KEYNECTIS

CIBLE DE SECURITE

Sequoia® e-ID

Cible de sécurité light
V0.1 07 juillet 2010 – Sequoia®

Protecteur d'identité
Protecteur de liberté
dans un monde connecté

11-13 rue René Jacques - 92131 Issy Les Moulineaux Cedex - France - Tél. : + 33 (0)1 55 64 22 00 - Fax : + 33 (0)1 55 64 22 01 - www.keynectis.com

CIBLE DE SECURITE LIGHT : SEQUOIA®

Version du document :	0.1	**Nombre total de pages :**	95
Statut du document :	☐ Projet	☒ Version finale	
Rédacteur du document :	DS	KEYNECTIS	

Historique du document :				
Date	Version	Rédacteur	Commentaires	Vérifié par
07/07/2010	0.1	EM	Création du document	

SOMMAIRE

TABLE DES ILLUSTRATIONS

1 INTRODUCTION

1.1 Identification

Auteur : KEYNECTIS.
Titre de la ST : Sequoia® : cible de sécurité.
Version de la ST : v 1.0
Identifiant de la TOE : Sequoia V2 qui est composée des composants KeySeed® v 2.6.2, Trust.Center® 2.3.4 et K.Registration® v 2.6.6.
Niveau d'évaluation : EAL4 augmenté du composant ALC_FLR.3.

Mots-clés : Infrastructure de Gestion de Clés (IGC ou PKI en anglais), autorité de certification (AC ou CA en anglais), Autorité de certification Racine (ACR), autorité d'enregistrement (AE ou RA en anglais), certificat électronique, certificat électronique qualifié, génération de certificat électronique, bi-clé asymétrique, enregistrement de certificat électronique, révocation de certificat électronique, renouvellement de certificat électronique.

1.2 Contexte

Cette cible de sécurité est élaborée par la société KEYNECTIS qui est éditeur de logiciel.

Le type de la TOE est une suite logicielle IGC.

1.3 Présentation générale de la cible d'évaluation

Nota : on trouvera une description détaillée de la TOE en Annexe A.

La sécurisation des échanges au sein d'une application s'effectue en utilisant des certificats électroniques qui permettent au porteur de certificat de mettre en œuvre des fonctions de sécurité (signature, chiffrement, contrôles d'accès, …). Le promoteur d'application valide les Politiques de Certification (PC) qui sont applicables pour la gestion des certificats que les porteurs doivent utiliser au sein des applications dont il a la responsabilité. Ces certificats sont délivrés par des AC. Un promoteur d'application peut alors être soit lui-même PSCO pour la gestion et la mise en œuvre des AC qu'il utilise, soit utiliser des PSCO externes à son organisme en intégrant au sein de ses systèmes d'information tout ou partie de la solution d'IGC du PSCO utilisé.

Un PSCO met en œuvre des AC pour son propre compte ou pour celui de promoteur d'application afin de délivrer des certificats électroniques conformément à des PC et des DPC. Un PSCO, qui héberge plusieurs AC, met donc en œuvre plusieurs PC à l'aide d'une même IGC. Les principales différences entre les PC résident dans les scénarios d'enregistrement, les scénarios de gestion d'un certificat (révocation, renouvellement, …) le profil d'un certificat, le profil des LCR, les caractéristiques algorithmiques utilisées pour l'AC et les certificats qu'elle émet, la définition des rôles de confiance et des droits associées et les modalités d'authentification des rôles de confiance et des porteurs de certificats.

Par conséquent le déploiement d'une IGC par un PSCO consiste à réutiliser un maximum de composantes d'IGC pour la mise en œuvre de différentes PC. La TOE offre la capacité à un PSCO de mettre en œuvre plusieurs AC et plusieurs PC à l'aide d'une même IGC. La confiance dans un PCSO repose sur sa capacité à mettre en œuvre des PC pour une AC de manière sécurisée afin de garantir le lien entre un certificat, la bi-clé cryptographique associée et le porteur de certificat conformément à la PC de référence. Cette confiance repose à la fois sur la définition des DPC et sur la qualité des logiciels employés afin de garantir le respect de la mise en œuvre de manière cloisonnée des différentes PC et DPC supportées.

La TOE représente une partie des composantes d'IGC qu'il est nécessaire d'implémenter dès lors qu'une IGC est déployée par un PSCO. Comme indiqué sur la figure ci-dessous, la TOE peut s'interconnecter avec d'autres composantes d'IGC (Autorité d'Enregistrement Locale, Service de Gestion de clés, Service d'horodatage, ressource cryptographique, …).

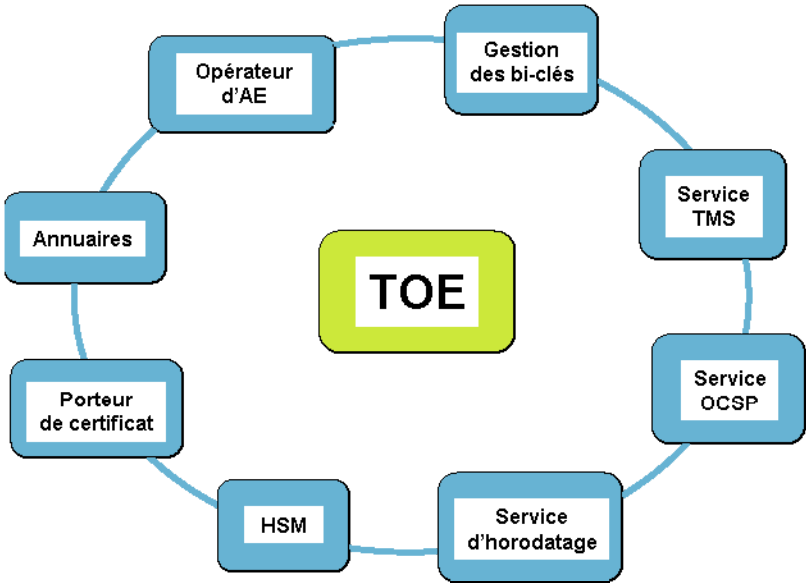


Figure 1 : Environnement de la TOE

1.4 Services de la TOE

Ce paragraphe identifie d'abord les services d'IGC de manière générique afin de clairement identifier et cerner ce que la TOE met en œuvre comme services d'IGC.

1.4.1 Services d'IGC

Les services génériques d'IGC tels qu'offerts par KEYNECTIS peuvent se synthétiser de la manière suivante :

- Service de génération de bi-clés : ce service (service type centre d'élaboration de bi-clé, carte à puces, …) génère des bi-clés cryptographiques et les prépare en vue d'une distribution ultérieure à l'aide d'un support de bi-clé qui peut être logiciel ou matériel ;

- Service de génération des données d'activation de support de bi-clé(s) : ce service génère la ou les données d'activation qui sont utilisées par un type de support de bi-clés afin de protéger l'accès et la mise en œuvre de la ou des clés privées contenus dans ce support ;

- Service de personnalisation de support de bi-clés : ce service permet de personnaliser graphiquement et électriquement un support matériel ou logiciel de bi-clé cryptographique en fonction des données fournies par le service génération de bi-clés, le service génération de certificats et le service génération des données d'activation ;

- Service de séquestre et de recouvrement de bi-clés : ce service fournit la capacité de séquestrer de manière sécurisée les clés privées de confidentialité des porteurs de certificat, fournies par le service de génération de bi-clés, puis de les recouvrer en cas de besoin, sur la base de demandes authentifiées et traitées par le service de gestion des recouvrements ;

- Service d'enregistrement : ce service permet de récupérer, de vérifier et de valider des informations d'identification et/ou des autorisations, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre une demande de certificat au service demande de certificat. Ce service est mis en œuvre par une Autorité d'Enregistrement (AE) ;

- Service de demande de certificat : ce service crée une demande de certificat, à l'aide des informations fournies par les services enregistrement et génération de bi-clé afin de créer et de transmettre une demande de certificat au service de génération de certificat ;

- Service de génération de certificat : ce service génère (création du format, signature électronique avec la clé privée d'une AC) les certificats à partir des informations transmises par le service demande de certificat ;

- Service de remise d'éléments secrets au porteur : ce service remet les clés privées (support matériel des clés cryptographiques, clé privée, données d'activation, …) ;

- Service de retrait de certificat : ce service permet à un opérateur d'AE ou un porteur de certificat de pourvoir retirer un certificat généré par la TOE ;

- Service de révocation : ce service traite les demandes de révocation et détermine les actions à mener afin d'informer qu'un certificat n'est plus utilisable. Les résultats des traitements (génération d'une LAR, génération d'une LCR, avis, …) sont diffusés via la fonction d'information sur l'état des certificats ;

- Service de création et de gestion des rôles de confiance : ce service permet de créer et de gérer l'ensemble des rôles de confiance utilisés par la TOE pour la mise en œuvre des services de la TOE ;

- Service de publication : ce service met à disposition les informations (certificat et LCR) nécessaires au bon fonctionnement et à l'utilisation de l'IGC (la TOE) aux annuaires désignés et au service d'information sur l'état des certificats ;

- Service de journalisation et d'audit : ce service permet de collecter l'ensemble des données utilisées et ou générées par la TOE afin d'obtenir des traces d'audits, consultables par les utilisateurs de la TOE, relatifs aux services d'IGC mise en œuvre à l'aide de la TOE par les acteurs de la TOE.

Les services connexes usuels à l'IGC sont les suivants :

- Services d'informations sur l'état des certificats : service qui permet à un utilisateur de certificat de savoir si un certificat est valide ou non. La mise en œuvre de ce service utilise des bi-clés et des certificats afin de signer les réponses fournies ;

- Services d'horodatage : service qui délivre des contremarques de temps à l'aide d'unités d'horodatage. L'élaboration des contremarques de temps est effectuée à l'aide de bi-clés et de certificats afin de signer les contremarques de temps, et de sources de temps de référence.

