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-CC-2010/54

Suite logicielle SEQUOIA v2 constituée des composantes logicielles K.Registration® v2.6.6, Trust.Center® v2.3.4 et KeySeed® v2.6.2

Paris, le 23 septembre 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-CC-2010/54

Nom du produit

Suite logicielle SEQUOIA v2 constituée des composantes logicielles K.Registration® v2.6.6, Trust.Center® v2.3.4 et KeySeed® v2.6.2

Référence/version du produit

Version 2

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ALC_FLR.3

Développeur

Keynectis

11-13 rue René Jacques, 92131 Issy les Moulineaux, France

Commanditaire

Keynectis

11-13 rue René Jacques, 92131 Issy les Moulineaux, 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 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 la « Suite logicielle SEQUOIA v2 constituée des composantes logicielles K.Registration® v2.6.6, Trust.Center® v2.3.4 et KeySeed® v2.6.2 » développée par la société Keynectis.

Ce produit est une suite logicielle modulaire qui permet à des prestataires de service de certification électronique (PSCE) de mettre en œuvre une Infrastructure de Gestion de Clés (IGC). Il fournit une solution qui permet à un PSCE de gérer le cycle de vie des certificats électroniques qu'il émet (notamment leur création, renouvellement et révocation), quel que soit leur usage : authentification, signature électronique, chiffrement, authentification serveur, cachet, …

La suite logicielle SEQUOIA v2 contient trois composantes logicielles distinctes qui sont :

- la composante K.Registration® v2.6.6: ensemble de modules logiciels qui permet de gérer des offres de certification pour le compte d'une Autorité d'Enregistrement (AE). Une offre de certification permet de retranscrire techniquement les cinématiques procédurales définies pour le cycle de vie d'un certificat (enregistrement, validation, remise de certificat, révocation, ….) ;

- la composante Trust.Center® v2.3.4: ensemble de modules logiciels qui permet de formater des données et de mettre en œuvre des clés privées d'Autorités de Certification (AC) pour la signature de certificats électroniques de porteurs et de listes de certificats révoqués (LCR) ;

- la composante KeySeed® v2.6.2: un module logiciel, hors ligne, qui assure les opérations de gestion du cycle de vie des AC à l'aide de ressources cryptographiques (noté HSM). Le module logiciel KeySeed® permet notamment la création des bi-clés d'AC, la signature des certificats, la signature des listes de révocation d'AC (LAR), l'importation et l'exportation de bi-clés d'AC et la création de clés secrètes.

La figure ci-dessous donne un exemple d'utilisation des trois composantes de la suite logicielle SEQUOIA.
Sur cette figure, ACR correspond à Autorité de Certification Racine et AEL correspond à Autorité d'Enregistrement Locale.

