Indian CC Certification Scheme (IC3S)

Certification Report

Report Number : IC3S/KOL01/ADVA/EAL2/0520/0021 /CR

Product / system : **Scalable Optical Transport Solution FSP 3000R7 Operating System (CC), Version R7 Rel.17.2.4**

Dated: 13th November 2020

Version: 1.0

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

Product developer:	ADVA OPTICAL NETWORKING SE, Fraunhoferstr.9a 82152 Martinsried, Munich, Germany
TOE evaluation sponsored by:	ADVA OPTICAL NETWORKING SE, Fraunhoferstr.9a 82152 Martinsried, Munich, Germany
Evaluation facility:	**Common Criteria Test Laboratory**, **ERTL (East**), 63 DN-Block, Sector V, Salt Lake, Kolkata-700091, India.
Evaluation Personnel:	**Evaluators:** Malabika Ghose & Manikanta Das **Test engineers:** Nischal, Sumit & Aniruddha Ghosh
Evaluation report:	IC3S/KOL01/ADVA/EAL2/0520/0021 /ETR/0020
Validation Personnel:	Tapas Bandyopadhyay, Scientist F, STQC, Govt. of India & A K Upadhyay Scientist F , STQC, Govt. of India

Table of Contents

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	ADVA OPTICAL NETWORKING SE, Fraunhoferstr.9a 82152 Martinsried, Munich, Germany
Developer	ADVA OPTICAL NETWORKING SE, Fraunhoferstr.9a 82152 Martinsried, Munich, Germany
The Target of Evaluation (TOE)	Scalable Optical Transport Solution FSP 3000 Operating System, version R7 Rel. 17.2.4 and its related guidance documentation. **TOE in short**: FSP 3000R7 Operating System (CC) **TOE Version**: R7 Rel.17.2.4
Security Target	FSP 3000R7 Operating System Release 17.2.4 Common Criteria Certification Security Target, version 2.0
Brief description of product	The FSP 3000 is a scalable optical transport solution, designed to respond to today's exploding bandwidth demands. It can be used by network/telecom service providers or in an enterprise environment. The modular design of the FSP 3000 ensures that networks are built on a flexible WDM foundation. The FSP 3000 represents Optical and Ethernet provisioning for seamless end-to-end connectivity from the access to the metro and on to long haul. The TOE is the operating system of the FSP 3000R7 system that can be found in the NCU-II card. The NCU-II provides system management capabilities and network connections to the FSP 3000R7 system.
Common Criteria Standard	Common Criteria Standard Version 3.1 Revision 5
CC Part 2 [CC-II]	Conformant with extended components
CC Part 3 [CC-III]	Conformant
EAL	EAL2
Evaluation Lab	Common Criteria Test Laboratory, ERTL(E), Kolkata, India
Date Authorized	13th November 2020

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/MeitY/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, Revision 5
- Common Evaluation Methodology (CEM) Version 3.1., Revision 5

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.

ADVA OPTICAL NETWORKING SE, Fraunhoferstr.9a 82152 Martinsried, Munich, Germany 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 25th September 2020 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 operating 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 [CCTL, ERTL (E)], ERTL (EAST), Block-DN Sector-V, Kolkata, India. 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 2**) have been met.

B 1.2 Evaluated product and TOE

The TOE consists of the operating system of the FSP 3000R7 system that can be found in the NCU-II card.

FSP 3000R7 Release 17.2.4 NCU Software.zip

SHA-256 2FAC5E5546AED6CD8211DA11261E7FEC762FED789650F887FE07F795F7E667DE

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 (Refer 3.3 and 4.1 of ST). All the Security Functional Requirements (SFRs) (listed in 6.1 of ST) are taken from CC Part 2 and also extended components are included.

