Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-CSPN-2010/01

Logiciel UCOPIA pour boîtiers appliances UCOPIA version 3.0 release 5

Paris, le 22 Février 2010

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2010/01**
Nom du produit **Logiciel UCOPIA pour boîtiers appliances UCOPIA**
Référence/version du produit **Version 3.0 Release 5**
Critères d'évaluation et version **CERTIFICATION SECURITE DE PREMIER NIVEAU (CSPN, Phase expérimentale)**
Développeur(s) **UCOPIA Communications** **99 rue Pierre Sémard** **92324 Chatillon Cedex** **France**
Commanditaire **UCOPIA Communications** **99 rue Pierre Sémard** **92324 Chatillon Cedex** **France**
Centre d'évaluation **THALES** **BPI 1414 18, avenue Edouard Belin 31401 Toulouse Cedex 9, France** **Tél : +33 (0)5 62 88 28 01, mél : nathalie.feyt@thalesgroup.com**

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 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 UCOPIA pour boîtiers appliances UCOPIA version 3.0 »**,** développé par la société UCOPIA Communications.

Le logiciel UCOPIA permet la gestion de la mobilité et la sécurisation des accès au sein des réseaux sans fil Wi-Fi et filaires.

Deux familles de fonctions sont proposées par le logiciel UCOPIA : les fonctions de sécurité et les fonctions de mobilité.

- **Sécurité :** le logiciel UCOPIA propose une authentification des utilisateurs nomades basée sur une architecture 802.1x et sur un serveur RADIUS. L'appliance transmet les clés de chiffrement négociées à l'issue de l'authentification au point d'accès Wi-Fi, permettant ainsi à l'utilisateur de bénéficier d'une liaison chiffrée selon les protocoles WPA ou WPA2 qui garantissent la confidentialité des communications. Un mode d'authentification basé sur HTTPS et sur un portail Web (login / mot de passe) est également proposé afin d'accueillir les visiteurs. Le logiciel UCOPIA permet de définir et de contrôler finement les droits d'accès en prenant en compte l'identité de l'utilisateur, la nature du service demandé, le lieu et l'heure de la demande. De plus, le logiciel UCOPIA assure une traçabilité du trafic des utilisateurs.
  Le logiciel UCOPIA peut s'interfacer avec un ou plusieurs annuaires LDAP, s'intègre avec les architectures VLANs et peut cohabiter avec d'autres solutions de sécurité en place (RADIUS, Domaine Windows, PKI, etc.).

- **Mobilité :** le logiciel UCOPIA permet de définir les politiques de mobilité de l'entreprise ou de l'organisation puis de les mettre en œuvre sur les différents sites concernés. Il permet à l'utilisateur nomade d'accéder en tout lieu aux services autorisés de façon simple et transparente (l'utilisateur n'a pas à reconfigurer ses différentes applications réseaux, telles que la messagerie, son navigateur Web, son poste de travail, lorsqu'il se déplace d'un réseau à un autre) et de bénéficier d'une qualité de service nécessaire à la bonne exécution de ses applications.

Le logiciel UCOPIA fournit deux outils d'administration accessibles via une interface Web. L'un est dédié à l'administrateur du réseau et autorise l'ensemble des fonctions d'administration, l'autre a des prérogatives plus restreintes et est dédié à des administrateurs délégués.

1.2 Description du produit évalué

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

1.2.1 Catégorie du produit

1 - détection d'intrusion
2 - anti-virus, protection contre les codes malicieux
3 – pare-feu
4 - effacement de données
5 - administration et supervision de la sécurité
6 - identification, authentification et contrôle d'accès
7 - communication sécurisée
8 - messagerie sécurisée
9 - stockage sécurisé
10 - matériel et logiciel embarqué
99-Autres

1.2.2 Identification du produit

Le numéro de version et la dénomination du produit apparaissent sur la page d'accueil de l'interface Web d'administration du produit.

1.2.3 Services de sécurité

Authentification

Le produit propose plusieurs modes d'authentification des utilisateurs, allant d'une authentification basée sur le protocole 802.1x/EAP jusqu'à une authentification de type portail Web captif basée sur HTTPS. Ces différents modes d'authentification cohabitent dans un même réseau, éventuellement sous différents réseaux logiques (VLAN), chacun correspondant à différentes catégories d'utilisateurs. Les mots de passe des utilisateurs sont créés à l'aide du module d'administration.