1.4.2 Services de la TOE

La TOE 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 publication ;
- Service de création et de gestion des rôles de confiance ;
- Service de journalisation et d'audit.

1.5 Identification des composantes de la TOE

1.5.1 Composantes de la TOE

Ce paragraphe détaille la composition de la suite logicielle Sequoia® afin de mieux cerner et identifier les composantes de la TOE.

La suite logicielles Sequoia® est définie par trois composantes logicielles distinctes qui sont :

- Composante Keyseed® : un module logiciel, hors ligne, qui assure les opérations de gestion du cycle de vie des AC à l'aide de ressource cryptographique (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 ou ARL en Anglais), l'importation et l'exportation de bi-clé d'AC et la création de clé secrète. Keyseed® ne manipule pas de clé en claires. La manipulation des clés est effectuée à l'aide des fonctions du HSM que Keyseed® active via des commandes Pkcs #11 ;

- Composante Trust.Center® : ensemble de modules logiciels qui permet de formater des données et de mettre en œuvre des clés privées d'AC pour la signature de certificats électroniques de porteurs (humains ou machines) et de listes de certificats révoqués (LCR). La signature des certificats et des LCR est effectuée suite à une demande de certificat ou de révocation émise par une AE. Ce composant est donc connecté des AE qui sont matérialisées par K.Registration® et par d'autres système d'information Client (SI Client) en utilisant le protocole XRMP ;

- Composante K.Registration® : ensemble de modules logiciels qui permet de gérer des offres de certification pour le compte d'une AE. Une offre de certification permet de retranscrire techniquement les cinématiques procédurales (enregistrement, validation, remise de certificat, révocation, ….) définies pour le cycle de vie d'un certificat. Ces offres de certification sont mises en œuvre par des opérateurs d'AE. Il utilise Trust.Center® auprès duquel il émet des demandes de certificat et de révocation en utilisant le protocole XRMP (via un proxy d'AE).

Le protocole XRMP est un protocole crée par KEYNECTIS. Lorsque le protocole XRMP est implémenté pour la composante K.Registration®, il est alors fait mention de « proxy d'AE ». Lorsque le protocole XRMP est implémenté chez un Client, il doit être implémenté dans le système d'information Client (SI Client) conformément aux spécifications édictées par KEYNECTIS.

Un PSCO délivre des services d'IGC qu'il formalise au travers de PC et de DPC. La TOE est un ensemble de composantes logicielles utilisé par un PSCO afin de mettre en œuvre des services d'IGC (PC et des DPC) pour la gestion des certificats électroniques qu'il délivre au profit d'AC. La déclinaison technique des services d'IGC (PC et des DPC) s'effectue entre autres par la définition des profils de certificats et de LCR au niveau de domaine de confiance de Trust.Center® et d'offre(s) de certification au niveau de K.Registration®. La multiplicité des PC et des DPC supportées, qui traduisent différentes manières de rendre des services d'IGC, se traduit entre autre par la multiplicité des offres de certification réparties sur différents domaines de certification. La gestion du cycle de vie des AC, définies dans les différentes PC et DPC, est quant à elle gérée par Keyseed®.

La gestion du cloisonnement, qui est nécessaire à la mise en œuvre mutualisée de services d'IGC pour différentes AC (différentes PC et DPC) par la TOE, est effectuée à l'aide des fonctions proposées par ses trois composantes logicielles. Il n'y a pas de fonctions à proprement parler de gestion des PC et DPC mais un ensemble de fonctions réparties sur les composantes Trust.Center®, K.Registration® et Keyseed® qui sont configurables et mises en œuvre de manière flexible et modulaire afin de réaliser le cloisonnement nécessaires aux services d'IGC de plusieurs AC.

Le terme « composante » sera utilisé pour désigner de manière générique les modules logiciels du Trust.Center®, de K.Registration® et de Keyseed® qui font l'objet d'une évaluation certification. Le terme « composante » est la traduction du terme « component », utilisé par les critères communs, qui désigne les parties de la TOE qui sont évaluées. Lorsque qu'il sera nécessaire d'identifier un module précis de la composante de la TOE, alors le terme exact du module sera utilisé.

Le schéma ci-dessous résume de manière macroscopique l'utilisation des trois composantes de la suite logicielle Sequoia®.

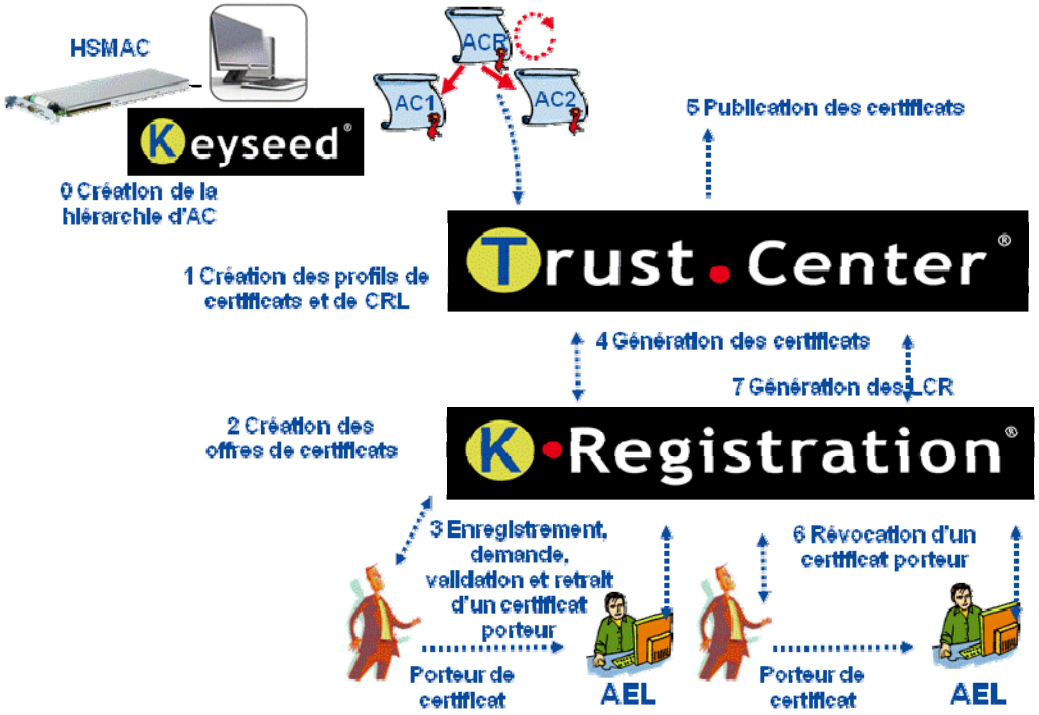


Figure 2 : Exemple d'utilisation de la suite logicielle Sequoia®

1.5.2 Combinaison possible de mise en œuvre des composantes de la TOE

Au sein d'un PSCO, les composantes sont utilisées ensemble afin de rendre des services d'IGC. Toutefois, ils peuvent aussi être utilisés indépendamment les uns des autres. Les configurations d'utilisation qui sont possibles sans remise en cause des résultats de l'évaluation sont les suivantes :

- Keyseed® tout seul : cette configuration permet de réaliser des cérémonies des clés pour des ACR et des AC et gérer les hiérarchies d'AC et leur cycle de vie, indépendamment de l'application d'IGC et à l'aide d'un module cryptographique (avec interface PKCS#11) qui va mettre en œuvre les clés privées d'ACR et d'AC ;

- Trust.Center® avec K.Registration® : cette configuration permet la gestion du cycle de vie des certificats de porteurs (humains ou machines). Cette configuration permet de mettre en œuvre et de gérer des certificats à l'aide d'AC et d'ACR qui ne sont pas gérées par le logiciel Keyseed® ;

- Trust.Center® seul : cette configuration permet de générer des certificats et des LCR (Liste de Certificats Révoqués). Ceci permet de gérer le cycle de vie de certificats dont l'authentification et l'identification des porteurs de certificat est faite soit directement auprès de Trust.Center® soit auprès d'un service de gestion de certificat d'AC sous la maîtrise de l'utilisateur de Trust.Center®. Cette configuration correspond au cas où seules les AC qui génèrent les certificats de porteur de certificats sont gérées par le PSCO. Dans ce cas, une partie de la chaîne de certification n'est pas maîtrisée par KEYNECTIS, les certificats des AC de niveaux supérieurs doivent être importés dans le Trust.Center®

- Trust.Center® avec Keyseed® : cette configuration permet de gérer des AC et de délivrer des certificats et des LCR à partir de demandes fournies par une AE qui utilise une autre composante logicielle que K.Registration®. Dans ce cas, l'AE possède un système d'information qui est authentifié par le Trust.Center® à l'aide d'un module logiciel fournit par KEYNECTIS (Client XRMP).

Lorsqu'une composante de la TOE est utilisée dans l'une des configurations particulières citées ci-dessus, alors la partie du service d'IGC mis en œuvre par d'autres composantes, que ceux de la TOE, est de la responsabilité du PSCO qui utilise la ou les composante(s) de la TOE. En ce cas, le PSCO doit s'assurer que les composantes qu'il utilise permettent de réaliser les objectifs et les exigences de sécurité des parties des services d'IGC qu'il supporte à l'aide des composantes hors TOE.

1.5.3 Environnement matériel et logiciel

Les composantes de la TOE forment un ensemble de plusieurs modules logiciels qui peuvent se répartir sur une ou plusieurs machines. La TOE est évaluée pour deux types d'architectures matériels possibles qui sont :

- Architecture matérielle 1 : les modules logiciels sont répartis sur des machines distinctes ;
- Architecture matérielle 2 : certains modules logiciels sont répartis sur machines identiques.