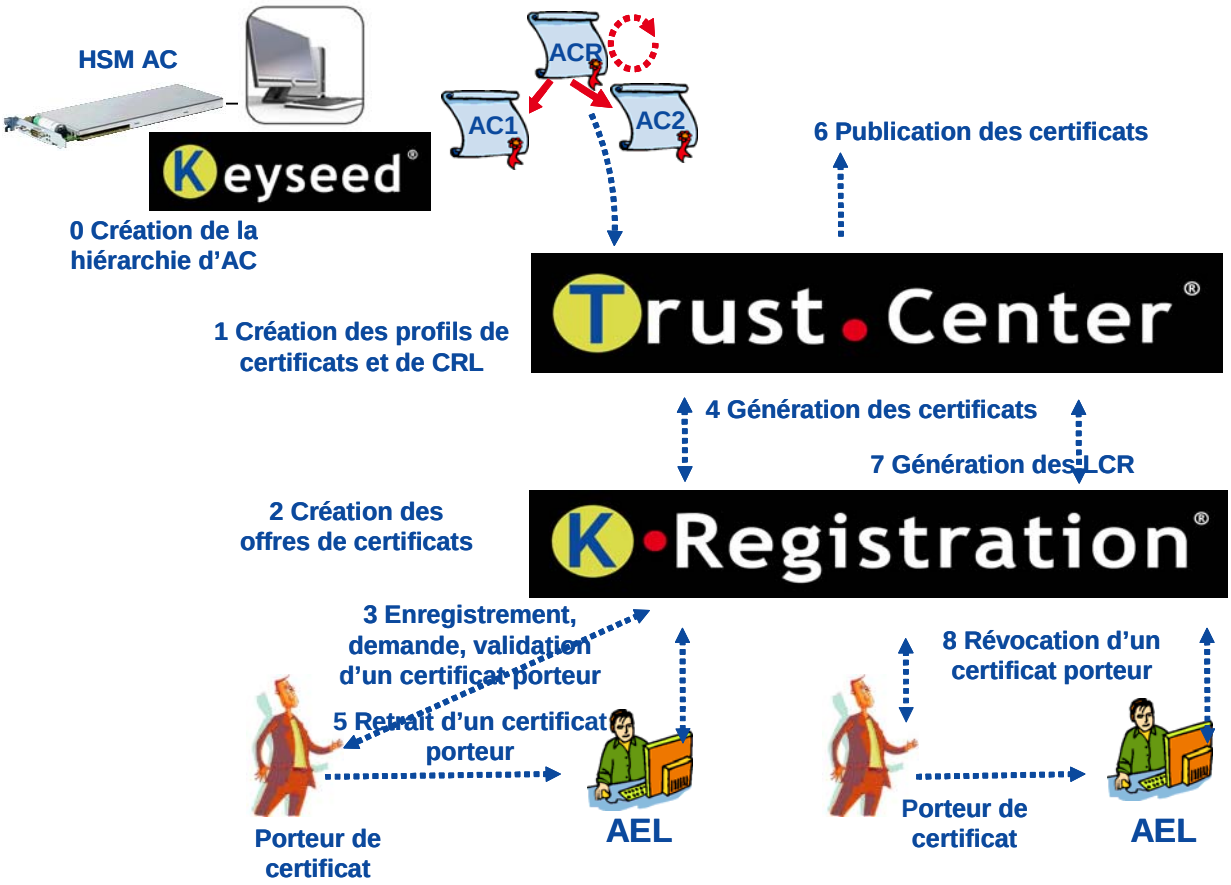

Figure 1 - Exemple d'utilisation de la suite logicielle SEQUOIA

Les composantes peuvent être utilisées ensemble afin de rendre des services d'IGC. Elles peuvent aussi être utilisées indépendamment les unes des autres. Les configurations d'utilisation qui sont possibles sans remise en cause des résultats de l'évaluation sont les suivantes :

- KeySeed® seul ;
- Trust.Center® avec K.Registration® ;
- Trust.Center® seul ;
- Trust.Center® avec KeySeed®.

1.2. Description du produit

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

1.2.1. Identification du produit

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

La version certifiée du produit est identifiable en accédant aux interfaces des composantes de la cible d'évaluation :

- pour K.Registration® et Trust.Center®, la version est indiquée sur la page web de l'interface utilisateur associée ;
- pour KeySeed®, la version est indiquée dans l'onglet « Help / About KeySeed ».

1.2.2. Services de sécurité

La TOE (*Target of Evaluation* – cible d'évaluation) permet de mettre en œuvre, pour la gestion des certificats et des LCR, les services suivants :

- service d'enregistrement ;
- service de demande de certificat ;
- service de génération de certificat ;
- service de retrait de certificat ;
- service de révocation ;
- service de création et de gestion des rôles de confiance (administrateur, opérateur, auditeur) ;
- service de journalisation et d'audit.

1.2.3. Architecture

La figure ci-dessous présente l'architecture de la cible d'évaluation, décomposée en composantes logicielles distinctes. Il est à noter que seuls les éléments en bleu-vert sont inclus dans la TOE. Les autres éléments (en bleu ciel, orange et jaune) sont des éléments nécessaires au fonctionnement de la TOE mais n'en font pas partie.

