PREMIER MINISTRE

General Secretariat for Defence and National Security

French Network and Information Security Agency

Certification Report ANSSI-CC-PP-2009/03

Protection Profile "Router with trusted embedded element"

(reference PP RECE, version 4.0)

Paris, the 21 December 2010

Courtesy Translation

Warning

This report testifies that the protection profile evaluated fulfill the evaluation criteria.
A protection profile is a public document which defined for a special product category a set of requirements and security objectives independently of the technology and the implementation.
The products defined from this protection profile satisfied the security needs from a common group of users.

Any correspondence about this report has to be addressed to:

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP
France

certification.anssi@ssi.gouv.fr

Certification report reference

ANSSI-CC-PP-2009/03

Protection profile name

Profil de Protection "Routeur avec élément de confiance embarqué"

"Router with trusted embedded element"

Protection profile reference

Reference PP RECE / version 4.0

Evaluation criteria and version

Common Criteria version 3.1

Evaluation level imposed by the PP

EAL 1 augmented

ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, AVA_VAN.2

Writer

Trusted Labs

5 rue du Bailliage, 78000 Versailles, France

Sponsor

Alcatel-Lucent France

Centre de Villarceaux, Route de Villejust, 91625 Nozay, France

Evaluation facility

Oppida

4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France

Tél : +33 (0)1 30 14 19 00, mail : cesti@oppida.fr

Recognition arrangements

CCRA

SOG-IS

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The French Network and Information Security Agency draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the sponsors desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site www.ssi.gouv.fr.

Contents

1. PRESENTATION OF THE PROTECTION PROFILE 6

1.1. PROTECTION PROFILE IDENTIFICATION 6
1.2. WRITER 6
1.3. PROTECTION PROFILE DESCRIPTION 6
1.4. FUNCTIONAL REQUIREMENTS 7
1.5. ASSURANCE REQUIREMENTS 8

2. EVALUATION 9

2.1. EVALUATION REFERENTIAL 9
2.2. SPONSORS 9
2.3. EVALUATION FACILITY 9
2.4. EVALUATION TASKS 9

3. CERTIFICATION 10

3.1. CONCLUSION 10
3.2. EUROPEAN RECOGNITION (SOG-IS) 10
3.3. INTERNATIONAL COMMON CRITERIA RECOGNITION (CCRA) 10

ANNEX 1. EVALUATION LEVEL OF THE PRODUCT 11

ANNEX 2. REFERENCES 12

1. Presentation of the protection profile

1.1. Protection profile identification

Title: Profil de Protection, Routeur avec élément de confiance embarqué.
Reference: PP RECE
Version: 4.0
Date: 8 December 2009

1.2. Writer

This protection profile has been written by:

Trusted Labs

5 rue du Bailliage
78000 Versailles
France

1.3. Protection profile description

The protection profile [PP], writen in the scope of the ESTER (***E**volution de la **S**écurité dans les **T**élécommunications et **E**quipements de **R**éseau* – Evolution of the Security in Telecommunications and Network Equipment) project, defines a set of security objectives and requirements, independent of the implementation, of a router which integrate a security module (a smartcard).

The main role of this router, called “ESTER router”, is the delivery of information between the different network nodes in a secure way. The smartcard integrated in this router allows improving the network infrastructures security, especially the authentication of management and control messages. It acts as an electronic strongbox. It protects the sensitive elements (protocol data, keys, …) within nodes of these infrastructures.

This solution provides a trust environment for the cryptographic keys generation and protection, the messages signature in order to their authentication, that is allow to protect itself against attacks aim at destroy or forge vital elements for the network functioning.

The target of evaluation defined in the protection profile [PP] allows providing a high security level for:

- the network infrastructure, by efficiently protecting management and control protocols (OSPF (Open Shortest Path First) keys, sorting table, …);
- the node itself, by allowing a security minimal mode where, even if the node has been attacked and that it is under the complete control of the attacker, some information will remain secret and protect by the smartcard. This thing, in order to avoid the attack propagats towards next networks.