A noter que seules les architectures matérielles supportant Trust.Center® et K.Registration® varient selon le type d'architecture système choisie, l'architecture matérielle supportant Keyseed® étant identique quelle que soit l'option retenue (un poste informatique uniquement).

La description est donnée en Annexe A.

1.6 Conformité critères communs

1.6.1 Conformité à des profils de protection

La présente cible de sécurité ne cherche pas une conformité au sens des critères communs avec les profils de protections mentionnés dans ce paragraphe. Cette cible de sécurité s'inspire et s'appuie, pour son élaboration, sur les profils de protection [PP_IGC], [PP_AE], [PP_AC] et [PP_CIMC]. L'utilisation de ces profils de protection vaut pour :

- le périmètre de la cible d'évaluation : identique ;
- la description des biens : plus détaillée dans le présent document ;
- la description des politiques de sécurité : enrichie au regard du contexte d'emploi de la TOE ;
- les hypothèses : plus détaillées dans le présent document ;
- les menaces : le principe de description est celui des [PP_AC], [PP_AE] et [PP_IGC] revu selon [EBIOS] ;
- les objectifs de sécurité : sont un peu plus détaillés que ceux des PP de référence.

1.6.2 Niveau d'évaluation

Niveau d'évaluation visé : EAL4 augmenté du composant ALC_FLR.3. Les classes d'assurance sont prises en compte conformément à la définition du niveau de qualification Standard défini par l'ANSSI [QS].

La version des Critères Communs applicable est la version 3.1 [CC]. Cette cible de sécurité est conforme à la partie 1, 2 et 3 stricte de la version 3.1 des Critères Communs ([CC]).

Note : Ce niveau d'assurance contient l'ensemble des exigences définies par l'ANSSI pour le niveau de qualification standard.

2 DEFINITION DU PROBLEME DE SECURITE

2.1 Biens

La description des biens sensibles est donnée en distinguant les informations et les modules logiciels. En effet, ce sont ces deux types de données qui sont étudiées dans le cadre de la cible d'évaluation.
Tous ces biens sont à protéger en intégrité et en disponibilité. La protection en confidentialité est le cas échéant précisée dans les tableaux ci-dessous.

2.1.1 Bien de la TOE (donnée)

Informations	N°	Description
Certificat d'AC	BTOE 1	Certificat de l'AC pour l'identification et l'authentification des certificats électroniques gérés par la suite logicielle Sequoia®. Cet élément est à protéger en disponibilité et en intégrité.

Informations	N°	Description
Certificat électronique des porteurs de certificat	BTOE 2	Certificat émis par les AC de Trust.Center®.
Certificats des rôles de confiance pour Trust.Center®	BTOE 3	Certificats utilisés pour l'authentification des acteurs ayant un rôle de confiance sur Trust.Center®.
Certificats des rôles de confiance pour K.Registration®	BTOE 4	Certificats utilisés pour l'authentification des acteurs ayant un rôle de confiance sur K.Registration®.
Certificat technique du SA - K.Registration®	BTOE 5	Certificat technique de K.Registration®.
Certificat technique du Proxy d'AE	BTOE 6	Certificat technique du proxy d'AE.
Certificat d'authentification de K.Registration®	BTOE 7	Certificat utilisé par les rôles de confiance et les porteurs de certificat pour authentifiée K.Registration® et mettre en œuvre des connexions SSL.
Certificat technique de Trust.Center®	BTOE 8	Certificat utilisé dans le cadre de la mise en œuvre du protocole XRMP.
Certificat d'authentification de Trust.Center®	BTOE 9	Certificat utilisé par les rôles de confiance et les porteurs de certificat pour authentifier K.Registration® et mettre en œuvre des connexions SSL par les composantes techniques (hors TOE).
Données d'audit Trust.Center®	BTOE 10	Journaux contenant des évènements de sécurité stockés par le module base de données du composant Trust.Center®. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certain rôle de confiance opéré par l'utilisateur de la TOE.
Données d'audit HSS	BTOE 11	Journaux contenant des évènements de sécurité générés par le HSS.
Données d'audit K.Registration®	BTOE 12	Journaux contenant des évènements de sécurité stockés par le module base de données du composant K.Registration®. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certain rôle de confiance opéré par l'utilisateur de la TOE.
Domaine de confiance de Trust.Center®	BTOE 13	La configuration (fichier XML ou saisie par IHM) des domaines de confiance sur Trust.Center® permet de mettre en œuvre un cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certain rôle de confiance opéré par l'utilisateur de la TOE. Cet élément est à protéger en

Informations	N°	Description
		intégrité.
Domaine de confiance de K.Registration®	BTOE 14	La configuration (fichier XML ou saisie par IHM) des domaines de confiance sur K.Registration® permet de mettre en œuvre un cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certain rôle de confiance opéré par l'utilisateur de la TOE. Cet élément est à protéger en intégrité.
Offre de certification	BTOE 15	L'offre de certification de K.Registration® est un fichier de configuration de l'AE qui permet de mettre en œuvre les processus de gestion des demandes des acteurs de la TOE. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certains rôles de confiance opérés par l'utilisateur de la TOE.
Script de cérémonie des clés	BTOE 16	Données insérées dans le composant KeySeed®, lors des cérémonies des clés, afin de générer des certificats d'AC et des LAR.
Profil de certificat dans Trust.Center®	BTOE 17	Contenu attendu ou prédéfini et forme type des certificats supportés par une ou des AC. Les formats de certificats sont conformes aux RFC 3280 et RFC 3739.
Profil de certificat dans K.Registration®	BTOE 18	Contenu attendu ou prédéfini et forme type des certificats supportés par une ou des AC. Les formats de certificats sont conformes aux RFC 3280 et RFC 3739. Ce profil est dépendant du bien (B22).
Profil de LCR pour le Trust.Center® (B25)	BTOE 19	Contenu et forme type des LCR supportées par une ou des AC, K.Registration® et Trust.Center®. Les formats de LCR sont conformes aux RFC 3280 et RFC 3739.
Définition des rôles de confiance de Trust.Center®	BTOE 20	L'attribution des droits pour chacun des rôles de confiance définis sur Trust.Center®.
Définition des rôles de confiance de K.Registration®	BTOE 21	L'attribution des droits pour chacun des rôles de confiance définis sur K.Registration®.
Demande de certificat pour Trust.Center®	BTOE 22	Des demandes de certificat qui sont produites par des rôles de confiance sur Trust.Center®. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certain rôle de confiance opéré par l'utilisateur de la TOE.
Demande de révocation pour Trust.Center®	BTOE 23	Des demandes de révocation qui sont produites par des rôles de confiance sur Trust.Center®. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certain rôle de confiance opéré par l'utilisateur de la TOE.
Demande de certificat de	BTOE 24	Les demandes de certificat sont produites par K.Registration® à destination du proxy d'AE. Cet élément est à protéger en confidentialité

Informations	N°	Description
K.Registration®		au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certain rôle de confiance opéré par l'utilisateur de la TOE.
Demande de certificat XRMP pour Trust.Center®	BTOE 25	Les demandes de certificat sont produites par un proxy d'AE à destination de Trust.Center®. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certain rôle de confiance opéré par l'utilisateur de la TOE.
Demande de révocation de K.Registration®	BTOE 26	Les demandes de révocation sont produites par K.Registration® à destination du proxy d'AE. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certain rôle de confiance opéré par l'utilisateur de la TOE.
Demande de révocation XRMP pour Trust.Center®	BTOE 27	Les demandes de révocation sont produites par un proxy d'AE à destination de Trust.Center®. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certain rôle de confiance opéré par l'utilisateur de la TOE.
Requête de signature SA-Trust.Center® vers HSS	BTOE 28	Les demandes de certificat et de révocation reçues par le SA-Trust.Center® à l'aide du protocole XRMP font l'objet de requêtes transmises au HSS pour signature.
Paramètres de configuration pour l'administration de Trust.Center®	BTOE 29	Paramètres permettant la configuration des composants logiciels de Trust.Center®. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certain rôle de confiance opéré par l'utilisateur de la TOE.
Paramètres de configuration pour l'administration de K.Registration®	BTOE 30	Paramètres permettant la configuration des composants logiciels de K.Registration®. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certain rôle de confiance opéré par l'utilisateur de la TOE.
Paramètres de configuration pour l'administration de KeySeed®	BTOE 31	Paramètres permettant la configuration des composants logiciels de KeySeed®. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou de certain rôle de confiance opéré par l'utilisateur de la TOE.
Données d'authentification d'un porteur de certificat	BTOE 32	Données permettant à un porteur de certificat de s'authentifier auprès de la TOE afin de faire une demande de certificat ou une révocation de certificat. Cette information est à protéger en confidentialité.
Règles de routage du Proxy d'AE	BTOE 33	Configuration du proxy d'AE pour transmettre au Trust.Center® les demandes de certificat et de révocation.
Règles de rouage du HSS	BTOE 34	Configuration du HSS pour transmettre au HSM les requêtes de signatures.