Contrôle d'accès par filtrage de flux

Le contrôle d'accès des utilisateurs doit s'exercer de manière fine, en fonction de l'utilisateur et de ses droits. Pour ce faire, le produit est placé en position de coupure réseau et utilise un mécanisme de filtrage de trafic basé sur des règles. Celles-ci sont automatiquement déduites du profil de l'utilisateur et du contexte de la connexion (notamment l'heure et lieu de connexion).

Cloisonnement VLAN

Le logiciel offre la possibilité d'utiliser des réseaux locaux privés virtuels (VLAN). En installant le produit, l'administrateur doit pouvoir continuer à bénéficier des mécanismes d'isolation des VLAN mis en place sur le réseau existant.

Traçabilité

Le produit enregistre et sauvegarde deux types d'informations : les informations de sessions des utilisateurs (qui s'est connecté et quand ?) et les informations de trafic (qui a fait quoi ?).

Administration
Le produit contrôle l'accès aux opérations d'administration de la sécurité.

Télémaintenance sécurisée de l'appliance

Les communications entre l'appliance et le support UCOPIA destinées à la mise à jour du produit et à sa maintenance à distance sont authentifiées et protégées en confidentialité.

1.2.4 Configuration évaluée

La configuration évaluée correspond au logiciel UCOPIA version 3.0 exécuté sur le modèle de boîtier appliance UCOPIA Advance 100.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément au référentiel « Certification de Sécurité de Premier Niveau en phase expérimentale ». Les références des documents se trouvent en annexe 2.

2.2 Charge de travail prévue et durée de l'évaluation

Le produit a fait l'objet de deux évaluations consécutives pour répondre à des observations formulées à l'issue de la première évaluation. La charge de travail totale a été de 51 h.j, y compris la charge d'évaluation de la cryptographie. L'évaluation de la version certifiée s'est déroulée de mi-septembre à mi-octobre 2009.

2.3 Travaux d'évaluation

Ce paragraphe apporte des compléments sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaborées par l'évaluateur suite à ses travaux.

2.3.1 Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1 Spécification de besoin du produit

Conforme à [CDS] (chapitre « Argumentaire »).

2.3.1.2 Biens sensibles manipulés par le produit

Conforme à [CDS] (chapitre « Description des biens sensibles que le produit doit protéger »).

2.3.1.3 Description des menaces contre lesquelles le produit apporte une protection

Conforme à [CDS] (chapitre « Description des menaces »).

2.3.1.4 Fonctions de sécurité

Conforme à [CDS] (chapitre « Description des fonctions de sécurité du produit »).

