Indian CC Certification Scheme (IC3S)

Certification Report

Report Number:	**STQC/CC/11-12/07/CR**
Product / system:	Router operating system: SEOS 11.1.2.3 , running on SE 100, SE 600, SE 1200 and SE 1200H hardware

Dated: 14 February 2013

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 Global Services Pvt Ltd, Ground Floor, West Wing, Salarpuria Supreme, Outer Ring Road, Marathahalli Junction, Bangalore – 560037
TOE evaluation sponsored by:	Ericsson India Private Limited, DLF Cyberciti, Sector 25A, Gurgoan – 122002, India
Evaluation facility:	Common Criteria Test Laboratory (CCTL), ERTL (East), DN-Block, Sector V, Salt Lake, Kolkata-700091, India.
Evaluation Personnel:	Tapas Bandopadhyay Malabika Ghose Subhendu Das
Evaluation report:	STQC IT (KOL)/STQC/CC/1112/07/ETRv1.0
Validation Personnel:	Alok Sain & B K Mondal

Contents

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, DLF Cyberciti, Sector 25A, Gurgoan – 122002, India
Developer	Ericsson India Global Services Pvt Ltd, Ground Floor, West Wing, Salarpuria Supreme, Outer Ring Road, Marathahalli Junction, Bangalore – 560037, India
Product and Version	SEOS V11.1.2.3 release no.:713
Security Target	Security target for Ericsson SmartEdge Series Router SE100, SE600, SE1200, SE1200H running SEOS ver 11.1 Software, Revision K
Brief description of product	The Target of Evaluation (TOE) is the Router Operating System, SEOS V11.1.2.3 release no.:713 running on SE 100, SE 600, SE 1200 and SE 1200H series router hardware. The router hardware act as environment to the TOE. The TOE is intended to protect the IP packets against incorrect routing caused by unauthorized changes in the network configuration. There are variations in 'hardware configuration' and 'performance' among the different models of the routers, as stated in ST. The variations are limited to the area of non–security functions of the routers, like processor, size of RAM, number of communication ports supported, number of available SIC slots etc. The TOE executable contains the operating system along with the software components required for specific hardware of the series.
CC Part 2 [CC-II]	Conformant
CC Part 3 [CC-III]	Conformant
EAL	EAL 3
Evaluation Lab	Common Criteria Test Laboratory, ERTL(E), Kolkata
Date Authorized	14th Feb 2013

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 service for evaluating the security functions or mechanisms of the IT products. It also provides a

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, and India. Hereafter this has been referred as CCTL. The evaluation facility is recognised under the IC3S scheme of STQC IT Certification Body.

The R&D center of Ericsson at Bangalore is the developer and Ericsson India Private Limited, Gurgoan is the sponsor.

The certification process is concluded with the completion of this certification report.

This evaluation was completed on 7th Feb 2013 after submission of [ETR] to the certification body. 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 B12 of this report. The TOE, SEOS V11.1.2.3 release no.:713 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

B1 Executive Summary

B 1.1 Introduction

The Certification Report documents the outcome of Common Criteria security evaluation of Router Operating System, SEOS V11.1.2.3 release no.:713 running on SE 100, SE 600, SE 1200 and SE 1200H series router hardware. 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, Ericsson and the Evaluation Technical Report [ETR] written by CCTL, ERTL (East), 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 (EAL 3) have been met.

B 1.2 Evaluated product and TOE

The product evaluated was:
The TOE is the Router Operating System, SEOS V11.1.2.3 release no.:713 running on SE 100, SE 600, SE 1200 and SE 1200H series router hardware. The router hardware acts as environment to the TOE.
The TOE is intended to protect the IP packets against incorrect routing caused by unauthorized changes in the network configuration.
There are variations in 'hardware configuration' and 'performance' among the different models of the routers, as stated in [ST]. The variations are limited to the area of non–security functions of the routers, like processor, size of RAM, number of communication ports supported, number of available SIC slots etc.
The TOE executable contains the operating system along with the software components required for specific hardware of the series.
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 B6).

B 1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter (Refer 4.1 of ST). Majority of the Security Functional Requirements (SFRs) (listed in 6.2 of ST) are taken from CC Part 2 and there are two extended SFRs related to requirement of 'protection of the TSF).

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/11-12/07 dated 18th Oct 2011.
The TOE as described in the [ST] is a dedicated router operating system running on the specified hardware platform.

The TOE was evaluated through evaluation of its documentation, site visit; testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM] and CCTL, Kolkata Operating Procedure OP-07.
The evaluation has been carried out under written agreement [dated 9-11-2011] between 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 IPv4 and evaluated routing protocols (BGP, OSPF & IS-IS) and other 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 TOE.