Informations	N°	Description
Liste de Certificat Révoqués	BTOE 35	Listes électroniques émises par l'AC afin que les utilisateurs de la TOE puissent ne plus faire confiance dans les certificats contenus dans cette liste.
Site web AET (Trust.Center®)	BTOE 36	Donnée de configuration du Trust.Center® qui permet de créer les IHM du site web AET.
Site web ATC (Trust.Center®)	BTOE 37	Donnée de configuration du Trust.Center® qui permet de créer les IHM du site web ATC.
Site web Administration (K.Registration®)	BTOE 38	Donnée de configuration du K.Registration® qui permet de créer les IHM du site web Administration.
Site web Opération (K.Registration®)	BTOE 39	Donnée de configuration du K.Registration® qui permet de créer les IHM du site web Opération.
Site web Utilisateur (K.Registration®)	BTOE 40	Donnée de configuration du K.Registration® qui permet de créer les IHM du site web Utilisateur.
Site web Service web (K.Registration®)	BTOE 41	Donnée de configuration du K.Registration® qui permet de créer les IHM du site web Service web.
Clé privée technique Proxy d'AE	BTOE 42	Clé privée de signature et de chiffrement du proxy d'AE utilisée pour la signature des demandes de certificat auprès du Trust.Center®. Cet élément est à protéger en confidentialité.
Clé privée d'authentification de K.Registration®	BTOE 43	Clé privée de K.Registration® utilisée pour la mise en œuvre des sessions SSL par les composantes techniques (hors TOE). Cet élément est à protéger en confidentialité.
Clé privée technique du SA - Trust.Center®	BTOE 44	Clé privée de signature et de chiffrement utilisée dans le cadre de la mise en œuvre du protocole XRMP. Cet élément est à protéger en confidentialité.
Clé privée d'authentification du Trust.Center®	BTOE 45	Clé privée du Trust.Center® utilisée pour la mise en œuvre des sessions SSL par les composantes techniques (hors TOE). Cet élément est à protéger en confidentialité.
Clé privée technique du SA - K.Registration®.	BTOE 46	Clé privée de signature et de chiffrement du SA - K.Registration® utilisée pour la signature des demandes de certificat auprès du proxy d'AE et pour les autres utilisations cryptographique du SA - K.Registration®. Cet élément est à protéger en confidentialité.

2.1.2 Biens de la TOE (logiciel)

Logiciel	N°	Description

Logiciel	N°	Description
Log_appli_ Trust.Center	BL1	Module logiciel du serveur applicatif pour Trust.Center®
Log_appli_K.Registration®	BL2	Module logiciel du serveur applicatif pour K.Registration®
Log_HSS	BL3	Module logiciel du serveur cryptographique pour Trust.Center®
Log_Keyseed	BL4	Module logiciel KeySeed®
Log_Proxy d'AE	BL5	Module logiciel proxy d'AE

2.1.3 Biens de l'environnement de la TOE

Informations	Description
Parts de secret (HSM) (BE1)	n éléments secrets détenus par des porteurs de secret et qui permettent la réalisation d'opérations sous multiples contrôles sur un HSM. Ces éléments sont à protéger en confidentialité.
Clé privée de signature AC (BE2)	Clé privée de l'AC pour la signature protégée par un HSM ou transportée de manière chiffrée. Cet élément est à protéger en confidentialité, en intégrité et en disponibilité.
Clé privée des rôles de confiance pour le Trust.Center® (BE 3)	Clé privée utilisée par le rôle de confiance pour mettre en œuvre les fonctions du SA - Trust.Center®.
Clé privée des rôles de confiance pour K.Registration® (BE 4)	Clé privée utilisée par le rôle de confiance pour mettre en œuvre les fonctions du SA – K.Registration®.
Cle(s) privée(s) des porteurs de certificats électroniques (BE 5)	Clé(s) privée(s) utilisée(s) par le porteur de certificat(s) électronique(s) pour mettre en œuvres des fonctions de sécurité.

Ces biens sont à protéger en intégrité et en disponibilité. La confidentialité de ces biens est également à assurer pour la partie code source du logiciel.

2.2 Utilisateur

2.2.1 Utilisateur de la TOE

Les utilisateurs de la TOE sont :

- Utilisateur « Porteur de certificat » : c'est une personne physique ou morale qui utilise certaines fonctions de la TOE pour ses besoins relatifs aux certificats qu'elle souhaite avoir ou qu'elle possède. Il agit conformément à la politique de certification et à la déclaration des pratiques de certification dont elle dépend ;

- Utilisateur avec un rôle de confiance « administrateur » : 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 politique de certification utilisées pour la mise en œuvre des services de la TOE. Sequoia met aussi en œuvre pour certain de ces modules un « administrateur root » qui sert pour la gestion des rôles du module ;

- Utilisateur avec un rôle de confiance « opérateur » : réalise l'exploitation de tout ou partie des fonctions offertes par des modules de la TOE, dans le cadre de ses attributions. Ce peut être une machine ou une personne (englobe le cas du SI client) ;

- Utilisateur avec un rôle de confiance « auditeur » : réalise les opérations de vérification de la bonne application de la politique de certification effectuée par les modules de la TOE.

Toutes les composantes logicielles de la TOE utilisent ces rôles quelques soit la configuration de déploiement (choix des modules, configuration matérielle ou architecture séparée ou groupée).

2.2.2 Utilisateur de l'environnement de la TOE

Les acteurs de l'environnement de la TOE sont les suivants :

- PSCO : organisme qui déploie la TOE et l'intègre au sein d'un système d'information. Il est responsable de l'utilisation de la TOE et de son utilisation par le système d'information suivant, en outre, les hypothèses et politiques de sécurité organisationnelles données dans la présente cible de sécurité. Un utilisateur de la TOE peut aussi être un Client du PSCO qui utilise la TOE hébergée par un PSCO et qui possède des rôles de confiance sur la TOE (définis ci-après) pour la mise en œuvre de sa politique de certification et de la déclaration des pratiques de certification ;

- Responsable de sécurité : est responsable de l'application de la politique de sécurité physique et fonctionnelle de la TOE et de son environnement. Par exemple, il gère les contrôles d'accès physiques à la plate-forme de la TOE. 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 ;

- Administrateur système : 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® ;

- Porteur de données d'activation (porteur de secret) : ce sont les rôles définis en fonction du module cryptographique pour la mise en œuvre et la gestion du module cryptographique utilisé par la TOE (BE1 à BE5) ;

- Développeur : est responsable du code source des logiciels des modules logiciel de la TOE (BL1 à BL5). Il est également en charge de la gestion en configuration des logiciels de la TOE, de la distribution des versions successives aux utilisateurs et de l'information, auprès des utilisateurs, lors de la découverte de problèmes trouvés dans les logiciels.

2.3 Typologie des attaquants

Les attaquants peuvent être « internes » ou « externes » à la TOE selon qu'ils sont sous le champ de responsabilité du PSCO ou non. Un attaquant est à l'origine de la réalisation d'une menace de manière volontaire ou involontaire.

Les attaquants sont des personnes physiques disposant d'un potentiel d'attaque de niveau élémentaire ce qui correspond à des personnes malintentionnées disposant des compétences informatiques d'une personne avertie.

2.3.1 Attaquant interne

Les entités internes pouvant nuire à la TOE sont les suivantes :

- Des acteurs de la TOE.

Il est nécessaire de couvrir des attaques techniques qui permettraient à un acteur autorisé de renier une action sur un service de la TOE ou de modifier des services de la TOE. Les acteurs concernés dans ce cas

sont ceux qui utilisent les modules de la TOE qui font partie de la cible d'évaluation et qui pourraient utiliser des vulnérabilités de la TOE ou des services de chacun des modules de la TOE.

2.3.2 Attaquant externe

Les entités externes pouvant nuire à la TOE sont les suivantes :

- Des acteurs de l'environnement de la TOE ;
- Des personnes physiques qui ne sont pas acteur de la TOE

2.4 Menaces

Ce paragraphe est décomposé en deux parties de la manière suivante :

- Menaces génériques : cette partie reprend la guide EBIOS v2 afin d'en extraire les méthodes d'attaque retenues pour la présente TOE. Cette partie est introduite afin de mieux positionner la cible d'évaluation au sein de l'analyse de risque globale qui portera sur le système d'information qui héberge la TOE ;
- Menaces sur la TOE : cette partie décrit les menaces qui portent sur la TOE à partir des menaces génériques, des biens et des garanties définies pour la TOE. Elle permet de particulariser les menaces génériques sur la TOE.

Nota : les nombres utilisés pour la notation correspondent à la numérotation utilisée par la méthode **[EBIOS v2]**

2.4.1 Menaces génériques

La liste des menaces retenues pour la TOE est extraite des méthodes d'attaques au sens du guide **[EBIOS v2]**. Elles sont explicitées par la suite au regard des biens sensibles (Cf. § 2.3.2) de la TOE.

En effet, la TOE est une suite logicielle mise en œuvre au sein d'un ou de plusieurs systèmes d'information du PSCO et/ou du promoteur d'application. Par conséquent les menaces non retenues pour la TOE sont prises en comptes dans l'analyse de risque du PSCO et/ou du promoteur d'application, l'un comme l'autre devant respecter au minimum les exigences de la présente cible de sécurité.

Les menaces applicables à la TOE sont les suivantes :

- Thème 5 – Compromission des informations
  - 19 – Ecoutes passives
  - 23 - Divulgation
  - 24 – Informations sans garanties d'origines
  - 26 – Piégeage du logiciel
- Thème 6 – Défaillances techniques
  - 31 – Dysfonctionnement logiciel
- Thème 7 – Actions illicites
  - 36 – Altération des données
- Thème 8 – Compromission des fonctions
  - 38 – Erreur d'utilisation
  - 39 – Abus de droit
  - 40 – Usurpation de droit
  - 41 – Reniement d'action

L'attaquant à l'origine des menaces listées ci-dessus est un attaquant comme décrit dans le § 2.3.

Les menaces qui portent sur des composants en ligne de la TOE, dont la réalisation est effectuée à l'aide d'un moyen connecté, ne sont pas prise en compte lors de l'évaluation pour le composant Keyseed®.

Les menaces qui portent sur l'environnement de la TOE sont prises en compte par des hypothèses qui font l'objet d'une vérification par expertise lors de l'évaluation certification.