1.4. Functional requirements

The security functional requirements which are identified in this protection profile are the following:

- Security alarms (FAU_ARP.1)
- Audit data generation (FAU_GEN.1)
- User identity association (FAU_GEN.2)
- Potential violation analysis (FAU_SAA.1)
- Audit review (FAU_SAR.1)
- Guarantees of audit data availability (FAU_STG.2)
- Cryptographic key generation (FCS_CKM.1)
- Cryptographic key destruction (FCS_CKM.4)
- Cryptographic operation (FCS_COP.1)
- Authentication failure handling (FIA_AFL.1)
- User authentication before any action (FIA_UAU.2)
- User identification before any action (FIA_UID.2)
- Management of security functions behaviour (FMT_MOF.1)
- Management of TSF data (FMT_MTD.1)
- Specification of management functions (FMT_SMF.1)
- Restriction of security roles (FMT_SMR.2)
- Replay detection (FPT_RPL.1)
- Reliable time stamps (FPT_STM.1)
- Inter-TSF trusted channel (FTP_ITC.1)
- Trusted path (FTP_TRP.1)

All these security functional requirements are extracted from Common Criteria part 2 [CC].

1.5. Assurance requirements

The assurance requirements required for this protection profile is **EAL 1 augmented with the following assurance requirements[1]:**

Components	Descriptions
ADV_ARC.1	Security architecture description
ADV_FSP.2	Security-enforcing functional specification
ADV_TDS.1	Basic design
ASE_OBJ.2	Security objectives
ASE_REQ.2	Derived security requirements
ASE_SPD.1	Security problem definition
AVA_VAN.2	Vulnerability analysis

Tableau 1 - Augmentations

All these security assurance requirements are extracted from Common Criteria part 3 [CC].

[1] **Erreur ! Source du renvoi introuvable.**: table of different evaluation assurance levels (EAL – Evaluation Assurance Level) predefined in the Common Criteria [CC].

2. Evaluation

2.1. Evaluation referential

The evaluation has been conducted in accordance with the **Common Criteria standard version 3.1** [CC] and the evaluation methodology defined within the CEM [CEM].

2.2. Sponsor

Alcatel-Lucent France

Centre de Villarceaux
Route de Villejust
91625 Nozay
France

2.3. Evaluation facility

OPPIDA

4-6 avenue du vieil étang
Bâtiment B
78180 Montigny le Bretonneux
France

Phone : +33 (0)1 30 14 19 00

Mail: cesti@oppida.fr

2.4. Evaluation tasks

The evaluation technical report [ETR], delivered to ANSSI the 9 December 2009, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality for a licensed evaluation facility. All the work performed permits the release of a certificate in conformance with the decree 2002-535.

3.2. European recognition (SOG-IS)

This certificate is issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].
The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

3.3. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[2], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Switzerland and United Kingdom.
2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Pakistan, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

Annex 1. Evaluation level of the product

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 1+	Name of the component
ADV Development	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**2**	Security-enforcing functional specification
	ADV_IMP				**1**	1	**2**	2		
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**1**	Basic design
AGD Guidance	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**1**	Labelling of the TOE
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**1**	TOE configuration management coverage
	ADO_DEL		**1**	1	1	1	1	1		
	ALC_DVS			**1**	1	1	**2**	2		
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**		
	ALC_TAT				**1**	**2**	**3**	3		
ST Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3		
	ATE_DPT			**1**	**2**	**3**	3	**4**		
	ATE_FUN		**1**	1	1	1	**2**	2		
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**1**	Independent testing - conformance
AVA Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**2**	Vulnerability analysis

Annex 2. References

Decree number 2002-535 dated 18th April 2002 related to the security evaluations and certifications for information technology products and systems.	
[CPP/P/01]	Procedure CPP/P/01 – Protection profiles certification, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[PP]	Profil de protection « Routeur avec élément de confiance embarqué », Reference: PP RECE, version 4.0 dated from 8 December 2009, Trusted Labs
[RTE]	Evaluation Technical Report, ESTER Project – APE evaluation task, Reference: OPPIDA/CESTI/PP-ESTER/APE/4.0 dated from 09/12/2009, Oppida