B 1.4 Conduct of Evaluation

The evaluation was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. IC3S/KOL01/ADVA/EAL2/0520/0021 dated 22nd May 2020.
The TOE as described in the [ST] is the operating system of the FSP 3000R7 system that can be found in the NCU-II card. The NCU-II provides system management capabilities and network connections to the FSP 3000R7 system. The TOE was evaluated through evaluation of its documentation; testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM] and Common Criteria Test Laboratory, ERTL (E), Kolkata, Operating Procedure OP-07(CC EAL 4).
The evaluation has been carried out under written agreement [29th May 2020] between Common Criteria Test Laboratory, ERTL (E), 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.

B2 Identification of TOE

The TOE is the FSP 3000R7 Operating System (CC), Version R7 Rel.17.2.3, a scalable optical transport solution designed to respond to today's exploding bandwidth demands. It can be used by service providers or in an enterprise environment. The modular design of the FSP 3000 ensures that networks are built on a flexible WDM foundation. The FSP 3000 represents Optical and Ethernet provisioning for seamless end-to-end connectivity from the access to the metro and on to long haul.

Table 1: TOE components along with users' manuals

TOE Component	Description
NCU-II operating system	Part of the NCU-II card is the operating system of the FSP 3000R7 family. The evaluated NCU-II operating system is **Error! Reference source not found.**.
Users' Manual (AGD_OPE)	In addition, the following guidance documents are part of the TOE: • FSP3000R7_R17.2_Network_Element_Director_IssB.pdf • FSP3000R7_R17.2_Network_Element_Director_Quick_Start_Guide_IssA.pdf • FSP3000R7_R17.2_Provisioning_and_Operations_Manual_IssA.pdf • FSP3000R7_R17.2_Safety_Guide_IssB.pdf • FSP3000R7_R17.2_System_Description_IssB.pdf • FSP3000R7_R17.2_TL1_Commands_and_Syntax_Guide_IssA.pdf • FSP3000R7_R17.2_TL1_Maintenance_and_Troubleshooting_Manual_IssA.pdf • FSP3000R7_R17.2_TL1_Module_Parameters_Guide_IssA.pdf • FSP 3000R7_R17.2_Network_Hypervisor_User_Guide_IssA.pdf • FSP3000R7_R17.2_Hardware_Description_IssB.pdf • FSP3000R7_R17.2_High-Density_Subshelf_Guide_IssB.pdf • FSP3000R7_R17.2_Installation and Commissioning_Manual_IssB.pdf • FSP3000R7_R17.2_Maintenance_and_Troubleshooting_Manual_IssA.pdf • FSP3000R7_R17.2_Management_Data_Guide_IssB.pdf • FSP3000R7_R17.2_Module_System_Specification_IssB.pdf • FSP3000R7 Secure System Configuration Guide 17.2.4.pdf

Non-TOE Environment: The NCU-II must be installed in the master shelf and requires a shelf control unit (SCU, SCU-S, SCU-II) in each (master + any additional) shelf to communicate with the modules.

An NCU communicates with the SCU types in the master shelf using an internal system bus. Exchange of information between the SCU types in the master shelf and the SCU types in the additional shelves takes place over the management fiber ring.

Over the management network an administrative remote connection to the TOE (NCU-II operating system) can be stablished. The hardware on which the TOE runs is not under evaluation.

B3 Security policy

There are following organizational security policy that the TOE must meet.

Table 2: Organizational Security Policies

Threat	Description
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Table 3: Assumptions

Assumption	Description
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ST.
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the ST will not include any requirements on physical tamper protection or other physical attack mitigations. The ST will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

B.5 Evaluated configuration

The TOE is the operating system of the FSP 3000R7 system that can be found in the NCU-II card. The NCU-II is the second generation network element control (NCU) unit, using a higher performance processor than the first generation (NCU-A, NCU-B, NCU-GDPS and NCU). The NCU-II can be accessed through a serial, USB or Ethernet port. The Ethernet ports labeled C1 and C2 are female 8P8C (RJ-45) receptacles and can be used to connect the NCU-II to a

network management system or a management PC, either directly or via an external network, using standard Ethernet crossover cabling.