2.4.2 Menaces sur la TOE

2.4.2.1 M_Rôle_de_confiance (40)

Un attaquant (externe) se fait reconnaître comme rôle de confiance sur la TOE afin d'utiliser ou d'altérer des fonctions des modules de la TOE. L'attaquant peut ainsi porter atteinte à la confidentialité, l'intégrité, l'imputabilité et la disponibilité des données et de tout ou parties des services de la TOE.

Cette menace concerne tous les biens de la TOE.

2.4.2.2 M_Rôle_de_confiance autorisé (39)

Un attaquant (interne) autorisé par son rôle de confiance accède aux fonctions des modules de la TOE afin d'utiliser ou d'altérer des fonctions des modules de la TOE. L'attaquant peut ainsi porter atteinte à la confidentialité, l'intégrité, l'imputabilité et la disponibilité des données et de tout ou parties des services de la TOE.

Cette menace concerne les biens BTOE 3, BTOE 4, BE 3, BTOE 5, BTOE 6, BTOE 7, BE 5, BTOE 8, BTOE 9, BTOE 10, BTOE 11, BTOE 12,, BTOE 14, BTOE 15, BTOE 16 et BTOE 17.

2.4.2.3 M_Journalisation (41)

Un attaquant (interne) met en œuvre des fonctions des modules de la TOE et renie cette action en portant atteinte aux données nécessaires à l'élaboration de traces d'audits et de preuves. Cette menace altère les garanties d'imputabilité de la TOE qui porte sur les services de la TOE ainsi que sur sa capacité à mettre en œuvres différentes politiques de certification (services d'IGC) pour des utilisateurs de la TOE différents.

Cette menace concerne les biens BTOE 10, BTOE 11 et BTOE 12.

2.4.2.4 M_Erreur_d'utilisation (38, 39 et 31)

Un utilisateur commet une erreur lors de l'utilisation des fonctions des modules de la TOE entraînant une utilisation non conforme des fonctions de la TOE. L'attaquant peut ainsi porter atteinte à la confidentialité, l'intégrité (pour les biens que l'attaquant n'est normalement pas autorisé à gérer), l'imputabilité et la disponibilité des données et de tout ou parties des services de la TOE.

Cette menace concerne l'ensemble des biens BTOE 1 à BTOE 46.

2.4.2.5 M_Altération_des_biens (36 et 26)

Un attaquant (interne ou externe) accède aux moyens de communication des modules de la TOE et altère la transmission des informations (par interception, insertion, destruction, …) qui circulent entre les modules de la TOE, entre les modules de la TOE et son environnement, entre les modules de la TOE et les rôles de confiance de la TOE ou altère les biens de la TOE. L'attaquant peut ainsi porter atteinte à la confidentialité, l'intégrité (pour les biens que l'attaquant n'est normalement pas autorisé à gérer), l'imputabilité et la disponibilité des données et de tout ou parties des services de la TOE.

Cette menace concerne tous les biens BTOE 1 à BTOE 46, BE 1 à BE 5.

2.4.2.6 M_Autorisation (24)

Un attaquant (interne ou externe) introduit des données (données telles que des biens, données non connues de la TOE, données qui sont des instructions machines, …), destinées à être intégrées et/ou interprétées dans les composants logicielles de la TOE, pour altérer l'identification et l'authentification des rôles de confiance et des porteurs de certificat et ainsi porter atteinte à la fiabilité de la TOE ou à la validité de ses informations. L'attaquant peut ainsi porter atteinte à la confidentialité, l'intégrité, l'imputabilité et la disponibilité des données et de tout ou parties des services de la TOE.

Cette menace concerne les biens BTOE 1 à BTOE 46.

2.4.2.7 M_Divulgation (23 et 19)

Un attaquant (interne ou externe) diffuse des biens de la TOE à d'autres modules de la TOE non censé gérer les données reçues ou à l'extérieur de la TOE. L'attaquant peut ainsi porter atteinte à la confidentialité, l'intégrité, l'imputabilité et la disponibilité des données et de tout ou parties des services de la TOE.

Cette menace concerne les biens BE 1 à BE 5, BTOE 10, BTOE 11, BTOE 12, BTOE 13, BTOE 14, BTOE 15, BTOE 17, BTOE 18, BTOE 19, BTOE 20, BTOE 21, BTOE 22, BTOE 23, BTOE 24, BTOE 25, BTOE 26, BTOE 27, BTOE 28, BTOE 29, BTOE 30, BTOE 31, BTOE 32, BTOE 33, BTOE 34, BTOE 42, BTOE 43, BTOE 44, BTOE 45 et BTOE 46.

2.5 Politique de sécurité organisationnelles (OSP)

2.5.1 Politiques relatives aux services offerts

2.5.1.1 OSP_Services de certification

Les composantes de la TOE K.Registration®, Trust.Center® et Keyseed®, indépendamment les unes des autres ou en interaction entre elles (cf. § 1.5.2), permettent de mettre en œuvre des services d'IGC au regard de politiques de certification et de déclaration des pratiques.

2.5.1.2 OSP_Cloisonnement

Les composantes de la TOE K.Registration® et Trust.Center® doivent mettre en œuvre un mécanisme de contrôle d'accès basé sur des règles de filtrage. Elle doit permettre de définir plusieurs niveaux de filtrage. Ces règles de contrôle d'accès doivent prendre en compte les critères relatifs aux utilisateurs (rôles détenus sur un domaine de confiance). Les composantes de la TOE K.Registration® et Trust.Center® doivent également permettre de faire du filtrage de donnée exportées en fonction du rôle de l'utilisateur de ces composantes de la TOE.

2.5.1.3 OSP_Rôles

Les composantes de la TOE K.Registration® et Trust.Center® doivent distinguer au minimum les rôles d'administrateur, d'auditeur, d'opérateur et d'utilisateur par domaine de confiance. Elle doit permettre de tracer les actions réalisées par les titulaires de ces rôles.

2.5.1.4 OSP_Admin

Les composantes de la TOE K.Registration® et Trust.Center® doivent permettre d'administrer, localement ou à distance, leur configuration et leurs règles de contrôle d'accès. La configuration et les règles de contrôles d'accès doivent pouvoir être visualisées par un rôle administrateur autorisé. L'accès et l'utilisation des fonctions d'administration doivent être contrôlés et uniquement autorisés pour un rôle de type Administrateur en fonction de son appartenance à un domaine de confiance sur la composante de la TOE K.Registration® ou Trust.Center®. Un administrateur de la composante K.Registration® n'a pas forcément accès aux fonctions d'Administration de la composante Trust.Center® et réciproquement.

2.5.1.5 OSP_Audit_admin

Les composantes de la TOE K.Registration® et Trust.Center® doivent tracer les actions d'administration conduisant à une modification de la configuration de la TOE (BTOE 14 et BTOE 15). Elle doit permettre de sélectionner, ordonner et visualiser ces données selon différents critères (date et acteur) et uniquement au profit des rôles autorisés Administrateur et Auditeur en fonction de l'appartenance à un domaine de confiance sur la composante de la TOE K.Registration® ou Trust.Center®.

2.5.1.6 OSP_Audit_flux

Les composantes de la TOE K.Registration® et Trust.Center® doivent pouvoir tracer les flux qu'elles traitent dans le cadre de la politique de sécurité (configuration des machines hôtes). Elle doit permettre de sélectionner, ordonner et visualiser ces données selon différents critères (horodatage, acteur, adresse réseau, application, protocole, acceptation ou rejet du flux). Ces traces d'audit sont consultables uniquement par le rôle Administrateur system autorisé sur la machine hôte des composantes.

2.5.1.7 OSP_Configuration_sûre

Les composantes de la TOE doivent pouvoir être réinstallées et reconfigurées permettant ainsi de disposer sur les machines hôtes d'une TOE dans un état sûr.

2.5.1.8 OSP_Sauvegarde

Les composantes de la TOE K.Registration® et Trust.Center® permettent de générer et conserver les biens de la TOE (Cf. § 2.1.1., BTOE 1 à BTOE 41) afin de pouvoir sauvegarder et restaurer la TOE à partir des données contenues dans le SBD.

2.5.1.9 OSP_Rôles de confiance

En fonction du rôle de confiance, le certificat du rôle de confiance est signé soit par une AC techniques de la TOE, soit par une AC déclarée de confiance au niveau de la TOE. Ces certificats sont régis conformément à une PC.

2.5.1.10 OSP_Service cryptographique TOE

Le TOE met en œuvre les protocoles d'accès (Pkcs#11 …) au HSM de manière à ne pas en compromettre les clés privées (par exemple, sélection des commandes, gestion des attributs des objets de la clé privée, export de tout ou parties d'une clé via des données entrantes ou sortante de la TOE, …).

2.5.2 Politique issues de la réglementation applicable

2.5.2.1 OSP_Crypto

Les mécanismes cryptographiques des modules de la TOE ou ceux mis en œuvre par la TOE (SSL, …) doivent être conformes aux exigences du référentiel cryptographique de l'ANSSI pour le niveau de robustesse standard [CRYPT_STD]. Les modules de la TOE doivent être conformes aux exigences du référentiel [CRYPT_GC] de l'ANSSI concernant la gestion des clés cryptographiques et aux exigences du référentiel [AUTH] de l'ANSSI concernant les mécanismes d'authentification. L'insertion de données d'activation (détenues par les porteurs de des secrets) ne peut pas se faire via les composantes de la TOE.

2.6 Hypothèses

2.6.1 Hypothèses concernant le personnel

2.6.1.1 H_Administrateur système

Les personnels ayant un rôle Administrateur Système sur les machines hôtes hébergeant les composantes de la TOE doivent être de confiance. Ils doivent disposer de la formation et des éléments nécessaires pour assurer correctement leur mission.

2.6.1.2 H_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. Ils doivent disposer de la formation et des éléments nécessaires pour assurer correctement leur mission.