B 2 Identification of TOE

The TOE is identified as:
Router Operating System, SEOS V11.1.2.3 release no.:713 running on SE 100, SE 600, SE 1200 and SE 1200H series router hardware. There are two executable for these four environments in the form of **.tar.gz** files. The MD5 and CRC hash values of the **.tar.gz** files, are used to uniquely identify the different configurations of the TOE for which the evaluation result is valid.

B 3 Security policy

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

B 4 Assumptions

B 4.1 Personnel assumptions

Assumption code	Description
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.

B 4.2 Physical Environmental Assumptions

Physical Assumptions

Assumption code	Description
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

IT Environment Assumptions

Assumption code	Description
A.EAUTH	External authentication services will be available through either a RADIUS server or a TACACS server, or both.
A.TIME	The NTP server in the network is available.

B 5 Evaluated configuration

The TOE operates on four types of hardware. These entire four hardware environment were supplied by the developer. There are two executable for these four environments in the form of **.tar.gz** files as listed in the table below. One executable runs on SE100 and other runs on SE600, SE1200 and SE1200H environment. The **.tar.gz** files consist of SEOS V11.1.2.3 release no. 713 along with drivers depending on the environment of the router. The MD5 and CRC hash values of the **.tar.gz** files, are used to uniquely identify the different configurations of the TOE for which the evaluation result is valid. The TOE is configured on respective hardware platforms (IT environment) as per the preparatory guidance document of the TOE on the respective models for the purpose of evaluation.

The executable	Hardware(IT environment)	File size	MD5 Hash value for the executable	CRC hash value for the executable
SEOS-se100-11.1.2.3.713.tar.gz	SE100	58 MB	99a95a5bb5fb8c8d946ceb8bf40c2e69	OE229E8E
SEOS-mips-11.1.2.3.713.tar.gz	SE600, SE1200 and SE1200H	142 MB	4cb14057ad1d7cb06144b8a78a905bef	A7EB546A

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 for Ericsson SmartEdge Series Router SE100, SE600, SE1200, SE1200H running SEOS ver 11.1.2.3 Software, Revision K
2. Security Architecture of Ericsson SEOS 11.1, Revision A
3. SEOS 11.1 Functional specification, Revision D
4. Design Specification of Ericsson SEOS 11.1, Revision C
5. Operational User Guidance, Revision H
6. SEOS 11.1 Preparative procedures, Revision M
7. Configuration Management, Revision F
8. SEOS 11.1 Delivery Process, Revision D
9. Life Cycle Model, Revision D
10. Test Coverage for C. C. EAL3 Certification, Revision 3.0

11. Test Depth Analysis for C. C. EAL3, Revision 3.0
12. Test Plan for C. C. EAL3 Certification, Revision 7.0
13. Security Process, Revision D

B 6.2 Analysis of document

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

Development process: The evaluators analysed the functional specification of the TOE and found that the TOE security function interfaces are described clearly and unambiguously. The evaluators also analysed design and architectural documents of the TOE and determined that TOE subsystems are clearly described in the design document. The evaluators determined that architectural description of the TOE demonstrates secure initialization of the TOE and that is protected against tampering and bypassing. The architectural description also shows domain separation between data plane dealing with network traffic and control plane dealing with management traffic of the TOE.

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 and operational user guidance clearly gives steps to administer as well as to use the TOE.

Life-cycle support: The Life cycle support process documents like Configuration Management, Development Security and Delivery Procedure were evaluated.

Configuration management: The evaluators analysed configuration management documentation and determined that the TOE and its associated documents are clearly identified as configurable items. The evaluators also analysed access control measures defined in the documentation and found satisfactory. These documented procedures were audited during site visit of the development site of developer.

Development security: The development security document was analysed and found that it describes sufficient security measures for the development environment and those documented measures were audited by the evaluators during their site visit.

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.

The final version of the respective evaluation evidences were found to comply with the requirements of Common Criteria.

B 7 Product Testing

Testing at EAL 3 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 analyzed the developer's test coverage and depth 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: SEOS 11.1.2.3.713, running on Ericsson SmartEdge Series Routers, SE100, SE600, SE1200 and SE1200H, 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, SEOS 11.1.2.3.713, running on Ericsson SmartEdge Series Routers, SE100, SE600, SE1200 and SE1200H has been installed properly as per the preparative procedure AGD_PRE 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 defined in the security target, interfaces available to the users to cover each of security functional requirements, TOE design information and its security architecture. 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. Audit Function

The TOE creates and stores audit records for auditable events like:

- Start-up and shutdown of the audit function
- User login/logout
- Login failures
- Configuration is committed
- Configuration is changed