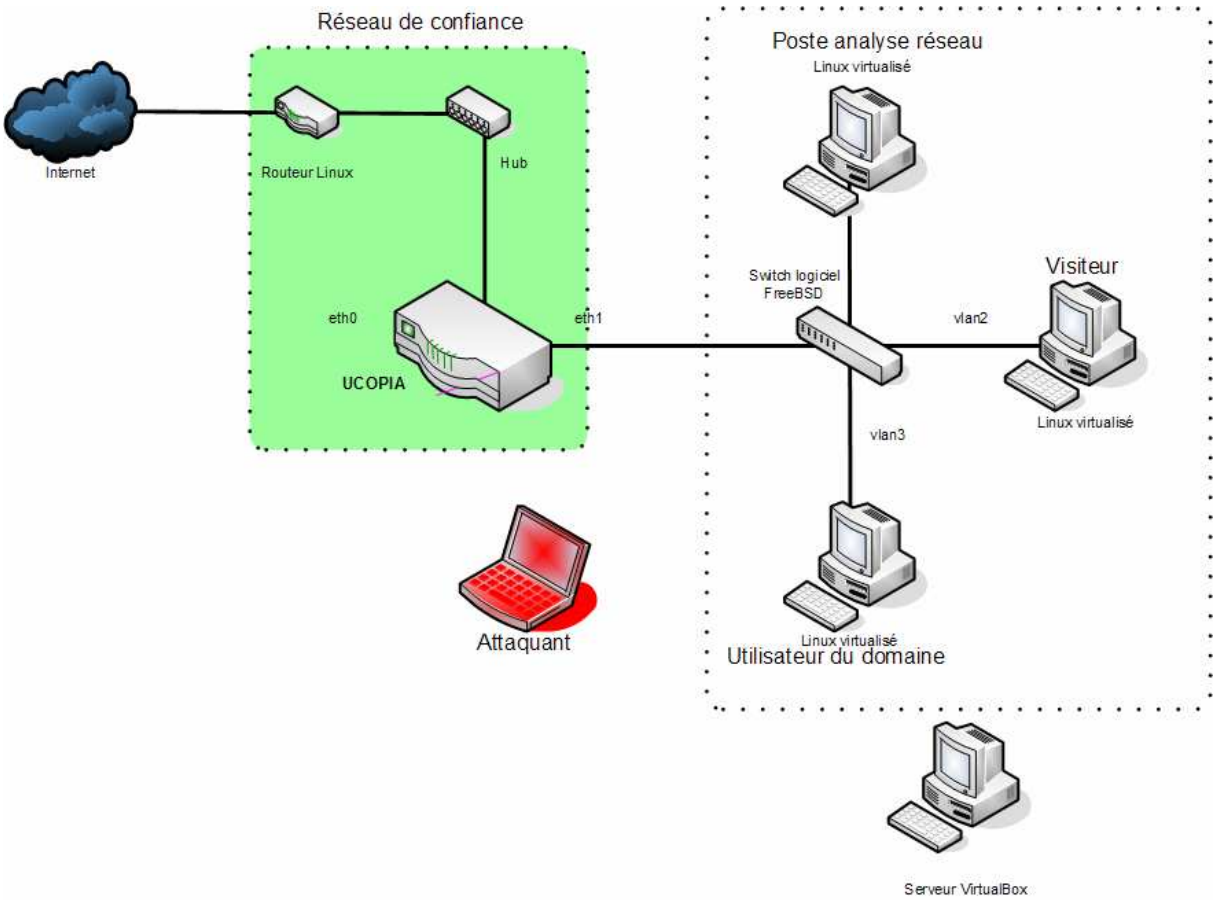
2.3.1.5 Utilisateurs typiques

Conforme à [CDS] (chapitre « Argumentaire »).

2.3.2 Installation du produit

2.3.2.1 Plate-forme de test

Le produit a été installé dans la configuration suivante :



Le routeur linux ci-dessus fait office de serveur DHCP et de DNS pour le réseau de confiance (192.168.1.0/24). Le produit UCOPIA prend donc l'adresse IP de son interface sur le réseau de confiance (eth0) par DHCP. Par ailleurs, deux VLANs sont configurés : le premier (vlan2) est un VLAN réservé aux visiteurs (accès restreint au proxy web), et le second (vlan3) réservé aux utilisateurs du domaine. Le numéro de VLAN utilisé correspond aux numéros de VLAN proposés par défaut par le boitier UCOPIA (ceux-ci peuvent être modifiés). L'authentification a été configurée pour autoriser les connexions au portail captif (vlan2) ainsi qu'en PEAP[1] (vlan3).
Le réseau VLAN est simulé sur une architecture réseau virtualisée (Sun Virtualbox).

2.3.2.2 Particularités de paramétrage de l'environnement

Sans objet.

[1] Protected Extensible Authentication Protocol

2.3.2.3 Options d'installation retenues pour le produit

Sans objet.

2.3.2.4 Description de l'installation et des non-conformités éventuelles

Il n'y a pas de non-conformité par rapport à la documentation. Les étapes présentées dans les documents [GUIDE] ont été suivies sans difficultés particulières.

2.3.2.5 Durée de l'installation

L'installation du produit et la configuration du réseau sous-jacent a duré deux jours

2.3.2.6 Notes et remarques diverses

Sans objet.

2.3.3 Analyse de la conformité

2.3.3.1 Analyse de la documentation

La documentation est claire et précise.

2.3.3.2 Revue du code source

Il n'y a pas eu de revue du code source

2.3.3.3 Fonctions testées

L'ensemble des fonctions suivantes a été testé :

Fonctionnalité	**Résultat**
Authentification par certificats (EAP-TLS) et protocole 802.1x	Réussite
Authentification par login/mot de passe (PEAP et TTLS) et protocole 802.1x	Réussite
Authentification depuis le portail Web captif UCOPIA (SSL/TLS)	Réussite
Génération des mots de passe utilisateurs	Réussite
Contrôle d'accès par filtrage de flux	Réussite
Cloisonnement VLAN	Réussite
Traçabilité	Réussite
Administration de l'appliance	Réussite
Télémaintenance de l'appliance	Réussite

2.3.3.4 Fonctions non testées

Les fonctions du produit qui sont hors du périmètre de l'évaluation n'ont pas été testées. Les fonctions de restriction de la bande passante par service et de gestion de la haute disponibilité n'ont pas été évaluées.

2.3.3.5 Synthèse des fonctions testées / non testées et des non-conformités

L'ensemble des fonctionnalités testées s'est avéré conforme à la cible de sécurité [CDS].

