PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2016/68

Fonctions de pare-feu et de VPN des équipements Arkoon FAST360 version 6.0

Paris, le 26 octobre 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

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

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2016/68

Nom du produit

Fonctions de pare-feu et de VPN des équipements Arkoon FAST360 version 6.0

Référence/version du produit

ARKOON FAST360, version 6.0/9

Conformité à un profil de protection

[PP FWIP] : Profil de protection Firewall d'interconnexion IP, version 2.2, 10 mars 2006

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 3 augmenté

ALC_FLR.3, AVA_VLA.2

Développeur(s)

Stormshield

1 place Verrazzano

69009 Lyon

Commanditaire

Stormshield

10 rue Marceau

92130 Issy-les-Moulineaux

Centre d'évaluation

Oppida

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

Accords de reconnaissance applicables

CCRA

Le produit est reconnu au niveau EAL3 et ALC_FLR.3

SOG-IS

Le produit est reconnu au niveau EAL3 et ALC_FLR.3

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 modifié. 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 disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est le logiciel FAST360, en version 6.0/9, embarqué dans les *appliances* UTM Arkoon FAST360 ; il s'agit d'un ensemble de logiciels développés et intégrés par la société *STORMSHIELD* et comprenant :

- des services d'authentification, d'administration, d'audit, d'échange de clés (IKE) ;
- un Centre d'Elaboration des Clés (hors du périmètre de l'évaluation) ;
- le noyau du système d'exploitation ;
- différents modules : IP *Stack*, IPSEC *Stack*, FAST *Engine*, IP *Packet filter*, *Transport Layer filters*, *Applicative layer filters* assurant les fonctionnalités de pare-feu et de VPN du logiciel FAST360.

1.2. Description du produit

1.2.1. Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme au profil de protection [PP FWIP] : Profil de protection Firewall d'interconnexion IP, version 2.2 du 10 mars 2006, certifié le 10 octobre 2006 sous la référence PP 2006/05.
La cible de sécurité s'inspire du profil de protection [PP CIP] : Profil de protection Chiffreur IP.

1.2.2. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est la version 6.0/9 ; elle est identifiable par les éléments suivants :

Elément	Version	Plateforme	Identification
Carte mémoire			dans le fichier /etc/arkoon_version
Arkoon Manager	20150623154748	Linux	dans le menu « Aide → A propos … »
	20150623170612	Windows/Java 1.7	
	20150623163341	Windows/Java 1.6	
Arkoon Monitoring	6.0.150623.1547	Linux	« ? → A propos d'Arkoon Monitoring »
	6.0.150623.1727	Windows/Java 1.7	
	6.0.150623.1727	Windows/Java 1.6	
Guide de première configuration	6.0/4 – 20140617_1600		sur la page de garde
Guide d'administration	6.0/4 – 20140617_1600		sur la page de garde

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par la TOE sont :

- des services d'administration :
  - la gestion des comptes d'administration ;
  - la définition des politiques de sécurité ;
  - la journalisation et l'audit des opérations d'administration ;
  - la supervision de l'état de la TOE ;
  - la gestion des clés cryptographiques ;
- l'application de la politique de sécurité VPN, incluant :
  - la protection en confidentialité des données applicatives ;
  - la protection de l'authenticité des données applicatives ;
  - la protection en confidentialité des données topologiques ;
  - la protection de l'authenticité des données topologiques ;
  - le cloisonnement des flux en divisant un réseau privé en plusieurs sous-réseaux ;
- l'application de la politique de filtrage du pare-feu ;
- l'audit et la journalisation des flux ;
- la réinitialisation et l'effacement sécurisé des données sensibles.

1.2.4. Architecture

Le logiciel Arkoon FAST360 est constitué des éléments suivants :

- le système « Administration », qui permet de réaliser des opérations d'administration d'un parc d'*appliance* FAST360 ; ce système est lui-même composé :
  - du sous-système « Arkoon Manager », qui permet de gérer la configuration de l'*appliance* FAST360, dont notamment la configuration des composants qui mettent en oeuvre les politiques de sécurité définies par l'administrateur ;
  - du sous-système « Arkoon Monitoring », qui permet de superviser l'appliance FAST360, c'est à dire de consulter/supprimer les journaux et alertes liés au trafic réseau et aux règles de sécurité établies par l'administrateur ;
- le système « Firewall » (FAST Engine), qui assure l'application des règles de filtrage, définies par le système « Administration », au trafic réseau transitant par l'*appliance*. Ce système « Firewall » s'appuie sur le moteur FAST (*Fast Applicative Shield Technology*) ;

- le système VPN (*Virtual Private Network*), qui offre la possibilité à des hôtes distants, statiques ou nomades, d'établir des tunnels IPSec avec l'appliance FAST360.