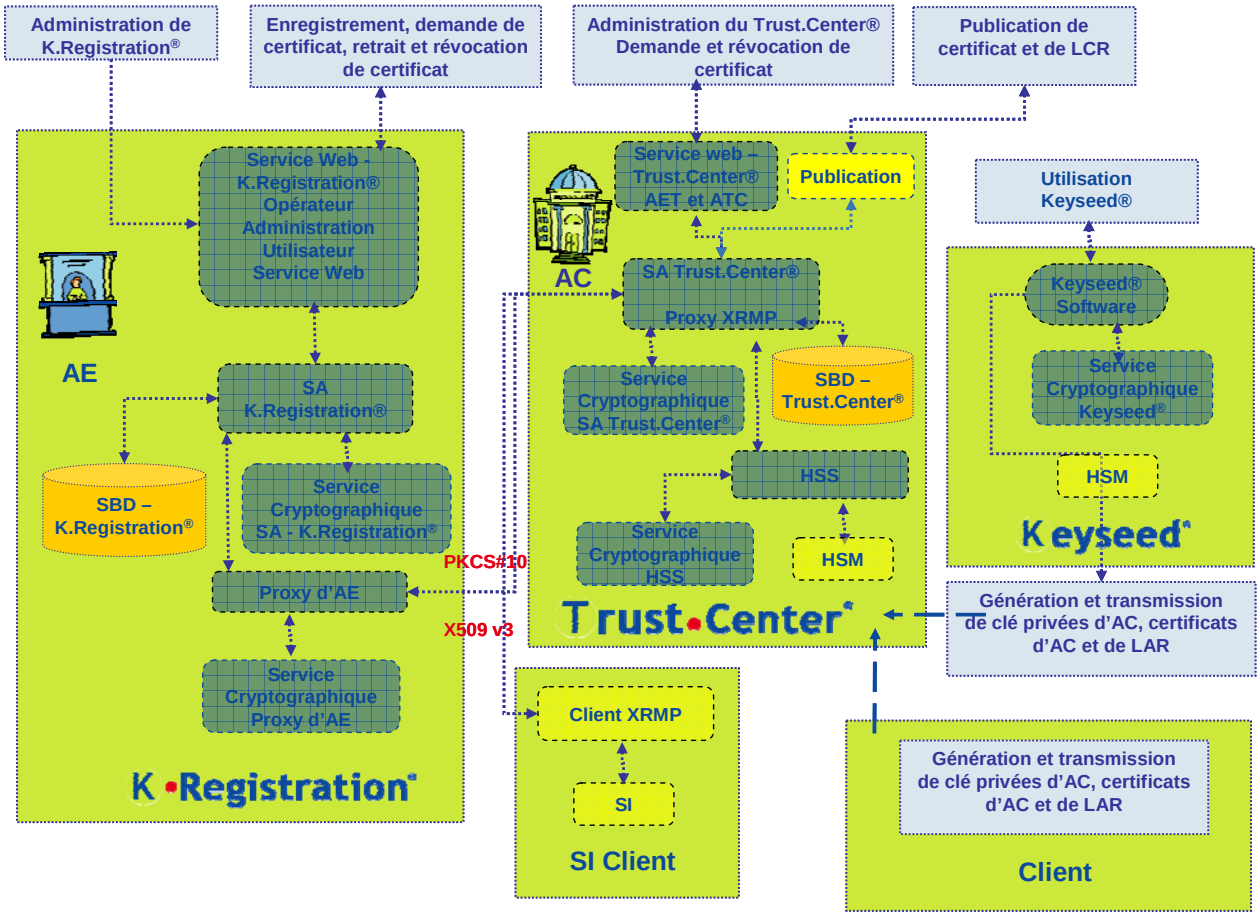

Figure 2 - Architecture de la TOE

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

- le développement et la livraison (de tout ou partie) du produit sont réalisés par Keynectis ;
- l'installation, l'administration et l'utilisation (de tout ou partie) du produit correspondent au déploiement du produit par le client.

Le produit a été développé sur le site suivant :

Keynectis

11-13 rue René Jacques
92131 Issy les Moulineaux
France

Pour l'évaluation, l'évaluateur a considéré les rôles suivants :

- « porteur de certificat » : personne physique ou morale qui utilise certaines fonctions de la TOE pour des besoins relatifs aux certificats qu'elle souhaite avoir ou qu'elle possède ;
- utilisateurs de la TOE (rôles de confiance)
  - « administrateur » : il est chargé de la configuration et de la gestion des rôles de confiance « administrateur », « opérateur » et « auditeur » pour les modules de la TOE, en fonction des politiques de certification utilisées pour la mise en œuvre des services de la TOE. La suite logicielle SEQUOIA met aussi en œuvre, pour certains de ces modules, un « administrateur root » qui sert à la gestion des rôles du module ;
  - « opérateur » : il réalise l'exploitation de tout ou partie des fonctions offertes par les modules de la TOE ;
  - « auditeur » : il réalise les opérations de vérification de la bonne application de la politique de certification effectuée par les modules de la TOE.