2.3.3.6 Avis d'expert sur le produit

Le produit implémente les fonctionnalités annoncées dans la documentation. L'enregistrement des actions de l'administrateur ou des administrateurs délégués mériterait une fonction dédiée (autre que les logs Apache).

2.3.4 Analyse de la résistance des mécanismes et des fonctions

2.3.4.1 Liste des fonctions testées et résistance

Les mécanismes mis en jeu sont l'authentification, le contrôle d'accès par filtrage de flux, le cloisonnement VLAN, la traçabilité et l'administration du produit.

Si l'administrateur n'a pas commis d'erreur de configuration ou de paramétrage, un attaquant non autorisé ne pourra pas accéder au réseau protégé par l'appliance.

2.3.4.2 Avis d'expert sur la résistance des mécanismes

Les mécanismes de sécurité sont robustes. Ceux qui s'appuient sur la cryptographie font l'objet d'une analyse théorique particulière dont les principales conclusions sont données au chapitre 2.4.

2.3.5 Analyse des vulnérabilités (conception, implémentation…)

2.3.5.1 Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur ce produit.

2.3.5.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

L'évaluation a mis en évidence une vulnérabilité concernant la fuite d'information par le protocole DNS. Le logiciel UCOPIA autorise les requêtes DNS vers Internet avant que l'utilisateur ne soit authentifié. Ce risque est assumé par UCOPIA et documenté comme tel. Une contre-mesure est proposée dans la documentation du développeur et précisée au. 2.3.6.2.

2.3.6 Analyse de la facilité d'emploi et préconisations

2.3.6.1 Cas où la sécurité est remise en cause

Il est possible d'administrer le produit depuis le réseau d'accès, ce qui est contraire aux bonnes pratiques de l'administration d'un produit de sécurité. Il est donc recommandé de n'autoriser les accès à l'interface d'administration que depuis le réseau de confiance.

2.3.6.2 Recommandations pour une utilisation sûre du produit

Afin de contrer la vulnérabilité présentée en 2.3.5.2, le constructeur recommande dans sa documentation de :

- configurer le serveur DNS utilisé par le logiciel UCOPIA pour rediriger les communications vers un serveur DNS sans accès Internet, ce qui évite les problèmes de requêtes DNS récursives. L'utilisation d'un proxy Web ayant accès à Internet est alors recommandée pour l'usage du Web.
- configurer le serveur DNS utilisé par le logiciel UCOPIA pour rediriger les communications vers un serveur DNS ne supportant pas les requêtes DNS récursives et/ou possédant des fonctionnalités de détection de trafic DNS malveillant.

De même, comme il est indiqué dans la documentation, il est fortement recommandé de n'autoriser les accès à l'interface d'administration que depuis le réseau de confiance.

2.3.6.3 Avis d'expert sur la facilité d'emploi

Le produit UCOPIA est, dans son ensemble, simple à utiliser ; l'interface web est claire et bien conçue. De même, la documentation fournie sur CD-ROM est complète et détaille de manière précise les opérations de connexion (visiteurs), d'installation et d'administration du produit.

2.3.7 Accès aux développeurs

L'évaluateur a bénéficié d'un support technique réactif et compétent.

2.4 Analyse de la résistance des mécanismes cryptographiques

Distribution de clé de chiffrement pour le point d'accès sans fil
Le produit implémente la version 3 du protocole SSL et la version 1 du protocole TLS pour protéger les données d'authentification et les clés.
Les suites cryptographiques suivantes utilisées par ces protocoles sont conformes au référentiel [RGS_B_1] de l'ANSSI :

Authentification	Echange de clés	Chiffrement	Code d'authentification de message
RSA 2048	DH 2048	CAMELLIA 256	SHA1
DSS 2048	DH 2048	CAMELLIA 256	SHA1
RSA 2048	RSA 2048	CAMELLIA 256	SHA1
RSA 2048	DH 2048	CAMELLIA 128	SHA1
DSS 2048	DH 2048	CAMELLIA 128	SHA1
RSA 2048	RSA 2048	CAMELLIA 128	SHA1
RSA 2048	DH 2048	AES 256	SHA1
DSS 2048	DH 2048	AES 256	SHA1
RSA 2048	RSA 2048	AES 256	SHA1
RSA 2048	DH 2048	AES 128	SHA1
DSS 2048	DH 2048	AES 128	SHA1
RSA 2048	RSA 2048	AES 128	SHA1
RSA 2048	DH 2048	3DES CBC 168	SHA1
DSS 2048	DH 2048	3DES CBC 168	SHA1
RSA 2048	RSA 2048	3DES CBC 168	SHA1