La figure 1 illustre la TOE dans son environnement :

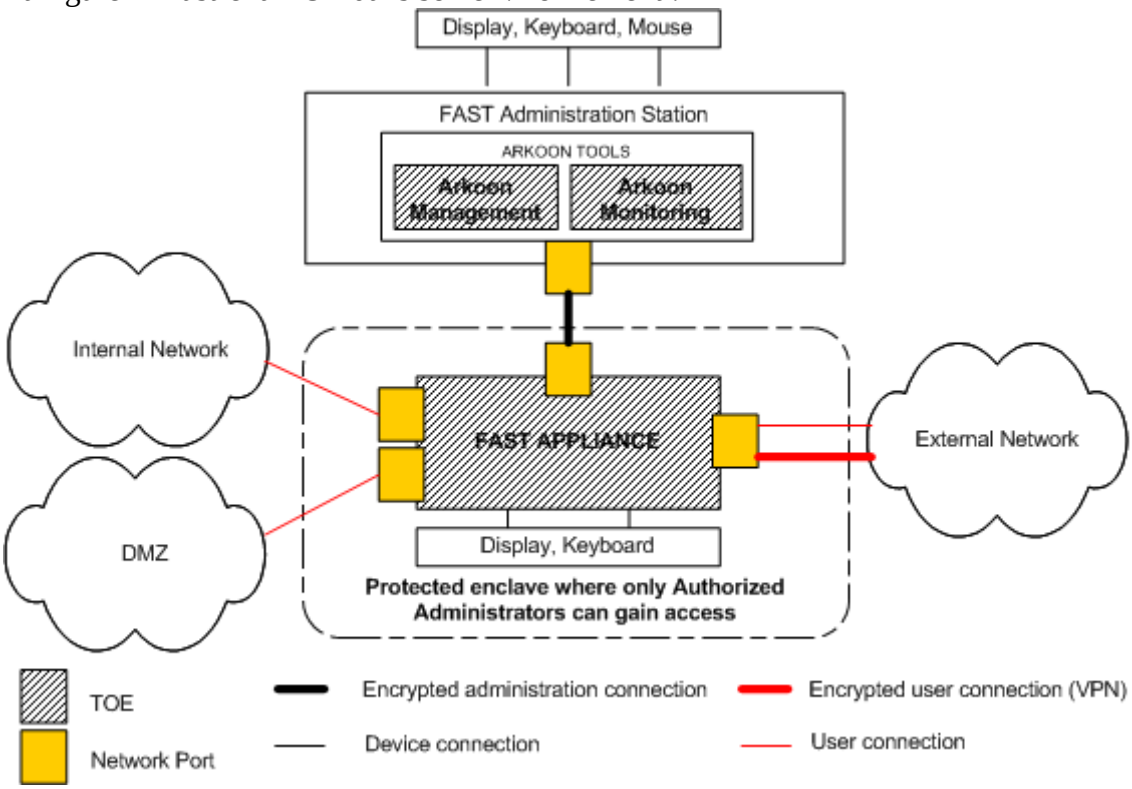

Figure 1 : périmètre et interfaces de la TOE

L'appliance UTM Arkoon FAST360 est dotée de quatre interfaces réseau :

- une interface d'administration, qui relie l'appliance à sa station d'administration pour permettre son administration à distance ;
- une interface réseau externe, qui relie l'appliance à un réseau externe, considéré comme non-sûr (Internet par exemple) ;
- une interface réseau interne qui relie l'appliance au réseau interne : le réseau protégé par l'appliance ;
- une interface réseau DMZ, qui relie l'appliance à un réseau DMZ où seules les machines devant être visibles depuis le réseau externe sont présentes.

1.2.1. Cycle de vie

Le produit a été développé sur le site suivant :

STORMSHIELD
1 place Verrazzano
69009 Lyon
France

Les rôles suivants identifiés dans la cible de sécurité sont considérés dans le cadre de l'évaluation comme des « Utilisateurs » des fonctions de sécurité de la TOE :

- L'utilisateur du réseau protégé (par le pare-feu) utilise les fonctionnalités de *firewalling* via les interfaces réseau interne, externe et DMZ ;

- L'utilisateur du réseau privé (via une liaison VPN IPSEC) utilise les fonctions de sécurité suivantes :
    - F.USER_DATA_PROTECTION_FW via les interfaces réseau interne, externe et DMZ ;
    - F.USER_DATA_PROTECTION_VPN via l'interface réseau externe sur les ports UDP/500 et UDP/4500. Deux cas d'utilisation sont admis par la TOE ; à savoir l'établissement d'un tunnel LAN-to-LAN ou Host-to-LAN. Le premier cas concerne l'administrateur ayant les droits de configurer une connexion vers un autre dispositif VPN. Il s'agit d'une fonction d'administration officiant de la même manière qu'un client logiciel tiers.