Les acteurs de l'environnement de la TOE sont les personnels du PSCE qui ne sont pas associés aux rôles de confiance définis ci-dessus, notamment :

- le responsable de sécurité : il est responsable de l'application de la politique de sécurité physique et fonctionnelle de la TOE et de son environnement. Il est aussi responsable de l'application de la politique et de la déclaration des pratiques de certification mise en œuvre à l'aide de la TOE ;
- l'administrateur système : il est chargé de la mise en route, de la configuration et de la maintenance technique des machines hôtes des composantes de la TOE. Il assure l'administration des machines hôtes et du réseau utilisé par les composantes de la TOE. Il est aussi administrateur des bases de données de la TOE pour les composantes Trust.Center® et K.Registration® ;
- les porteurs de données d'activation (porteurs de secret) : ce sont les rôles définis pour la mise en œuvre et la gestion du module cryptographique (HSM) utilisé par la TOE.

1.2.5. Configuration évaluée

L'architecture suivante a été retenue pour réaliser les tests fonctionnels et de vulnérabilités :

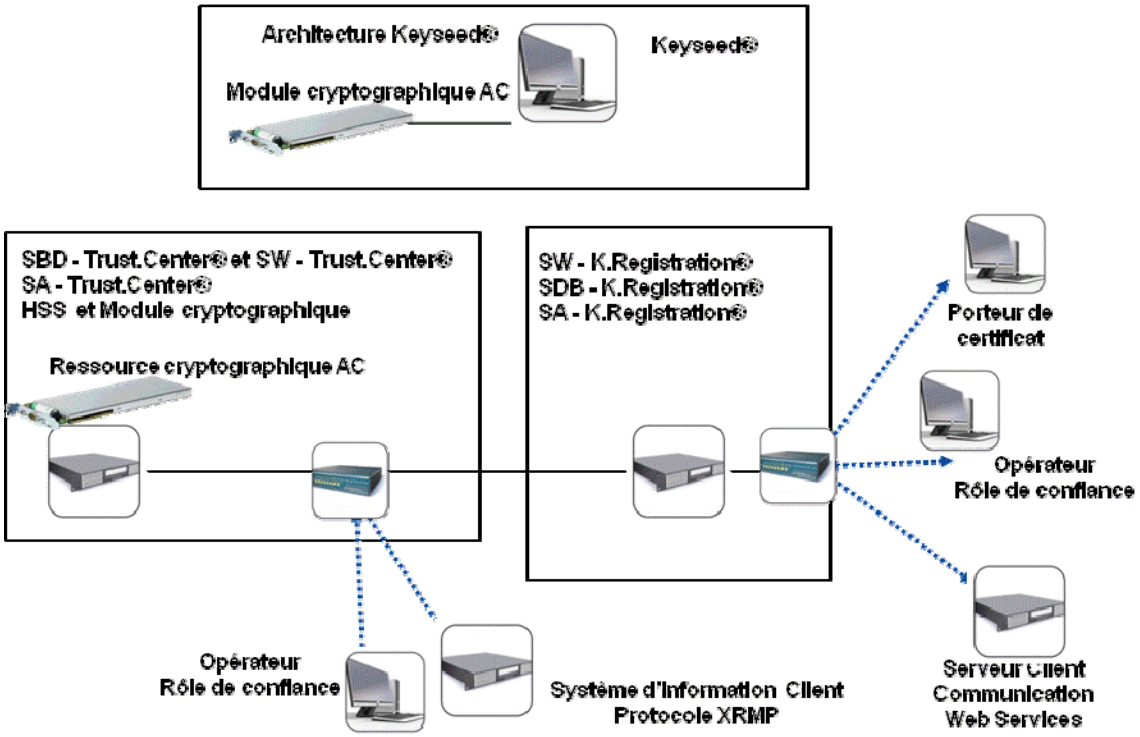

Figure 3 - Architecture de la plateforme d'évaluation

Le présent certificat porte sur la configuration suivante :

- systèmes d'exploitation des machines hôtes :
  - pour KeySeed® : Microsoft Windows XP Professionnel Version 2002 service Pack 3 ;
  - pour K.Registration® : RedHat Enterprise Linux 5 Update 3 (Default Install) ;
  - pour Trust.Center® : RedHat Enterprise Linux 5 Update 3 (Default Install) ;
- bases de données pour K.Registration® et Trust.Center® : Oracle 11g ;
- module (ou ressource) cryptographique (HSM) pour KeySeed® et Trust.Center® : carte Trustway PCA2 version S503.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Bien que la cible de sécurité [ST] se réfère aux Critères Communs version 3.1 révision 2, la révision 3, publiée après le démarrage de cette évaluation, a été prise en compte au cours de cette évaluation. Pour rappel, la principale différence entre ces deux révisions correspond au remplacement du composant ATE_DPT.2 par le composant ATE_DPT.1 au niveau EAL4.