2.6.1.3 H_Attribution de rôle

Les utilisateurs de l'environnement de la TOE (Cf. § 2.2.2) ne peuvent pas avoir de rôle de type « utilisateur de la TOE » (Cf. § 2.2.1) hormis « Porteur de certificat ».

2.6.2 Hypothèses concernant l'environnement TI

2.6.2.1 H_Machines hôtes

Les machines hôtes hébergeant les composantes de la TOE doivent leur fournir les ressources nécessaires à son fonctionnement.

L'accès aux fonctions d'administration des machines hôtes est restreint aux seuls administrateurs systèmes de celles-ci.

L'installation et la mise à jour de logiciels sur les machines hôtes est sous le contrôle de l'administrateur systèmes.

Les machines hôtes doivent journaliser les actions réalisées sur la TOE (en tant que logiciel hébergé par les machines hôtes) et sur les logiciels hôtes de la TOE.

Les machines hôtes doivent être configurées à l'état de l'art des règles de configuration et de protection pour parer les vulnérabilités publiques.

Les machines hôtes utilisées pour la mise en œuvre des modules logiciels de la TOE ne doivent supporter aucuns autres logiciels applicatifs.

2.6.2.2 H_Réseau

Les échanges entre les machines hôtes qui hébergent la TOE (K.Registration® et Trust.Center®) avec les machines hôtes qui hébergent la TOE (K.Registration® et Trust.Center®) et avec d'autres machines de l'environnement de la TOE via un réseau sont contrôlés par des pare feu contrôlant et limitant les échanges.

2.6.2.3 H_Sauvgarde

Les administrateurs de la TOE doivent disposer de moyens permettant de sauvegarder, contrôler par rapport à un état de référence, et restaurer une configuration de la TOE et les biens de la TOE (Cf. § 2.1) à partir des données issues du service SBD de chacune des composantes de la TOE (Trust.Center® et K.Registration®), des biens de la TOE (BL1 à BL5) et des données des machines hôtes des composantes de la TOE.

Les sauvegardes du SBD de la composante K.Registration® doivent être protégées en confidentialité car elles contiennent des informations sensibles (Cf. **Erreur ! Source du renvoi introuvable.**).

2.6.2.4 H_machine hôte Keyseed®

Le système d'exploitation de la machine hôte offre des contextes d'exécution séparés pour les différentes tâches qu'il exécute. On suppose de plus que les mesures suivantes sont appliquées :

- La machine hôte utilisée pour la mise en œuvre du module logiciel de la composante Keyseed® de la TOE doit servir uniquement pour le module logiciel de cette composante ;
- La machine hôte opérationnelle qui héberge Keyseed® ne doit jamais être connectée à aucun réseau (Internet, intranet, wifi, …) ;
- La machine hôte journalise les actions réalisées sur Keyseed® (en tant que logiciel hébergé par la machine hôte) et sur les logiciels hôtes de la TOE.

2.6.2.5 H_machine hôte Trust.Center®

L'adresse IP du SI Client est connue à l'avance et permet de mettre en place des règles de filtrage réseau, à l'aide de pare-feux, entre le SI Client et la composante Trust.Center®. La communication entre le SI Client et le Trust.Center® est réalisée en utilisant le protocole XRMP.

Les machines hôtes journalisent les actions réalisées sur chacun des modules logiciels du Trust.Center® (en tant que logiciel hébergé par la machine hôte) et sur les logiciels hôtes de chacun des modules logiciels du Trust.Center®.

2.6.2.6 H_machine hôte K.Registration®

Les machines hôtes journalisent les actions réalisées sur chacun des modules logiciels du K.Registration® (en tant que logiciel hébergé par la machine hôte) et sur les logiciels hôtes de chacun des modules logiciels du K.Registration®.

2.6.2.7 H_Client XRMP

Le Client qui possède un SI connecté à la composante Trust.Center® implémente un client XRMP conformément aux spécifications et aux guides élaborés par KEYNECTIS.

2.6.2.8 H_SI Client

L'environnement du SI Client doit assurer l'identification et l'authentification des utilisateurs qui se connectent, localement ou à distance, au machine du SI Client qui interagissent avec le Trust.Center®. Le Client protège suffisamment les clés techniques qui permettent de mettre en œuvre la sécurité demandée par le protocole XRMP.

2.6.2.9 H_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. Le temps de référence est une approximation locale du temps UTC qui est obtenue à partir d'une ou plusieurs sources de temps dont la précision est connue par rapport à une ou plusieurs sources UTC(k). A titre informatif, l'établissement d'un temps de référence peut par exemple utiliser :

- Une horloge située dans l'environnement contrôlé du système d'horodatage garantissant la précision attendue pendant toute la durée de vie des unités du système d'horodatage (une horloge atomique par exemple),
- Une source de temps externe authentifiée (accessible via le protocole NTP et une liaison VPN par exemple),
- Un nombre supérieur ou égal à trois de sources de temps externes non authentifiées de natures différentes (serveurs NTP, sources radio,…) dont les valeurs sont combinées au travers d'un algorithme de décision (par vote majoritaire dans le cas d'un nombre impair de sources par exemple).

Exception : le module logiciel Keyseed est hébergé sur une machine hôte qui n'est pas connectée au réseau et de ce fait ne peut être synchronisée automatiquement par rapport au temps UTC. Des consignes organisationnelles d'exploitation doivent être mises en œuvre afin de s'assurer de la conformité du temps de la machine hôte avec le temps UTC.

2.6.2.10 H_ Service cryptographique_AC (HSM)

Le HSM a pour fonction de générer, protéger, détruire, importer, exporter des clés cryptographiques et de permettre leur utilisation de manière sûre à partir des éléments communiqués par la TOE.

Le module cryptographique est également en charge de l'authentification de l'ensemble des rôles de confiance qu'il utilise (porteur de données d'activation) pour la création et la gestion des clés d'AC.

Les données suivantes sont stockées et utilisées de manière sûre par le module cryptographique :

- Biens relatifs à la génération de la signature :
  - o les clés privées des AC, protégées en confidentialité et en intégrité ;
  - o les certificats des AC, protégés en intégrité, à défaut une référence non ambiguë à ces certificats ;
  - o l'association clé privée/certificat, protégée en intégrité ;
- Biens relatifs aux services du HSS ou de Keyseed® :
  - o Des clés secrètes ;

On suppose que l'ensemble des composants logiciels et/ou matériels assurant l'interface entre la TOE et le module cryptographique gère (ouvrir/fermer) un canal de communication garantissant l'intégrité et l'exclusivité de la communication. Les modules cryptographiques sont administrés par des postes d'administrations dédiés à ce type d'opération. L'importation et l'exportation des clés cryptographique par le HSM, ne peut pas se faire sur demande des composantes de la TOE (K.Registration® et Trust.Center®). Seul le composant Keyseed® peut demander l'exportation de clé cryptographique au HSM, lorsque la fonction d'exportation est prévue par le HSM. Dans tous les cas, le HSM est conçu de telle manière que l'importation et l'exportation des clés cryptographiques doivent nécessiter au moins un porteur de donnée d'activation avec son secret pour réaliser l'opération.

2.6.2.11 H_bi-clés_Rôle de confiance

Les rôles de confiance de type ; « Administrateur », « Opérateur » et « Auditeur » qui sont détenus par des personnes physiques ou des machines, qui utilisent les services de la TOE, possèdent chacun une bi-clé et un

certificat associé sur carte à puce pour les personnes physique, une bi-clé et un certificat associé dans un module cryptographique logiciel ou matériel pour les machines.

2.6.2.12 H_Protection d'une clé privée associée à un certificat

Les rôles de confiance (humain et machine) sont responsables de la protection en confidentialité, en intégrité et en disponibilité des clés privées associées aux certificats qu'ils détiennent. Ces certificats sont soit délivrés par la TOE soit obtenus d'une autre IGC. Les clés privées sont dans tous les cas utilisées par l'acteur pour mettre en œuvre des fonctions de la TOE.

2.6.3 Hypothèses concernant l'environnement non TI

2.6.3.1 H_Politique de certification

Le promoteur d'application ou le PSCO définit et met en œuvre un ensemble de Politiques de Certification (PC) - Déclarations des Pratiques de Certification (DPC) pour les certificats émis et gérés à l'aide de la TOE pour définir :

- L'organisation générale de l'IGC dans laquelle intervient la TOE. Cette organisation concerne notamment les échanges de biens (Cf. § 2.3.2) entre la TOE et les autres composantes de l'IGC ;
- Les AC qui seront utilisées pour la signature des certificats, des LCR et des LAR ;
- Les formats de certificat, de LCR et de LAR ;
- Les rôles de confiance et les opérations à réaliser sur la TOE ;
- Les contraintes temporelles qui sont imposées à la TOE (période de validité d'un certificat, temps de révocation, …) ;
- La sécurité physique et logique du système d'information qui héberge les composants de la TOE.

2.6.3.2 H_Protection physique de la TOE

L'environnement de la TOE doit assurer une protection physique suffisante afin de limiter les risques d'attaque contre l'intégrité de la TOE (matériels et supports de données) par des personnels non habilités à accéder physiquement aux machines qui mettent en œuvre la TOE.

3 OBJECTIFS DE SECURITE

3.1 Objectif de sécurité pour la TOE

O.SERVICES : Les fonctions des modules de la TOE doivent permettre à la TOE de réaliser l'ensemble des services d'IGC (Cf. § 1.4.2) conformément aux différentes PC et DPC supportées. Les modules de la TOE doivent permettre d'émettre des certificats et des LCR signés par les AC mises en œuvre par la TOE conformément aux PC et DPC supportées par la TOE.

