Indian CC Certification Scheme (IC3S)

Certification Report

Report Number : STQC/CC/1314/09/CR
Product / system : IPOS, Build Number IPOS Release 15.2 running on Ericsson Smart Service Routers, SSR 8020 / SSR 8010

Dated: 24th April, 2018

Version: 1.0

Government of India
Ministry of Communication & Information Technology
Department of Electronics and Information Technology
Standardization, Testing and Quality Certification Directorate
6. CGO Complex, Lodi Road, New Delhi – 110003
India

Product developer:	Ericsson India Private Limited
TOE evaluation sponsored by:	Ericsson India Private Limited
Evaluation facility:	ERTL (E)-CCTL, ERTL (East), DN-Block, Sector V, Salt Lake, Kolkata-700091, India.
Evaluation Personnel:	Subhendu Das, Malabika Ghose & Tapas Bandyopadhyay
Evaluation report:	STQC IT (KOL)/STQC/CC/1314/09/ETR/0658/v1.0
Validation Personnel:	Alok Sain

Table of Contents

Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY 4
A1 Certification Statement 4
A2. About the Certification Body 4
A3 Specifications of the Certification Procedure 5
A4 Process of Evaluation and Certification 5
A5 Publication 5
PART B: CERTIFICATION RESULTS 6
B.1 Executive Summary 6
B 2 Identification of TOE 7
B 3 Security policy 7
B.4 Assumptions 7
B.5 Evaluated configuration 7
B.6 Document evaluation 8
B 7 Product Testing 9
B 8 Evaluation Results 11
B 9 Validator Comments 12
B 10 List of Acronyms 12
B 11 References 12

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

A1 Certification Statement

The product below has been evaluated under the terms of the Indian Common Criteria Certification Scheme (IC3S) and has met the stated Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	Ericsson India Private Limited
Developer	Ericsson India Private Limited
The Target of Evaluation (TOE)	The TOE is the IPOS, Build Number IPOS Release 15.2 running on Ericsson Smart Service Routers, SSR 8020 / SSR 8010.
Security Target	Security Target identification: Security Target for Ericsson Smart Service Router SSR 8020, SSR 8010 running IPOS Software, Revision PA12
Brief description of product	IPOS running on an Ericsson SSR series routing platform is a complete routing system that supports Ethernet interfaces for medium/large networks and network applications. Ericsson routers share common IPOS software, features, and technology for compatibility across platforms. The Smart Service Router is a carrier-class product that supports high availability and the ability to have multiple virtual routers through the configuration of “contexts”, known as a Multi-Service Edge Router (MSER), with an architecture that supports packetized traffic. This router is considered "smart" as it combines different kinds of network traffic such as mobile, video, and so on and manages them in one single router. The 3 main system components are the chassis, controller cards, and traffic cards also known as Ethernet line cards.
CC Part 2 [CC-II]	Conformant
CC Part 3 [CC-III]	Conformant
EAL	EAL3
Evaluation Lab	Common Criteria Test Laboratory, ERTL(E), Kolkata
Date Authorized	April 24, 2018

A2. About the Certification Body

STQC IT Certification Services, the IT Certification Body of Standardization Testing and Quality Certification – was established in 1998 and offers a variety of services in the context of security evaluation and validation. It is the first Certification Body in India for BS 7799/ISO 27001 certification of Information Security Management Systems (ISMS). The Indian CC Certification Scheme (IC3S) is the IT security evaluation & certification Scheme based on Common Criteria standards, it is established by Govt. of India under Department of Information Technology, STQC Directorate to evaluate & certify the trustworthiness of security features in Information Technology (IT) products and systems. The IC3S is an Indian independent third party evaluation and certification scheme for evaluating the security functions or mechanisms of the IT products. It also provides framework for the International Mutual Recognition of such certificates with the member countries of CCRA (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security). The principal participants in the scheme are-

a) Applicant (Sponsor/Developer) of IT security evaluations;
b) STQC Certification Body (STQC/DeitY/MCIT/Govt. of India);
c) Common Criteria Testing Laboratories (CCTLs).