The objective of the test is to verify whether the TOE generates all auditable events as documented in the [ST], in the required format.

b. Protection of TSF through crypto function:

The TOE implements secure shell (SSH) as a remote access mechanism using DSA key generation and 168 bits 3DES or 128, 192 or 256 bits AES encryption. This protects all the management sessions initiated from remote client from eavesdropping. The objective of the test is to investigate the correctness of implementation of crypto algorithms, key management and the versions for SSH protocol.

c. Information flow function of user data protection

The TOE is designed primarily to route unauthenticated network traffic. Network traffic represents information flows between source and destination network entities. The specific routing of traffic is based on the routing configuration data that has been created by the TOE users or has been collected from network peers as defined by the TOE users.
The objective of the test is to verify whether the TOE is able to flow traffic as per defined ACL only.

d. Identification and authentication

The TOE offers local as well as remote authentication mechanism to be used for authenticated users. If the identity specified is defined locally, the TOE can successfully authenticate that identity if the authentication data provided matches that stored in conjunction with the provided identity. Alternatively,

if the TOE is configured to work with a RADIUS or TACACS server, the identity and authentication data is provided to the server and the TOE enforces the result returned from the server. Regardless, no administrative actions are allowed until successful authentication as an authorized administrator.
The objective of the test is to investigate authentication mechanism implemented in the TOE for local authentication and also compatibility with remote authentication servers.

e. Security management

The TOE restricts its management functions to authenticated users only depending on the users' privilege level. Mechanism which makes it possible is proper authorization of authenticated users. The user could be authorized through sending authorization request to local or external AAA servers & obtaining the authorization information for the user, and only after successful authorization of the privilege level associated with the user.
The objective of the test is to verify whether authorization mechanism is implemented properly in the TOE and the users get access to their defined privileges only. The test also focusses authentication mechanism implemented among peers and no unauthorized changes take place in routing table.

f. Protection of the TSF through clock function, self- test, trusted recovery, fail secure mechanism and domain separation functions

- The clock function of the TOE provides a source of date and time information for the appliance, used in audit timestamps. The function is reliant on the system clock provided by the underlying hardware. The TOE is also compatible with external NTP server.
- The TOE consists of a set of daemons, which implement the functions. These daemons are invoked by the process manager. The process Manager checks the integrity of the daemon binaries, before starting them up.
- The TOE implements trusted recovery during failure of some of its critical functions.
- The TOE implements fail secure mechanisms for Controller card failure (SE600, SE1200, and SE1200H only) and Process termination.
- The TOE offers clear separation of data and control/management plane at its architecture.

This test aims to verify mechanisms implemented for TSF protection.

g. TOE access function

The TOE restricts its management access to authenticated users only and can be configured to control access from specific IP for a specified numbers of simultaneous sessions. The TOE terminates a session after 10 minutes of inactivity.
This test aims to verify controls implemented to access the TOE.

B 7.3 Vulnerability Analysis and Penetration testing

In search of potential vulnerabilities, the evaluator has conducted public domain search, focussing on the type of the TOE. The listed vulnerabilities in the public domain for this type of TOE were analysed and a filtered list was prepared with those which are candidate for testing.

The TOE documents like, Security Target (ST), TOE architecture & Design (TDS), TOE Preparatory guidance document etc. were analysed to find out potential security vulnerabilities and the same were listed.
The attack potential for each vulnerability was calculated using guidance given in [CEM] 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:

- Escalation of privileges that should otherwise be denied
- Unauthorized reading , writing and modifying TSF data through FTP service
- Unauthorized reading of TSF data through TFTP service
- Denial of service in case of UDP flooding
- Denial of service in case of flooding with TCP malformed packets
- Resource exhaustion by filling the Audit log

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 EAL 3.
Site visit:
The TOE is developed at Ericsson, Bangalore and distributed through their software distribution gateway, SWGW.
The evaluators performed two 'Site Visits' at the development and distribution site in Bangalore. The objectives of the visits were to evaluate the respective work units for assurance classes related to configuration management, development security and delivery of the TOE. The requirements of Common Criteria for EAL 3 were found to be complied.
Testing:
The developer's tests and the independent functional tests yielded the expected results, giving assurance that SEOS 11.1.2.3 release no. 713 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 Validators have 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 the TOE, SEOS V11.1.2.3 release no. 713, satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for EAL 3 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 SmartEdge Series Router SE100, SE600, SE1200, SE1200H running SEOS ver 11.1.2.3 Software, Revision K
6. [ETR]: Evaluation Technical Report No. STQC IT (KOL)/STQC/CC/1112/07/ETR, Version No. 1.0
7. [OP-07]: CCTL operating procedure