L'évaluateur considère que le service de pare-feu offert par la TOE est passif pour un utilisateur de réseau protégé ; cet utilisateur n'a aucune interaction particulière avec la TOE pour ce service.

Les rôles suivants identifiés dans la cible de sécurité sont considérés dans le cadre de l'évaluation comme des « Administrateurs » des fonctions de sécurité de la TOE :
- responsable sécurité ;
- administrateur système et réseau ;
- superviseur système et réseau ;
- administrateur sécurité ;
- superviseur sécurité ;
- auditeur ;
- rôle « toutes autorisations ».

Un administrateur peut combiner plusieurs de ces rôles.

1.2.2. Configuration évaluée

Le certificat porte sur la configuration au niveau de sécurité maximal, tel que décrit au chapitre 1.3.9 du guide de première configuration du produit (voir [GUIDES]), en utilisant l'application *minarkconf*.

La figure 2 illustre la plateforme de tests mise en œuvre dans le cadre de cette évaluation :

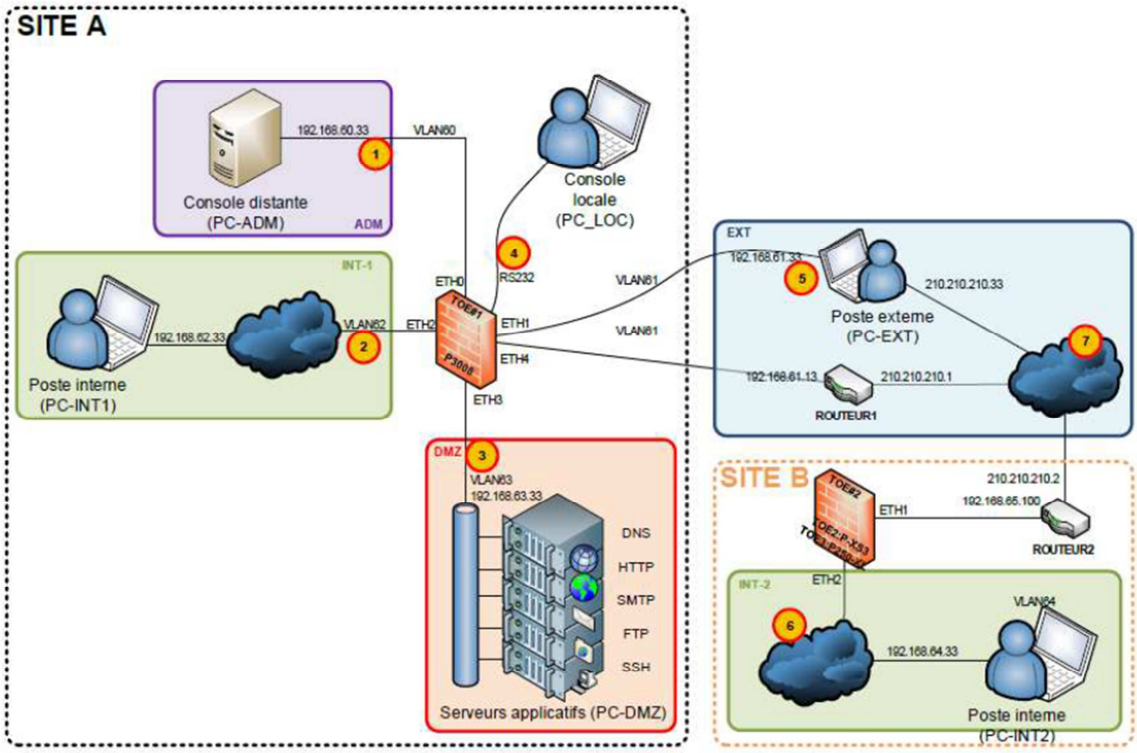

Figure 2 : Plateforme de tests

Les tests réalisés dans le cadre de cette évaluation ont porté sur les *appliances* ARKOON P-XS3, P3008 et P-250XL, de la série *Performance*, selon l'architecture réseau illustrée par la Figure 3.