A3 Specifications of the Certification Procedure

The certification body operates under the official administrative procedures according to the criteria and procedures laid down in the following:

- ISO/IEC Guide 65, and the requirements laid down in Annex C of CCRA
- Indian Common Certification Scheme (IC3S)
- STQC/CC/DO2: Standard Operating Procedure (SOP) for Certification Body - Quality Manual – describes the quality management system for the Scheme.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, Version 3.1
- Common Evaluation Methodology (CEM) Version 3.1.

A4 Process of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The TOE has undergone the certification procedure at **STQC IT Certification Body**. The evaluation of the product was conducted by the evaluation body Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. Hereafter this has been referred as CCTL. The evaluation facility is recognized under the IC3S scheme of STQC IT Certification Body.

Ericsson India Private Limited is the developer and sponsor of the TOE evaluation.

The certification process is concluded with the completion of this certification report.
This evaluation was completed on 8th Sept 2017 after submission of [ETR] to the certification body. Subsequent modification was done in {ETR} on 23rd April, 2018. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stated condition regarding configuration and operation, as given in part B of this report, are observed,
- The product is operated – where indicated – in the environment described.

This certification report applies only to the version and release of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

A5 Publication

The following Certification Results consist of Sections B1 to B11 of this report. The TOE will be included in the list of the products certified under IC3S Scheme of STQC IT Certification Body. The list of certified products is published at regular intervals in the Internet at http://www.commoncriteria-india.gov.in. Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form on request to the Certification Body.

PART B: CERTIFICATION RESULTS

B.1 Executive Summary

B.1.1 Introduction

The Certification Report documents the outcome of Common Criteria security evaluation of the TOE. It presents the evaluation results and the conformance results. This certificate is intended to assist the prospective buyers and users when judging the suitability of the IT security of the product for specified requirements.

Prospective buyers and users are advised to read this report in conjunction with the referred [ST] of the product, which specifies the functional, environmental and assurance requirements.

The evaluation was performed by Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. The information in the test report is derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] written by Common Criteria Test Laboratory [ERTL (E)-CCTL], ERTL (EAST), Block-DN Sector-V, Kolkata. The evaluation team determined the product to be CC Version 3.1, Part 2 and Part 3 conformant and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL3) have been met.

B 1.2 Evaluated product and TOE

The TOE consists of IPOS, Build Number IPOS Release 15.2 running on Ericsson Smart Service Routers, SSR 8020 / SSR 8010.

The evaluated sub-set and configuration of the product is described in this report as the Target of Evaluation (TOE). The Evaluated Configuration, its security functions, assumed environment, architectural information and evaluated configuration are given below (Refer B2 to B5).

B 1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter. Most of the Security Functional Requirements (SFRs) are taken from CC Part 2.

B 1.4 Conduct of Evaluation

The evaluation was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. STQC/CC/1314/09 dated 19th June 2013.

The TOE as described in the [ST] is called as IPOS. It is a router operating system running on Ericsson Smart Service Routers, SSR 8020 / SSR 8010. The TOE was evaluated through evaluation of its documentation; testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM] and ERTL (E)-CCTL, Kolkata Operating Procedure OP-07.

The evaluation has been carried out under written agreement [dated Nov 2013] between ERTL (E)-CCTL, Kolkata and the sponsor.

B 1.5 Independence of Certifier

The certifier did not render any consulting or other services for the company ordering the certification and there was no relationship between them which might have an influence on this assessment.

B 1.6 Disclaimers

The certification results only apply to the version and release of the product as indicated in the certificate. The certificate is valid for stated conditions as detailed in this report. This certificate is not an endorsement of the IT product by the Certification Body or any other organization that recognizes or gives effect to this certificate. It is also not an endorsement of the target of evaluation (TOE) by any agency of the Government of India and no warranty of the TOE is either expressed or implied.

B 1.7 Recommendations and conclusions

- The conclusions of the Certification Body are summarized in the Certification Statement at Section A1.
- The specific scope of certification should be clearly understood by reading this report along with the [ST].
- The TOE should be used in accordance with the environmental assumptions mentioned in the [ST].
- The TOE should be used in accordance with the supporting guidance documentation.
- This Certification report is only valid for the evaluated configurations of the TOE.