O.ADMINISTRATION : Les modules de la TOE doivent permettre leur initialisation et leur configuration par les seuls rôles de confiances autorisés afin de garantir le respect du cloisonnement entre les rôles de confiances pour la mise en œuvre des fonctions des modules de la TOE. Les modules de la TOE doivent pouvoir être initialisés et configurés afin de garantir la confidentialité (lorsque cela est nécessaire), la disponibilité et l'intégrité des biens qu'elle va gérer.

O.AUDIT : Les modules de la TOE doivent permettre d'auditer les évènements issus de la mise en œuvre de la configuration et des fonctions de chacun des modules de la TOE qui concourent à la sauvegarde. Toutes les opérations réalisées à l'aide de fonctions (traitement de données et flux entre la composante K.Registration® et Trust.Center®) des modules de la TOE par les rôles de confiances doivent être tracée, et imputable (identifiant du rôle de confiance, date et heure, opération réalisée, …) à son auteur. L'intégrité, la disponibilité et la confidentialité (besoin d'en connaître) des traces doit être garantie par la TOE afin d'éviter que des rôles de confiances de la TOE puissent, via les fonctions des modules de la TOE, altérer des données d'audits ou en prendre connaissance s'ils n'y sont pas autorisés.

O.AUTHENTIFICATION : Les modules de la TOE doivent identifier et authentifier, de manière unique, les entités ayant un rôle de confiance pour la mise en œuvre des fonctions de ces modules.

O.AUTORISATION : Suite à l'authentification et l'identification d'un rôle de confiance, les modules de la TOE doivent restreindre les fonctions qu'un rôle de confiance peut mettre en œuvre en fonction de ses droits liés à son certificat de rôle de confiance qui est déclaré dans le module de la TOE.

O.PROTECT_DONNEES : Les modules de la TOE doivent permettre de garantir que les biens gérés par les modules sont accessibles aux rôles de confiance de la TOE (administrateur, opérateur et auditeur) uniquement par la mise en œuvre des fonctions des modules de la TOE. De même, les modules de la TOE doivent permettre de rendre inaccessibles des données confidentielles manipulées lorsqu'un rôle de confiance a terminé un traitement. De même, les modules de la TOE doivent s'assurer de la cohérence et de l'intégrité des formats de données utilisés pour les biens gérés et échangés entre les modules de la TOE et entre les modules de la TOE et leur environnement. La TOE doit aussi permettre aux acteurs d'authentifier tous les biens qu'elle publie (ou met à disposition). Les clés privées sont utilisées de manière sûre par le module cryptographique de manière à ne pas porter atteinte à leur confidentialité et leur intégrité.

O.TRANS_DATA : Les modules de la TOE doivent protéger, si nécessaire, en intégrité, en disponibilité et en confidentialité tous les biens échangés entre les module de la TOE ou entre les modules de la TOE et leur environnement. Les modules de la TOE doivent être conçus de manière à contrôler, à l'aide d'interfaces dédiées, l'ensemble des échanges de biens entre les modules distincts de la TOE et entre des modules de la TOE et leur environnement.

O.ESPIONNAGE_DISTANT : Les modules de la TOE doivent limiter l'existence d'interfaces de saisie et d'affichage de données confidentielles. Lorsqu'elles existent, elles doivent être conçues de manière à limiter ou éviter la possibilité d'espionnage visuel.

O.TEMPSREF : les modules de la TOE doivent utiliser un temps de référence unique permettant aux modules de la TOE de délivrer une date et une heure en utilisant une source de temps de confiance.

O.CRYPTO : Les mécanismes cryptographiques des modules de la TOE doivent être conformes aux exigences du référentiel cryptographique de l'ANSSI pour le niveau de robustesse standard [CRYPT_STD]. Les modules de la TOE doivent être conformes aux exigences du référentiel [CRYPT_GC] de l'ANSSI concernant la gestion des clés cryptographiques et aux exigences du référentiel [AUTH] de l'ANSSI concernant les mécanismes d'authentification.

3.2 Objectifs de sécurité pour l'environnement opérationnel

3.2.1 Objectifs concernant le personnel

3.2.1.1 OE_Administrateur système

Les personnels ayant un rôle Administrateur Système sur les machines hôtes hébergeant les composantes de la TOE doivent être de confiance. Ils doivent disposer de la formation et des éléments nécessaires pour assurer correctement leur mission.

3.2.1.2 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. Ils doivent disposer de la formation et des éléments nécessaires pour assurer correctement leur mission.

3.2.1.3 OE_Attribution de rôle

Les utilisateurs de l'environnement de la TOE (Cf. § 2.2.2) ne peuvent pas avoir de rôle de type « utilisateur de la TOE » (Cf. § 2.2.1) hormis « Porteur de certificat ».

3.2.2 Objectifs concernant l'environnement TI

3.2.2.1 OE_Machines hôtes

Les machines hôtes hébergeant les composantes de la TOE doivent assurer une protection suffisante des éléments constituant la TOE (programmes, fichiers de données, journaux) et des éléments nécessaires à son fonctionnement (datation sûre, éléments relatifs aux applications, aux utilisateurs, à la connexion).

Les machines hôtes hébergeant les composantes de la TOE doivent leur fournir les ressources nécessaires à son fonctionnement.

L'accès aux fonctions d'administration des machines hôtes est restreint aux seuls administrateurs systèmes de celles-ci.

L'installation et la mise à jour de logiciels sur les machines hôtes est sous le contrôle de l'administrateur systèmes.

Il existe des fonctions d'audit et de journalisation pour les machines hôtes.

3.2.2.2 OE_Réseau

Les échanges entre les machines hôtes qui hébergent la TOE (K.Registration® et Trust.Center®) avec les machines hôtes qui hébergent la TOE (K.Registration® et Trust.Center®) et avec d'autres machines de l'environnement de la TOE via un réseau sont contrôlés par des pare feu contrôlant, journalisant et limitant les échanges.

3.2.2.3 OE_Sauvegarde

Les administrateurs de la TOE doivent disposer de moyens permettant de sauvegarder, contrôler par rapport à un état de référence, et restaurer une configuration de la TOE et les biens de la TOE (Cf. § 2.1) à partir des données issues du service SBD de chacune des composantes de la TOE (Trust.Center® et K.Registration®).

3.2.2.4 OE_RETOUR_ETAT_SUR

L'environnement de la TOE doit fournir des fonctionnalités permettant un retour dans un état opérationnel sûr (après dysfonctionnement ou panne). Ce retour dans un état opérationnel sûr peut être soit direct soit via un état "maintenance" nécessitant alors une action d'administration de sécurité (réinitialisation ou re-paramétrage de données de sécurité par exemple).

3.2.2.5 OE_machine hôte Keyseed®

Le système d'exploitation de la machine hôte offre des contextes d'exécution séparés pour les différentes tâches qu'il exécute. On suppose de plus que les mesures suivantes sont appliquées :

- La machine hôte utilisée pour la mise en œuvre du module logiciel de la composante Keyseed® de la TOE doit servir uniquement pour le module logiciel de cette composante ;
- La machine hôte opérationnelle qui héberge Keyseed® ne doit jamais être connectée à un autre réseau (Internet, intranet, wifi, …) ;
- La machine hôte doit avoir des fonctions d'audit et de journalisation.

3.2.2.6 OE_machine hôte Trust.Center®

Les machines hôtes utilisées pour la mise en œuvre des modules logiciels de la composante Trust.Center® de la TOE doivent servir uniquement pour les modules logiciels de cette composante.

L'adresse IP du SI Client est connue à l'avance et permet de mettre en place des règles de filtrage réseau, à l'aide de pare-feux, entre le SI Client et la composante Trust.Center®. La communication entre le SI Client et le Trust.Center® est réalisée en utilisant le protocole XRMP.

Les machines hôtes de chaque module logiciel du Trust.Center® doivent avoir des fonctions d'audit et de journalisation.

3.2.2.7 OE_machine hôte K.Registration®

Les machines hôtes utilisées pour la mise en œuvre des modules logiciels de la composante Trust.Center® de la TOE doivent servir uniquement pour les modules logiciels de cette composante.

Les machines hôtes de chaque module logiciel de K.Registration® doivent avoir des fonctions d'audit et de journalisation.

3.2.2.8 OE_Client XRMP

Le Client qui possède un SI connecté à la composante Trust.Center® implémente un client XRMP conformément aux spécifications et aux guides élaborés par KEYNECTIS.

3.2.2.9 OE_SI Client

L'environnement du SI Client doit assurer l'identification et l'authentification des utilisateurs qui se connectent, localement ou à distance, au machine du SI Client qui interagissent avec le Trust.Center®. Le Client protège suffisamment les clés techniques qui permettent de mettre en œuvre la sécurité demandée par le protocole XRMP.

3.2.2.10 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. Le temps de référence est une approximation locale du temps UTC qui est obtenue à partir d'une ou plusieurs sources de temps dont la précision est connue par rapport à une ou plusieurs sources UTC(k). A titre informatif, l'établissement d'un temps de référence peut par exemple utiliser :

- Une horloge située dans l'environnement contrôlé du système d'horodatage garantissant la précision attendue pendant toute la durée de vie des unités du système d'horodatage (une horloge atomique par exemple),
- Une source de temps externe authentifiée (accessible via le protocole NTP et une liaison VPN par exemple),
- Un nombre supérieur ou égal à trois de sources de temps externes non authentifiées de natures différentes (serveurs NTP, sources radio,…) dont les valeurs sont combinées au travers d'un algorithme de décision (par vote majoritaire dans le cas d'un nombre impair de sources par exemple).

3.2.2.11 OE_ Service cryptographique_AC (HSM)

Le HSM a pour fonction de générer, protéger, détruire, importer, exporter des clés cryptographiques et de permettre leur utilisation de manière sûre à partir des éléments communiqués par la TOE.

