PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-PP-2009/03

Profil de Protection « Routeur avec élément de confiance embarqué » (référence PP RECE, version 4.0)

Paris, le 21 décembre 2009

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

Avertissement

Ce rapport atteste la conformité de la version évaluée du profil de protection aux critères d'évaluation.
Un profil de protection est un document public qui définit, pour une catégorie de produits, un ensemble d'exigences et d'objectifs de sécurité, indépendants de leur technologie et de leur implémentation, qui satisfont les besoins de sécurité communs à un groupe d'utilisateurs.

Toute correspondance relative à ce rapport doit être adressée au :

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

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-PP-2009/03

Nom du profil de protection

Profil de Protection « Routeur avec élément de confiance embarqué »

Référence/version du profil de protection

Référence PP RECE / version 4.0

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation imposé par le PP

EAL 1 augmenté

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

Rédacteur

Trusted Labs

5 rue du Bailliage, 78000 Versailles, France

Commanditaire

Alcatel-Lucent France

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

Centre d'évaluation

Oppida

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

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

Accords de reconnaissance applicables

CCRA

SOG-IS

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Table des matières

1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : Profil de Protection, Routeur avec élément de confiance embarqué
Référence : PP RECE
Version : 4.0
Date : 8 décembre 2009

1.2. Rédacteur

Ce profil de protection a été rédigé par :

Trusted Labs

5 rue du Bailliage
78000 Versailles
France

1.3. Description du profil de protection

Le profil de protection [PP], rédigé dans le cadre du projet ESTER (**E**volution de la **S**écurité dans les **T**élécommunications et **E**quipements de **R**éseau), définit un ensemble d'objectifs et d'exigences de sécurité, indépendant de l'implémentation, d'un routeur intégrant un module de sécurité (une carte à puce).

Le rôle principal de ce routeur, appelé « routeur ESTER », est l'acheminement des informations entre les différents nœuds du réseau d'une manière sécurisée. La carte à puce intégrée dans ce routeur permet d'améliorer la sécurité des infrastructures réseau, notamment l'authentification des messages de gestion et de contrôle. Elle agit comme un coffre-fort électronique. Elle protège les éléments sensibles (données de protocole, clés, …) au sein même des noeuds de ces infrastructures.

Cette solution assure un environnement de confiance pour la génération, la protection des clés cryptographiques, la signature des messages en vue de leur authentification, ce qui permet de se protéger contre des attaques visant à détruire et falsifier les éléments vitaux pour le fonctionnement du réseau.

La cible d'évaluation définie dans le profil de protection [PP] permet d'assurer un niveau élevé de sécurité pour :

- l'infrastructure réseau, en protégeant efficacement les protocoles de gestion et de contrôle (clés OSPF (*Open Shortest Path First*), tables de routage, …) ;
- le noeud lui-même, en permettant un mode minimal de sécurité où, même si le noeud a été attaqué et qu'il est sous contrôle complet de l'attaquant, certaines informations resteront secrètes et protégées par la carte à puce. Ceci afin d'éviter que l'attaque se propage vers les réseaux voisins.

1.4. Exigences fonctionnelles

Les **exigences fonctionnelles de sécurité** définies par le profil de protection sont les suivantes :

- 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)

Toutes les exigences fonctionnelles du profil de protection sont extraites de la partie 2 des Critères Communs [CC].

1.5. Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau **EAL1 augmenté des composants d'assurance suivants**[1] :

Composants	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

Toutes les exigences d'assurance imposées par le profil de protection sont extraites de la partie 3 des Critères Communs [CC].

[1] Voir l'Annexe 1 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Commanditaire

Alcatel-Lucent France

Centre de Villarceaux
Route de Villejust
91625 Nozay
France

2.3. Centre d'évaluation

OPPIDA

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

Téléphone : +33 (0)1 30 14 19 00

Adresse électronique : cesti@oppida.fr

2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 9 décembre 2009, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation relatives à la classe d'exigences d'assurance APE sont à « **réussite** ».

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

3.2. Reconnaissance européenne (SOG-IS)

Ce rapport de certification est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3. Reconnaissance internationale (CC RA)

Ce rapport de certification est émis dans les conditions de l'accord du CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni, la Suède.
[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 1+	Intitulé du composant
ADV Développement	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 Guides d'utilisation	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 Support au cycle de vie	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		
ASE Evaluation de la cible de sécurité	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**	1	**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 Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**2**	Vulnerability analysis

Annexe 2. Références

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CPP/P/01]	Procédure CPP/P/01 Certification de profils de protection, 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 » Réf : PP RECE, version 4.0 du 8 décembre 2009 Trusted Labs
[RTE]	Rapport technique d'évaluation, Projet ESTER – Tâche d'évaluation APE, référence OPPIDA/CESTI/PP-ESTER/APE/4.0 du 09/12/2009. OPPIDA