B 2 Identification of TOE

The TOE is the IPOS, Build Number IPOS Release 15.2 running on Ericsson Smart Service Routers, SSR 8020 / SSR 8010.

B 3 Security policy

There are no organizational security policies that the TOE must meet.

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Table 1: Assumptions

A. Type	Description
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.NOEVIL	The authorized users will be competent, and not careless or willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.EAUTH	External authentication services will be available through either a RADIUS server or a TACACS server, or both.
A.TIME	External NTP services will be available.

B.5 Evaluated configuration

IPOS running on an Ericsson SSR series routing platform is a complete routing system that supports Ethernet interfaces for medium/large networks and network applications. Ericsson routers share common IPOS software, features, and technology for compatibility across platforms.

The Smart Service Router is a carrier-class product that supports high availability and the ability to have multiple virtual routers through the configuration of “contexts”, known as a Multi-Service Edge Router (MSER), with an architecture that supports packetized traffic. This router is considered "smart" as it combines different kinds of network traffic such as mobile, video, and so on and manages them in one single router. The 3 main system components are the chassis, controller cards, and traffic cards also known as Ethernet line cards.

The RPSW card runs the software that controls the system and is responsible for the packet routing protocols and the IPOS command-line interface (CLI).

The architecture is a carrier-class or ISP-class product (depending on customer needs), targeted towards edge network markets. Its architecture supports packet-based IP traffic.

The router architecture of each platform cleanly separates routing and control functions from packet forwarding operations, thereby eliminating bottlenecks and permitting the router to maintain a high level of performance.

The TOE can optionally use the service of external servers, for example, RADIUS and TACACS for authentication, NTP for time synchronization, Syslog for event logging. However the TOE is able to function even in the absence of these components also.

Table 2: Details of evaluated instantiations of the TOE

The image files	File size in kilo bytes	Hash values of the image files	Hardware platform	Software Version and Release
SSR-IPOS-15.2.129.1.108.tar.gz	1,964,891 KB	MD5: BADFE4499D117F63441D6AFE88F0E38E	SSR8020 / SSR8010	Version 15.2.129.1.108-Release

B.6 Document evaluation

B.6.1 Documentation

The list of documents, those were presented, as evaluation evidences to the evaluators at the evaluation facility, are given below:

1. **Security Target**: Security Target for Ericsson Smart Service Router SSR 8020, SSR 8010 running IPOS Software, Revision PA12.
2. **TOE Architecture document**: Architecture: Security Architecture.
3. **TOE Functional Specification document**: IPOS Functional specification.
4. **TOE Design document**: Design Specification of Ericsson IPOS.
5. **Preparative procedures**: Preparatory Guidance Document
6. **Operational User guidance**: Operational User Guidance, AGD_OPE: EAL3 Certification
7. **Configuration Management, Capability /scope and TOE delivery**:.CONFIG.MANAGEM. PLAN
8. **Test cases, logs and coverage**: Test specification

B.6.2 Analysis of document

The documents related to the following areas were analyzed using [CEM]. The summary of analysis is as below:

Development process: The evaluators analyzed the functional specification of the TOE and found that the TOE security function interfaces are described clearly and unambiguously. The evaluators also analyzed design and architectural descriptions of the TOE and determined that the only subsystem of the TOE (i.e. router subsystem) is clearly described in the design description. The evaluators determined that architectural description of the TOE includes secure initialization of the TOE and also means of protection of the TOE from tampering and bypassing.

Guidance Documents: The evaluators analysed guidance documents like preparative procedure and operational user guidance and determined that preparative procedure describes clear and unambiguous steps to bring the TOE to its secure state. The operational user guidance information was also clear and unambiguous.

Life-cycle support documents: The Life cycle support process document, containing information on

Configuration Management and Delivery Procedure were evaluated.