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 10 septembre 2010, 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

La cotation des mécanismes cryptographiques selon les référentiels techniques [REF-CRY], [REF-KEY] et [REF-AUT] n'a pas été réalisée par l'ANSSI. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le produit ne comporte pas de générateur d'aléas entrant dans le périmètre d'évaluation.

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 n°2002-535.

Ce certificat atteste que le produit « Suite logicielle SEQUOIA v2 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

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 [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- (OE_Administrateur système) les personnels ayant un rôle « Administrateur Système » sur les machines hôtes qui hébergent les composantes de la TOE doivent être de confiance et doivent disposer de la formation et des éléments nécessaires pour assurer correctement leur mission ;

- (OE_Porteur de données d'activation) les personnels ayant un rôle « Porteur de données d'activation » sur les HSM hébergeant les clés AC doivent être de confiance et disposer de la formation et des éléments nécessaires pour assurer correctement leur mission ;

- (OE_Attribution de rôle) les acteurs de l'environnement de la TOE identifiés précédemment ne peuvent avoir comme autre rôle que « Porteurs de certificat » ;

- (OE_Machines hôtes) les machines hôtes hébergeant les composantes de la TOE doivent assurer une protection suffisante des éléments constituant la TOE et des éléments nécessaires à son fonctionnement et avoir des fonctions d'audit et de journalisation ;

- (OE_Réseau) les échanges réseau entre les machines hébergeant Trust.Center® et K.Registration®, ainsi que les échanges réseau entre ces machines et celles de l'environnement, doivent être contrôlés, journalisés et limités par des pare-feux ;

- (OE_Sauvegarde et OE_Retour état sûr) les administrateurs de la TOE doivent disposer de moyens permettant de sauvegarder, contrôler par rapport à un état de référence et restaurer une configuration et les biens de la TOE à partir des données

issues du service de bases de données de chacune des composantes Trust.Center® et K.Registration® ;

- (OE_Machine hôte KeySeed®) la machine hôte utilisée pour la mise en œuvre du module logiciel de la composante KeySeed® ne doit pas accueillir d'autres applications et ne doit être connectée à aucun réseau ;

- (OE_Machine hôte Trust.Center® et OE_Machine hôte K.Registration®) les machines hôtes utilisées pour la mise en œuvre des modules logiciels des composantes Trust.Center® et K.Registration® ne doivent pas accueillir d'autres applications ;

- (OE_SI_Client) l'environnement du système d'information Client doit assurer l'identification et l'authentification des utilisateurs qui se connectent, localement ou à distance, aux machines qui interagissent avec la suite logicielle SEQUOIA ;

- (OE_Temps de référence) les machines hôtes qui supportent un module de la TOE doivent avoir une horloge interne qui est synchronisée avec un temps de référence UTC (Temps Universel Coordonné) ;

- (OE_Bi-clés Rôle de confiance) les rôles de confiance « Administrateur », « Opérateur » et « Auditeur » qui utilisent les services de la TOE doivent posséder chacun une bi-clé et un certificat associé sur carte à puce ;

- (OE_Protection d'une clé privée associée à un certificat) les porteurs de certificats doivent être garants de la protection en confidentialité, en intégrité et en disponibilité des clés privées associées aux certificats qu'ils détiennent ;

- (OE_Protection physique) l'environnement de la TOE doit assurer une protection physique suffisante afin de limiter les risques d'attaques contre l'intégrité de la TOE ;

- (OE_Politique de certification) le PSCE ou l'organisme mettant en œuvre une application nécessitant des certificats doit définir et mettre en œuvre un ensemble de Politiques de Certification (PC) et de Déclarations des Pratiques de Certification (DPC) pour les certificats émis et gérés à l'aide de la TOE.

