation) | • Web Interface<br>• Authentication Database Interface | **PASS.** The testing has proved that the password will be the default values for security attributes and this value will be able to login the object or user account. |

| | | | |
|---|---|---|---|
| To test that the TSF shall be capable of performing the following management functions:<br>a) mapping user IDs to roles<br>b) creation of users with default passwords<br>c) enrolment of new camera<br>d) deletion of users<br>e) deletion of camera<br>f) changing of passwords<br>g) management of Access Control lists<br>h) log management | FMT_SMF.1 (Specification of Management Functions) | • Web Interface<br>• Authentication Database Interface | **PASS.** The testing has proved that the TSF is able to perform the listed management functions. |
| 1) To test that the TSF shall maintain the roles for custom user and administrator.<br>2) To test that the TSF shall be able to associate users with roles. | FMT_SMR.1 (Security roles) | • Web Interface<br>• Authentication Database Interface | **PASS.** The testing demonstrated that normal user and administrator will be maintain and associate with role in TOE. |

33 All tests performed by the evaluators produced the expected results and as such the TOE behaved as expected.

#### 2.1.4.2 Penetration Testing

34 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, and functional specification.

35 From the vulnerability analysis, the evaluators conducted penetration testing to determine whether potential vulnerabilities could be exploited in the intended operating environment of the TOE, to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE;

d) Window of opportunity; and

e) IT hardware/software or other requirement required for exploitation.

36 The penetration tests focused on:

a) Injection attacks;

b) Security misconfiguration; and

c) Information disclosure.

37 The results of the penetration testing note that there is no exploitable vulnerability and/or residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment.

#### 2.1.4.3 Testing Results

38 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

39 Based on the results of penetration testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

# 3 Result of the Evaluation

40 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of RADIUSS Core performed by the Stratsec MySEF.

41 Stratsec MySEF found that RADIUSS Core upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL1.

42 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities undiscovered in its claimed security functionality. This risk is reduced as the certified level of assurance increases for the TOE.

## 3.1 Assurance Level Information

43 EAL1 provides a basic level of assurance by a limited Security Target and an analysis of the security functions in that Security Target, using a functional and interface specification and guidance documentation, to understand the security behaviour.

44 The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TOE security functions.

45 EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

## 3.2 Recommendation

46 In addition to ensure secure usage of the product, below are additional recommendations for RADIUSS Core consumers:

a) The users of the TOE should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

b) The TOE and database servers are hosted in a secure operating facility with restricted physical access and on dedicated hardware.

c) Appropriate network layer protection, such as firewall, that will permit only access through specific ports for external users to access the web server.

d) The underlying operating system, web server and database server are patched and hardened to protect against known vulnerabilities and security configuration issues.

e) All SSL certificates are maintained and valid (not revoked or expired), and are sourced from a trusted entity.

f) Use the product only in its evaluated configuration.

g) Ensure the installation and configuration, done by the developer, follow the installation guidance document.

# Annex A References

## A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[6] Radmik Solution RADIUSS Core EAL1 Security Target, Version 1.1, 9 July 2012

[7] EAL1 Evaluation of Radmik RADIUSS Core, Version 3.1, 18 September 2012

[8] Radmik Solution RADIUSS Core EAL1 Guidance Documentation, Version 1.1, 9 July 2012

## A.2 Terminology

### A.2.1 Acronyms

Table 3: List of Acronyms

| Acronym | Expanded Term |
|---|---|
| ACL | Access control list |
| CB | Certification Body |
| CC | Common Criteria (ISO/IEC15408) |
| CEM | Common Evaluation Methodology (ISO/IEC 18045) |
| CCRA | Common Criteria Recognition Arrangement |
| IEC | International Electrotechnical Commission |
| ISCB | Information Security Certification Body |
| ISO | International Standards Organisation |
| MyCB | Malaysian Common Criteria Certification Body |
| MyCC | Malaysian Common Criteria Evaluation and Certification Scheme |
| MyCPR | MyCC Scheme Certified Products Register |
| MySEF | Malaysian Security Evaluation Facility |

| Acronym | Expanded Term |
|---|---|
| PP | Protection Profile |
| RADIUSS | Radmik Intelligent Universal Surveillance System |
| ST | Security Target |
| TOE | Target of Evaluation |

### A.2.2 Glossary of Terms

Table 4: Glossary of Terms

| Term | Definition and Source |
|---|---|
| CCTV | Closed-circuit television which transmit a signal to a specific place such as a storage room in a store that are connected on a monitor. Mostly used as surveillance systems. |
| Certificate | The official representation from the CB of the certification of a specific version of a product to the Common Criteria. |
| Certification Body | An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA |
| Consumer | The organisation that uses the certified product within their infrastructure. |
| Developer | The organisation that develops the product submitted for CC evaluation and certification. |
| Evaluation | The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS ISO/IEC Guide 65 |
| Evaluation and Certification Scheme | The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA. |
| Interpretation | Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. |
| Certifier | The certifier responsible for managing a specific certification task. |
| Evaluator | The evaluator responsible for managing the technical aspects of a specific evaluation task. |

| Term | Definition and Source |
|---|---|
| Maintenance Certificate | The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme. |
| Motion sensor camera | A type of camera that is able to detect motion changes for example object's movement. Normally, if motion is detected, the camera will send an alarm. |
| National Interpretation | An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only. |
| NTP Server | Network Time Protocol server, a protocol that provide for synchronizing the time of computer systems in a network. |
| Security Evaluation Facility | An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy |
| Sponsor | The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer. |

--- END OF DOCUMENT ---