Configuration management: The evaluators analyzed configuration management documentation and determined that the TOE and its associated documents are clearly identified as configurable items. The evaluators also analyzed access control measures defined in the documentation and found satisfactory**.**

Delivery procedure: The delivery procedure document was audited with the objective to ascertain whether it covers secure delivery of the TOE to the end-users. The secure delivery procedure has been described in the document and the same has been audited by the evaluators during their site visit. The end-users can check integrity of the evaluated TOE using hash value of that, if felt necessary.

The final version of the respective evaluation evidences were found to comply with the requirements of CCv3.1 for EAL3.

B 7 Product Testing

Testing at EAL3 consists of the following three steps: Testing by developer, Independent Testing by Evaluation Team, and Penetration testing.

B 7.1 IT Product Testing by Developer

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the [ETR].

The evaluators reviewed the developer's test coverage and depth analysis and found them to be complete and satisfactory. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design was complete.

B 7.2 IT Product Independent Testing by Evaluation Team

The evaluators' independent functional testing effort is summarized as below.
All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and reproducibility of results.
The evaluators have examined the TOE and it is found to be configurable as per the description given in the developer's preparative guidance document. It is also observed that the test configuration is consistent with the description as given in the security target document. Highlights of Independent testing are given below:
The TOE has been installed properly as per the preparative procedure document.
The evaluators have repeated the developer's test at CCTL, Kolkata to confirm the reproducibility of the test results.
While making the test strategy for independent testing, consideration is given to cover the security requirements, as well as the security specification as defined in the security target, interfaces available to the users to cover each of security functional requirements, TOE design and security architecture information. Independent testing is designed to verify the correct implementation of security functionalities available to different levels of users and to check whether audit is being generated for auditable events.

The tests were designed to cover following TSFs and associated TSFIs of the TOE:

a. Security Audit

IPOS auditable events are stored locally in the syslog folder and they can also be sent to an external log server, the requirements for auditing are met by local storage. Audit events cover authentication

activity and configuration changes. Audit logs include the date and time, event category, event type & username. An accurate time is gained by the appliance ntp daemon, acting as a client, from an NTP server in the IT environment. This external time source allows synchronization of the TOE audit logs with external audit log servers in the environment.

b. User data protection

The TOE is designed to forward network packets (i.e., information flows) from source network entities to destination network entities based on available routing information. This information is either provided directly by TOE users or dynamically gets generated through routing protocols.

c. Identification and authentication

The TOE requires users to provide unique authentication information before any access to the system is granted. TOE provides five levels of authority to the users (in increasing level of privilege) – Non-privileged user, Restricted-Operator, Operator, Restricted-Admin, and Administrator providing administrative flexibility.

Authentication services can be handled either internally (user selected passwords) or through a RADIUS or TACACS authentication server in the IT environment (the external authentication server is considered outside the scope of the TOE). SSH can use Public Key Authentication or password for the validation of the user credentials, but the user's identity and privileges are still handled internally.

d. Security management

The appliance is managed, including user management and the configuration of the router functions, through a Command Line Interface (CLI) protected by SSH. The CLI interface is accessible through SSH session, or via a local terminal console.

e. TOE Access function

The TOE can be configured by the user through use of packet filters such that users can only gain access from specific management networks/stations at specific IP addresses. All access attempts to the TOE require passing through an authentication mechanism.

f. Protection of Security Functions

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate before any administrative operations can be performed on the system, whether those functions are related to the management of user accounts or the configuration of routes. Another protection mechanism is that all routing functions of the TOE are confined to the appliance itself.

The TOE is completely self‐contained, and maintains its own execution domain as follows:

- Each sub-component of the appliance software operates in an isolated execution environment, protected from accidental or deliberate interference by others.
- The entire software environment is protected from accidental or deliberate corruption.

B 7.3 Vulnerability Analysis and Penetration testing

In search of potential vulnerabilities from public domain, scanning tools are used. Scanning was conducted to find out open ports and their vulnerabilities. OpenVas scanning tool is used with the latest feeds to find out hypothesized potential vulnerabilities present in the TOE.

The TOE documents like, Security Target (ST), TOE architecture & Design (TDS), TOE Preparatory guidance document etc. were analyzed to find out potential security vulnerability and the same is listed in.