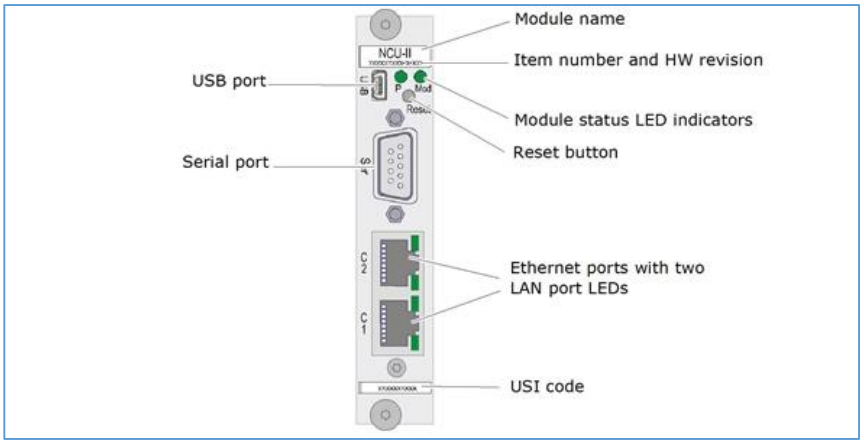

Figure 1: NCU-II card

FSP 3000R7 Release 17.2.4 NCU Software.zip
SHA-256 2FAC5E5546AED6CD8211DA11261E7FEC762FED789650F887FE07F795F7E667DE

Note:
Serial and USB connections have not been evaluated and are outside the scope of the certified usage.

B6 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**: FSP 3000R7 Operating System Release 17.2.4 Common Criteria Certification Security Target version 2.0, document number: 80000046683
2. **TOE Architecture:** FSP 3000R7 Operating System Security Architecture (ADV_ARC) ver. 1.1, document no.: 80000046685
3. **TOE Functional Specification:** FSP 3000R7 Operating System Common Criteria Certification Functional Specification, Ver. 1.8, document no.: 80000046684
4. **TOE Design description**: FSP 3000R7 Operating System Common Criteria Certification TOE Design, version 1.5, document no.: 80000046688
5. **Preparative Guidance**: Fiber Service Platform 3000R7 Secure System Configuration Guide release 17.2.4 Document Number: 80000045627
6. **Operational Guidance**: FSP 3000R7 AGD_OPE, Ver. 1.2
7. **Configuration Management Capability:** FSP 3000R7 ALC_CMC Revision: 1.4 document number:80000046691
8. **Configuration Management Scope:** FSP 3000R7 ALC_CMS, Ver. 1.3; Document Number: 80000046692
9. **TOE delivery:** FSP 3000R7 ALC_DEL, version 0.3
10. **Test cases, logs and coverage**: FSP 3000R7 Operating System Common Criteria Certification Test Documentation, version 2.1, doc. no.: 80000046694 and: FSP 3000R7 Operating System Common Criteria Certification Test Documentation, version 2.1, doc. no.: 80000046694

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 were 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 virtual 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 was found to comply with the requirements of CCv3.1 for EAL2.

B7 Product Testing

Testing at EAL2 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 analysed the developer's test coverage 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, ERTL(E), 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. Protected Communication

To ensure that sensitive data is transmitted to and from the TOE the TOE will provide encryption for these communication paths between themselves and the endpoint. These channels are implemented using following standard protocols:

- HTTPS (TLS), and
- SSH, and
- SNMPv3.

b. System Monitoring

The TOE has the capability of generating audit data targeted at detecting administrative activities. Auditing of administrative activities provides information that may hasten corrective action should the system be configured incorrectly. Audit of select system events can provide an indication of failure of critical portions of the TOE (e.g., a cryptographic provider process not running), repeated failures to establish sessions or authenticate to the system) of a suspicious nature.

c. TOE Administration

The TOE provides a password-based logon mechanism. The administrator has the capability to compose a strong password. To avoid attacks where an attacker might observe a password being typed by an administrator, passwords must be obscured during logon. Session locking or termination must also be implemented to mitigate the risk of an account being used illegitimately. Passwords must be stored in an obscured form, and there must be no interface provided for specifically reading the password or password file such that the passwords are displayed in plain text

d. TSF Self-test

In order to detect some number of failures of underlying security mechanisms used by the TSF, the TSF performs self-tests.