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. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

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. 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 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, 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 4+	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	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	3	Basic modular 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	4	Production support, acceptance, procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	Problem tracking configuration management coverage
	ALC_DEL		1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	1	Identification of security measures
	ALC_FLR								3	Systematic flaw remediation
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	Well-defined development tools
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	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	2	Testing: security enforcing modules
	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_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité SEQUOIA, Référence : DS_Cible_Sequoia_ST 07072010_2.2, version 2.2 du 06/07/2010 Keynectis Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Cible de sécurité light Sequoia, Référence : DS_Cible_Sequoia_Light, version 0.1 du 07/07/2010 Keynectis
[RTE]	Rapport technique d'évaluation – Projet CARAT Référence : OPPIDA/CESTI/CARAT/RTE/2.2 du 10/09/2010 OPPIDA
[CONF]	Liste de configuration suite logicielle SEQUOIA Référence : DSQ_NT_Liste-Configuration_1.4, version 1.4 du 06/07/2010 Keynectis
[GUIDES]	Guide de recommandations sécuritaires : - Recommandations sécuritaires SEQUOIA Référence : ERD_INST_Sécurisation_produits_1.3, du 18/06/2010 Keynectis Guides d'installation du produit : - Manuel d'installation K.Registration® Référence : ERD_INST_KREG_2.6.5_1.9, du 06/07/2010 Keynectis - Manuel d'installation Trust.Center® Référence : ERD_INST_TC_2.3.4_1.4, du 06/07/2010 Keynectis - Manuel d'installation KeySeed® Référence : ERD_INST_KSD_2.6.2_1.2, du 06/07/2010 Keynectis Guides de configuration du produit : - Manuel de configuration K.Registration® Référence : ERD_CONFIG_KREG_2.6.5_EAL4Plus_1.3, du 06/07/2010 Keynectis - Manuel de configuration Trust.Center® Référence : ERD_CONFIG_TC_2.3.4_EAL4Plus_1.4, du 06/07/2010 Keynectis - Manuel de configuration KeySeed® Référence : ERD_CONFIG_KSD_2.6.2_ 1.3, du 06/07/2010

	Keynectis Guides de mise en service du produit : - Manuel de mise en service K.Registration® Référence : ERD_MES_KREG_2.6.5_EAL4Plus_1.2, du 06/07/2010 Keynectis - Manuel de mise en service Trust.Center® Référence : ERD_MES_TC_2.3.4_EAL4Plus_1.2, du 06/07/2010 Keynectis Guides d'exploitation du produit : - Manuel d'exploitation K.Registration® Référence : ERD_EXPL_KREG_2.6.5_1.7, du 16/07/2010 Keynectis - Manuel d'exploitation Trust.Center® Référence : ERD_EXPL_TC_2.3.4_1.4, du 16/07/2010 Keynectis Guides d'utilisation du produit : - Manuel utilisateur du site opérateur K.Registration® Référence : ERD_MU_KREG_2.6.5_OPER_1.3, du 06/07/2010 Keynectis - Manuel utilisateur pour le site utilisateur K.Registration® Référence : ERD_MU_KREG_2.6.5_USER_1.7, du 06/07/2010 Keynectis - Manuel utilisateur pour le site administrateur K.Registration® Référence : ERD_MU_KREG_2.6.5_ADMIN_1.3, du 06/07/2010 Keynectis - Manuel utilisateur Interfaces Webservices K.Registration® Référence : ERD_MU_KREG_2.6.5_WEBSERVICES_1.11, du 20/07/2010 Keynectis - Manuel utilisateur AET Trust.Center® Référence : ERD_MU_TC_2.3.4_AET_1.3, du 06/07/2010 Keynectis - Manuel utilisateur ATC Trust.Center® Référence : ERD_MU_TC_2.3.4_ATC_1.3, du 06/07/2010 Keynectis - Manuel utilisateur Interface XRMP Trust.Center® Référence : ERD_MU_TC_2.3.4_WS-XRMP_1.5, du 06/07/2010 Keynectis - Manuel utilisateur KeySeed® Référence : ERD_MU_KSD_2.6.2_1.2, du 06/07/2010 Keynectis

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, 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 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010, voir www.ssi.gouv.fr
[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008, voir www.ssi.gouv.fr
[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010, voir www.ssi.gouv.fr