Les suites cryptographiques suivantes mis en œuvre par ces protocoles ne sont pas conformes au référentiel [RGS_B_1] de l'ANSSI :

RSA 2048	RSA 2048	RC4	SHA1
RSA 2048	RSA 2048	RC4	MD5

Utilisation du protocole HTTPS pour l'authentification

Les suites cryptographiques suivantes, mises en œuvre par le produit dans le cadre de la version 3 du protocole SSL et de la version 1 du protocole TLS, sont conformes au référentiel [RGS_B_1] de l'ANSSI :

Authentification	Echange de clés	Chiffrement	Code d'authentification de message
RSA 2048	DH 2048	CAMELLIA 256	SHA1
DSS 2048	DH 2048	CAMELLIA 256	SHA1
RSA 2048	RSA 2048	CAMELLIA 256	SHA1
RSA 2048	DH 2048	CAMELLIA 128	SHA1
DSS 2048	DH 2048	CAMELLIA 128	SHA1
RSA 2048	RSA 2048	CAMELLIA 128	SHA1
RSA 2048	DH 2048	AES 256	SHA1
DSS 2048	DH 2048	AES 256	SHA1
RSA 2048	RSA 2048	AES 256	SHA1
RSA 2048	DH 2048	AES 128	SHA1
DSS 2048	DH 2048	AES 128	SHA1
RSA 2048	RSA 2048	AES 128	SHA1
RSA 2048	DH 2048	3DES CBC 168	SHA1
DSS 2048	DH 2048	3DES CBC 168	SHA1
RSA 2048	RSA 2048	3DES CBC 168	SHA1

Les suites cryptographiques suivantes, mises en œuvre par le produit dans le cadre de la version 3 du protocole SSL et de la version 1 du protocole TLS, ne sont pas conformes au référentiel [RGS_B_1] de l'ANSSI :

RSA 2048	RSA 2048	RC4	SHA1
RSA 2048	RSA 2048	RC4	MD5

Utilisation du protocole SSH

Les mécanismes cryptographiques mis en œuvre par le produit sont conformes au référentiel [RGS_B_1] de l'ANSSI.

Hachage du mot de passe administrateur

L'algorithme proposé pour le hachage du mot de passe est satisfaisant.

Chiffrement et signature d'un fichier de mise à jour ou correctif[1]
Les mécanismes cryptographiques mis en œuvre par le produit sont conformes au référentiel [RGS_B_1] de l'ANSSI. Cependant, il est recommandé d'employer le mécanisme de signature défini par le standard PKCS#1 v2.1, tout en respectant les règles Fact-2 ou Fact-3 et Fact-4 du référentiel.

2.5 Analyse du générateur d'aléas

Le générateur d'aléas a fait l'objet d'une analyse et est conforme au référentiel [RGS_B_1] de l'ANSSI.

[1] L'expertise cryptographique de cette fonctionnalité n'a pas été réalisée.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles en vigueur, avec la compétence et l'impartialité requise pour un centre d'évaluation agréé.

Ce certificat atteste que le « logiciel UCOPIA pour boîtiers appliances UCOPIA version 3.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS], aux limites près indiquées dans le présent rapport.

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 s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [CDS], suivre les recommandations énoncées dans le présent rapport de certification au paragraphe 2.3.6.2 ainsi que celles se trouvant dans les guides fournis [GUIDES] avec le produit.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN v2.2* UCOPIA3.0.pdf référence UCPCSPN-3.0-09 Disponible sur www.ssi.gouv.fr/site_rubrique54.html
[RTE]	Certification de Sécurité de Premier Niveau - Rapport Technique d'Evaluation UCOPIA ; Thales-CSPN-UCOPIA2-v4.0.doc du 06/01/2010 référence UC2_RTE
[GUIDES]	Guides utilisateurs et administrateurs ; Ucp_Advance_Manuel_Installation_fr_.pdf , Ucp_Advance_Manuel_Installation_fr_.pdf , Ucp_Manuel_Editeur_Portail_fr_.pdf , Ucp_Manuel_Administration_Delegue_fr_.pdf , Ucp_Advance_Manuel_Administration_fr_.pdf.

Annexe 2. Références liées à la certification

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.	
[CER/P/01]	Procédure CSPN-CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI, disponible sur www.ssi.gouv.fr/site_article80.html
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 2.4, phase expérimentale, n° 915/SGDN/DCSSI/SDR/CCN du 25 avril 2008. Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1.4. Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1.3. Documents disponibles sur www.ssi.gouv.fr/site_article80.html
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, v1.11