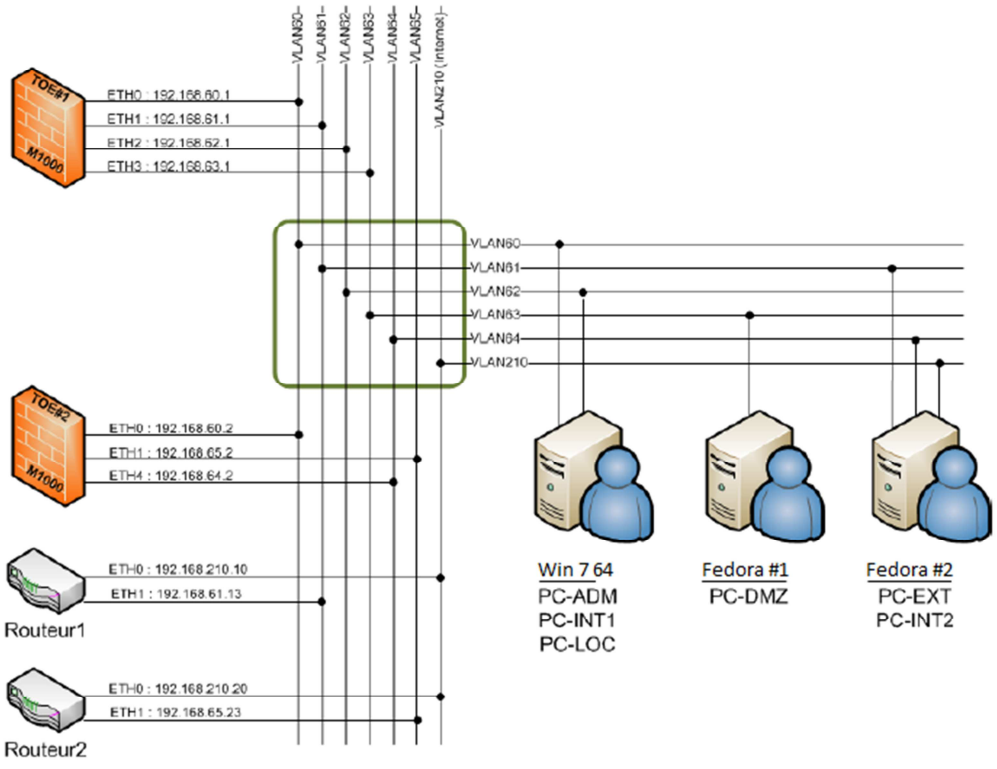

Figure 3 : architecture réseau de la plateforme de tests

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 10 octobre 2016, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Dans le cadre du processus de qualification standard, la cotation des mécanismes cryptographiques (rapport [ANA-CRY]) et l'expertise de l'implémentation de la cryptographie (rapport [EXP-CRY]) ont été réalisées. Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VLA visé.

Le produit FAST360 autorise un grand nombre d'algorithmes cryptographiques et de tailles de clés à des fins de compatibilité avec des produits existants. Il est toutefois vivement recommandé de n'utiliser que les algorithmes et les tailles de clés suivants, proposés par défaut par le produit:

- *Diffie-Hellman* avec des clés d'au minimum 2048 bits (groupes 14, 15 et 16) ;
- RSA avec des clés d'au minimum 2048 bits ;
- AES-CBC avec des clés de 256 bits ;
- HMAC SHA-2.

2.4. Analyse du générateur d'aléas

Les mécanismes de génération d'aléas suivants ont été analysés dans le cadre de cette évaluation (rapports [ANA-CRY] et [EXP-CRY]) :

- génération d'aléas pour la mise en œuvre du protocole IKE : non conforme au RGS ;
- génération d'aléas pour la mise en œuvre du protocole ESP : conforme au RGS ;
- génération d'aléas pour la mise en œuvre du protocole TLS : conforme au RGS.

Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VLA visé.

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.

Ce certificat atteste que le produit « Fonctions de pare-feu et de VPN des équipements ARKOON FAST360 version 6.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants ALC_FLR.3 et AVA_VLA.2.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra configurer le produit selon le niveau de sécurité maximal, comme décrit au chapitre 1.3.9 du guide de première configuration du produit (voir [GUIDES]), à l'aide de l'application *minarkconf*, et s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST] :