The attack potential for each of the vulnerabilities was calculated using guidance given in CEMv3.1 and considering various factors like the time to identify & exploit the vulnerability, expertise required, knowledge of the TOE, windows of opportunity and equipment requirement.

Subsequent to the independent review of public domain vulnerability databases and all evaluation evidences, potential vulnerabilities were identified with their attack potentials. The potential vulnerabilities with '**Basic**' attack potential were considered for penetration testing.

The potential vulnerabilities with higher than 'Basic' attack potential are treated as residual vulnerabilities.

Penetration testing scenarios are summarized as below:

- TSF behavior in case of UDP flooding on SSR 8010 TOE environment
- TSF behavior in case of UDP flooding on SSR 8020 TOE environment
- TSF behavior in case of TCP flooding on SSR 8010 TOE environment
- TSF behavior in case of TCP flooding on SSR 8020 TOE environment
- Inheriting privileges or other capabilities that should otherwise be denied; i.e., whether users of different roles can escalate their privileges beyond their defined privileges as given in ST, bypassing implemented mechanism in SSR8010 environment
- Inheriting privileges or other capabilities that should otherwise be denied; i.e., whether users of different roles can escalate their privileges beyond their defined privileges as given in ST, bypassing implemented mechanism in SSR8020 environment
- TSF behavior in case of filling the Audit log in SSR8010 environment
- TSF behavior in case of filling the Audit log in SSR8020 environment

The penetration testing could not exploit any vulnerability in the intended operational environment of the TOE. However, these vulnerabilities may be exploited with higher attack potential.

B 8 Evaluation Results

The evaluation results have been documented in the [ETR].
The TOE was evaluated through evaluation of its documentation, site visit, testing and vulnerability assessment using methodology stated in [CEM] and laboratory operative procedure [OP-07].

Documentation evaluation results:
The documents for TOE and its development life cycle were analyzed by the evaluator in view of the requirements of the respective work units of the [CEM]. The final versions of the documents were found to comply with the requirements of CCv3.1 for EAL3.

Testing:
The developer's tests and the independent functional tests yielded the expected results, giving assurance that 'IPOS, Build Number IPOS Release 15.2 running on Ericsson Smart Service Routers, SSR 8020 / SSR 8010)' behaves as specified in its [ST], functional specification and TOE design.

Vulnerability assessment and penetration testing:
The penetration testing with '**Basic**' attack potential could not exploit the potential vulnerabilities identified through vulnerability assessment.

B 9 Validator Comments

The Validator has reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidences, documents, records, etc. and are in agreement with the conclusion made in it i.e.

- **The [ST] has satisfied all the requirements of the assurance class ASE.**
- **The results of evaluation of product and process documentation, testing and vulnerability assessment confirm that 'IPOS, Build Number IPOS Release 15.2 running on Ericsson Smart Service Routers, SSR 8020 / SSR 8010', satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for EAL3 Certification**.

However it should be noted that there are no **Protection Profile** compliance claims.

B 10 List of Acronyms

ACL: Access Control List
CC: Common Criteria
CCTL: Common Criteria Test Laboratory
CEM: Common Evaluation Methodology
DVS: Development security
EAL: Evaluation Assurance Level
ETR: Evaluation Technical Report
FSP: Functional Specification
IC3S: Indian Common Criteria Certification Scheme
IT: Information Technology
PP: Protection Profile
ST: Security Target
TOE: Target of Evaluation
TDS: TOE Design Specification
TSF: TOE Security Function
TSFI: TOE Security Function Interface

B 11 References

1. [CC-I]: Common Criteria for Information Technology Security Evaluation: Part 1: Version 3.1
2. [CC-II]: Common Criteria for Information Technology Security Evaluation: Part 2: Version 3.1
3. [CC-III]: Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1
4. [CEM]: Common Methodology for Information Methodology: Version 3.1
5. [ST] : Security Target for Ericsson Smart Service Router SSR 8020, SSR 8010 running IPOS Software, Revision PA12
6. [ETR]: Evaluation Technical Report No. STQC IT (KOL)/STQC/CC/1314/09/ETR/0658/v2.0
7. [OP-07]: CCTL operating procedure