B 7.3 Vulnerability Analysis and Penetration testing

A scanning has been conducted on the TOE with following plugin set of the tool 'nessus' to find out presence of hypothesized potential vulnerabilities, identified in the public domain, pertaining to this type of product. Port map scanning has been carried out with 'NMap' tool. Based on the results of Port Scanning, web

application security Assessment tool 'Acunetix' used to find out web application security vulnerabilities, if any.

The evaluator has analyzed the evaluation evidences like, the ST, the Functional Specification, the TOE Design, the Security Architecture Description and the Guidance Documentation and as well as the operational environment, stated in the ST and then hypothesized the security vulnerabilities considering five categories of attack to the Security functions, viz. 'Bypassing', 'Tampering', 'Direct Attacks', 'Monitoring' and 'Misuse'.

Considering the type of the TOE and its intended use, the possibility of "Direct Attack" is negligible; evaluator's judgement is justified and supported by analysis. The evaluator has identified the following Attack scenarios.

AT1. Encrypted channel may be intercepted if attacker becomes successful to decrypt the encrypted channel.

AT2. Password may be accessed from storage if password is stored in clear text and remains accessible to the attacker.

AT3. 'Raima DB database module', containing TSF data may be accessed by the attacker by exploiting its vulnerabilities and subsequently make the TSF to fail.

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.

The relevant attack potentials, corresponding to the identified vulnerabilities have been estimated considering various factors like the 'time to identify & exploit', 'expertise required', 'knowledge of the TOE', 'windows of opportunity' and 'equipment required'. The potential vulnerabilities with '**Basic**' attack potential were considered for penetration testing. The calculated attack potentials are as follows:

AT1. Encrypted channel may be intercepted if attacker becomes successful to decrypt the encrypted channel. Attack Potential: 10 (Beyond Basic)

AT2. Password may be accessed from storage if password is stored in clear text and remains accessible to the attacker. Attack Potential: 8 (Within Basic)

AT3. 'Raima DB database module', containing TSF data may be accessed by the attacker by exploiting its vulnerabilities and subsequently make the TSF to fail. Attack Potential: 8 (Within Basic)

The evaluator conducted Penetration Testing (PT1 and PT2 respectively) for AT2 and AT3 and could not able to exploit the hypothesized Security vulnerabilities of the TOE evolved through analysis of evaluation objects. Hence, it is concluded that the TOE does not contain any exploitable vulnerability for 'Basic Attack Potential'.

B 8 Evaluation Results

The evaluation results have been documented in the [ETR].

Report No: IC3S/KOL01/ADVA/EAL2/0520/0021/ETR/0020

The TOE was evaluated through evaluation of its documentation, testing and vulnerability assessment using methodology stated in [CEM] and laboratory operative procedure [OP-07 CC EAL 4].

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 Revision 5 for EAL2.

Testing:

The developer's tests and the independent functional tests yielded the expected results, giving assurance that '**FSP 3000R7 Operating System (CC), Version R7 Rel.17.2.4 on the in the NCU-II card of FSP 3000R7**', 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] FSP 3000R7 Operating System Release 17.2.4 Common Criteria Certification Security Target Version 2.0 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 FSP 3000R7 Operating System (CC), Version R7 Rel.17.2.4 on the in the NCU-II card of FSP 3000R7, satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for EAL2 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, Revision 5
3. [CC-III]: Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1 Revision 5
4. [CEM]: Common Methodology for Information Methodology: Version 3.1 Revision 5
5. [ST] : FSP 3000R7 Operating System Release 17.2.4 Common Criteria Certification Security Target , Version 2.0
6. [ETR]: Evaluation Technical Report No. Report No: IC3S/KOL01/ADVA/EAL2/0520/0021/ETR/0020
7. [OP-07 CC EAL 4]: CCTL, ERTL(E) Operating procedure