- l'exploitation du produit doit être réalisée conformément aux référentiels cryptographique de l'ANSSI [REF-CRY], [REF-KEY] et [REF-AUT], notamment concernant la génération et la gestion des clés réalisées hors TOE (OE.CRYPTO, OE.VPN.CRYPTO_EXT) ;
- les équipements sur lesquels le produit est déployé (appliances et postes d'administration), ainsi que tous les supports contenant des biens sensibles du produit (papier, disquettes, sauvegardes, etc.) doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs (OE.PROTECTION_LOCAL) ;
- l'initialisation des équipements sur lesquels le produit est déployé doit être réalisée à partir de postes d'administration directement connectée sur les équipements et dans le local protégé de l'appliance (OE.INITIALISATION_LOCAL) ;
- les administrateurs doivent être de confiance (OE.ADMIN) ;
- les événements d'audit et les alarmes de sécurité générés par le produit doivent être analysés régulièrement (OE.FW.ANALYSE_AUDIT, OE.VPN.ANALYSE_AUDIT, OE.FW.TRAITE_ALARMES, OE.VPN.TRAITE_ALARMES) ;
- les événements d'audit et les alarmes de sécurité générés par le produit doivent faire l'objet de mesures de sauvegarde et d'archivage (OE.FW.ANALYSE_AUDIT, OE.VPN.ANALYSE_AUDIT) ;
- l'environnement du produit doit permettre d'authentifier les administrateurs sur les postes d'administration (OE.AUTHENTIFICATION_ADMIN_DISTANT) ;
- l'administrateur doit disposer de moyens de contrôler la configuration matérielle et logicielle de l'appliance par rapport à un état de référence (OE.FW.INTEGRITE, OE.VPN.INTEGRITE).

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

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

L'accord de reconnaissance européen du SOG-IS de 2010 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 E3 Elémentaire et CC EAL4 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Le produit est reconnu au niveau EAL3 et ALC_FLR.3

3.3.2. Reconnaissance internationale critères communs (CCRA)

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs.
Pour les évaluations enregistrées avant septembre 2014, la reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR lorsque les dépendances CC sont satisfaites.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Le produit est reconnu au niveau EAL3 et ALC_FLR.3

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et 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, le Qatar, 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 3+	Intitulé du composant
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2		
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**3**	Authorisation controls
	ACM_SCP			**1**	**2**	**3**	3	3	**1**	TOE CM coverage
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**1**	Delivery procedures
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**1**	Informal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3		
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2		
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3		
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic Flow remediation
	ALC_LCD				**1**	**2**	2	**3**		
	ALC_TAT				**1**	**2**	**3**	3		
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-level design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing – sample
AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**1**	Examination of guidance
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *ARKOON FAST360 6.0 Common Criteria Security Target Level EAL3+*, référence : ST_ARKOON_FAST360_60, version 3.1, du 13 octobre 2015, *STORMSHIELD*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *ARKOON FAST360 6.0 Version 6.0/9 Common Criteria Security Target Level EAL3+*, référence : ST_ARKOON_FAST360_60, version 3.1.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation Projet CHILUNG, Référence : OPPIDA/CESTI/CHILUNG/RTE/2.0, version 2.0 du 10 octobre 2016, *OPPIDA*.
[ANA-CRY]	Cotation des mécanismes cryptographiques Qualification Mehetia, référence : N° 2912 /ANSSI/ACE, 18 novembre 2010.
[EXP-CRY]	Analyse des mécanismes cryptographiques, référence : OPPIDA/CESTI/CHILUNG/CRYPTO/1.0, version 1.0 du 25 avril 2016, *OPPIDA*.
[CONF]	Liste documentaire : - Liste des documents, référence : AKV6-LIST-DOCS-CERTIF, version 3.3, 13 octobre 2015, *STORMSHIELD*. Liste de configuration logicielle : - Liste-configuration_system.txt, version 1.0 ; - Liste-configuration_tools.txt, version 1.0. Release Note : - ARKOON FAST360/AMC Release Notes 6.0/9, référence : Release_Notes_FAST360_6_0_9_FR, septembre 2015, *STORMSHIELD*.
[GUIDES]	Guides d'administration et d'installation du produit : - « ARKOON FAST360 6.0/9 – Guide de Première Configuration », référence 20160425_1600, avril 2016 ; - « ARKOON FAST360 6.0/9 – Guide d'administration », référence 20160425_1600, avril 2016.
[PP_CIP]	« Profil de protection Chiffreur IP », référence PP-CIP, version 1.5, 3 février 2005. Ce PP n'est pas certifié.
[PP_FWIP]	« Profil de protection Firewall d'interconnexion IP », référence PPFWIP, version 2.2, 10 mars 2006. Certifié par l'ANSSI sous la référence PP 2006/05.

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, août 2005, version 2.3, référence CCMB-2005-08-001; Part 2: Security functional requirements, août 2005, version 2.3, référence CCMB-2005-08-002; Part 3: Security assurance requirements, août 2005, version 2.3, référence CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, août 2005, version 2.3, référence CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, septembre 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.
	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), voir www.ssi.gouv.fr.