Le module cryptographique est également en charge de l'authentification de l'ensemble des rôles de confiance qu'il utilise (porteur de données d'activation) pour la création et la gestion des clés d'AC.

Les données suivantes sont stockées et utilisées de manière sûre par le module cryptographique :

- Biens relatifs à la génération de la signature :
  - o les clés privées des AC, protégées en confidentialité et en intégrité ;
  - o les certificats des AC, protégés en intégrité, à défaut une référence non ambiguë à ces certificats ;
  - o l'association clé privée/certificat, protégée en intégrité ;
- Biens relatifs aux services du HSS ou de Keyseed® :
  - o Des clés secrètes ;
- Biens relatifs à l'authentification du signataire :
  - o les données d'authentification du signataire, protégées en intégrité et en confidentialité ;
  - o l'association entre des données d'authentification et le couple clé privée/certificat, protégée en intégrité.

On suppose que l'ensemble des composants logiciels et/ou matériels assurant l'interface entre la TOE et le module cryptographique gère (ouvrir/fermer) un canal de communication garantissant l'intégrité et l'exclusivité de la communication. Les modules cryptographiques sont administrés par des postes d'administrations dédiés à ce type d'opération. L'importation et l'exportation des clés cryptographique par le HSM, ne peut pas se faire sur demande des composantes de la TOE (K.Registration® et Trust.Center®). Seul le composant Keyseed® peut demander l'exportation de clé cryptographique au HSM, lorsque la fonction d'exportation est prévue par le HSM. Dans tous les cas, le HSM est conçu de telle manière que l'importation et l'exportation des clés cryptographiques doivent nécessiter au moins un porteur de donnée d'activation avec son secret pour réaliser l'opération. L'insertion du secret du porteur d'activation ne peut pas se faire via les composantes de la TOE.

3.2.2.12 OE_bi-clés_Rôle de confiance

Les rôles de confiance de type ; « Administrateur », « Opérateur » et « Auditeur » qui sont détenus par des personnes physiques ou des machines, qui utilisent les services de la TOE, possèdent chacun une bi-clé et un certificat associé sur carte à puce pour les personnes physique, une bi-clé et un certificat associé dans un module cryptographique logiciel ou matériel pour les machines.

3.2.2.13 OE_Protection d'une clé privée associée à un certificat

Les porteurs de certificats sont responsables de la protection en confidentialité, en intégrité et en disponibilité des clés privées associées aux certificats qu'ils détiennent. Ces certificats sont soit délivrés par la TOE soit obtenus d'une autre IGC. Les clés privées sont dans tous les cas utilisées par l'acteur pour mettre en œuvre des fonctions de la TOE.

3.2.3 Objectifs concernant l'environnement non TI

3.2.3.1 OE_Protection_physique

L'environnement de la TOE doit assurer une protection physique suffisante afin de limiter les risques d'attaque contre l'intégrité de la TOE (matériels et supports de données).

3.2.3.2 OE_Politique de certification

Le promoteur d'application ou le PSCO définit et met en œuvre un ensemble de Politiques de Certification (PC) - Déclarations des Pratiques de Certification (DPC) pour les certificats émis et gérés à l'aide de la TOE pour définir :

- L'organisation générale de l'IGC dans laquelle intervient la TOE. Cette organisation concerne notamment les échanges de biens (Cf. § 2.3.2) entre la TOE et les autres composantes de l'IGC ;
- Les AC qui seront utilisées pour la signature des certificats, des LCR et des LAR ;
- Les formats de certificat, de LCR et de LAR ;
- Les rôles de confiance et les opérations à réaliser sur la TOE ;
- Les contraintes temporelles qui sont imposées à la TOE (période de validité d'un certificat, temps de révocation, …) ;
- La sécurité physique et logique du système d'information qui héberge les composants de la TOE.

4 EXIGENCES

4.1 Introduction

La figure ci-dessous identifie les différents modules de la suite logicielle Sequoia®. Les composantes de la TOE sont constituées de plusieurs modules logiciels. Les modules logiciels (composantes de la TOE) inclus dans la cible de sécurité sont identifiés ci-dessous en bleu-vert dans le schéma ci-dessous. Les autres modules logiciels nécessaires à la mise en œuvre des services mais non inclus dans la cible d'évaluation sont colorés d'une autre couleur (bleu ciel, orange et jaune). Les fonctions de sécurité de la TOE et les exigences fonctionnelles de sécurités sont données pour le SA - Trust.Center®, le HSS, le SA - K.Registration®, le Proxy d'AE et KeySeed®.

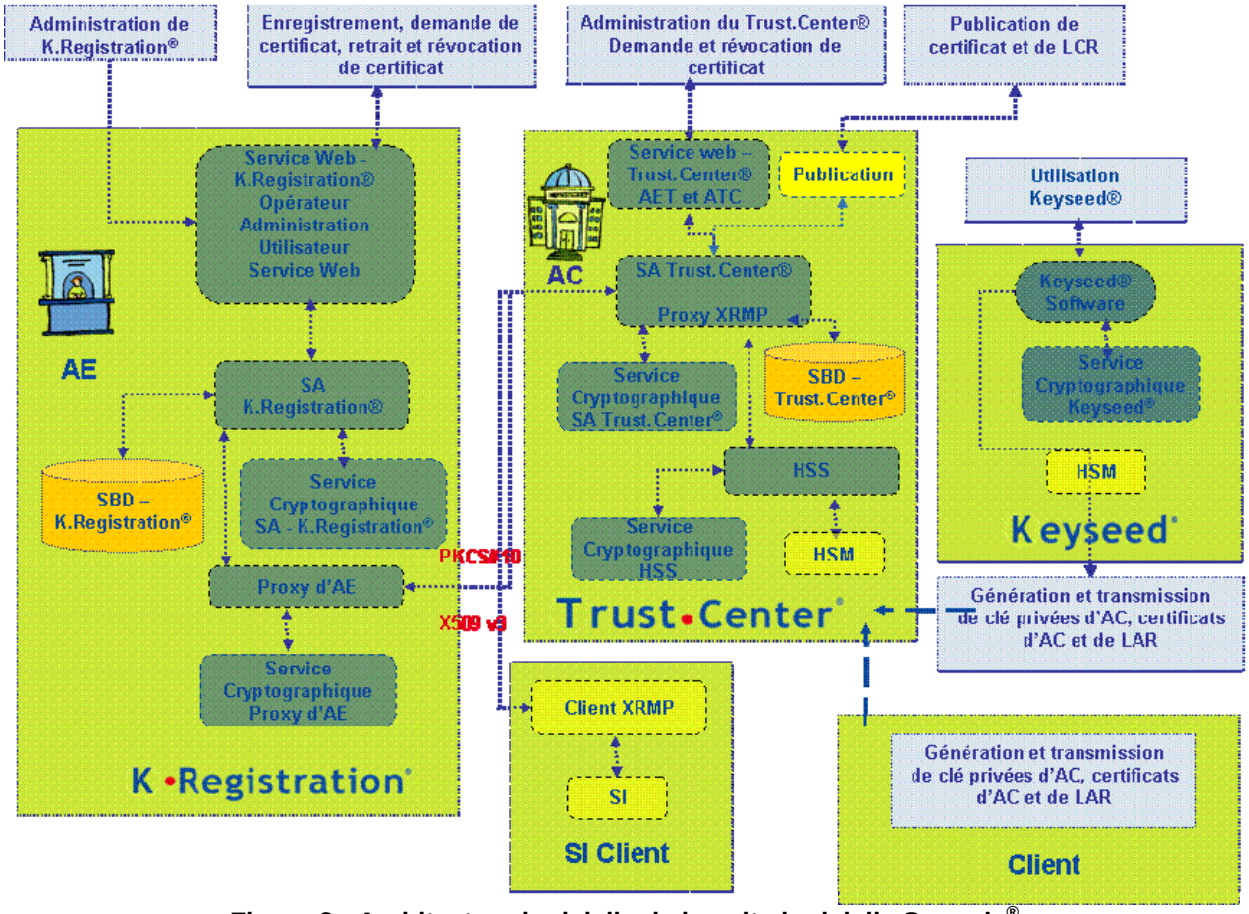


Figure 3 : Architecture logicielle de la suite logicielle Sequoia®

4.1.1 Sujets

Les sujets de la TOE sont :

- SA - Trust.Center® ;
- le HSS ;
- le SA - K.Registration® ;
- le Proxy d'AE ;
- KeySeed® ;
- Utilisateur de la TOE (Cf. § 2.2.1).

4.1.2 Objets

Les objets sont l'ensemble des biens de la TOE de type donnée (cf. § 2.1.1).

4.1.3 Opérations

Les opérations réalisées par les sujets sur les objets sont regroupées dans les catégories suivantes :

- L : cette opération correspond à la lecture d'une donnée présentée par la TOE à un utilisateur ;
- C : cette opération correspond à la création de donnée par un utilisateur ou par la TOE ;
- M : cette opération correspond à la modification d'une donnée (y compris son effacement) ;
- E : cette opération correspond à l'exportation d'une donnée d'une composante de la TOE ;
- I : cette opération correspond à l'importation d'une donnée par une composante de la TOE.

4.1.4 Attributs de sécurité

Les attributs de sécurité sont les suivants :

- Certificats : tous les utilisateurs de la TOE de types « Rôles de confiances » ont un certificat pour utiliser la TOE. Les utilisateurs de type porteurs de certificats peuvent utiliser ce type d'attribut de

sécurité pour interagir avec la TOE. Les composantes de la TOE ont ce type d'attribut de sécurité pour communiquer avec d'autres composantes de la TOE, des utilisateurs ou des machines de l'environnement IT de la TOE ;

- Données d'identification et d'authentification : ceux sont des couples « login/mot de passe ». Seuls les utilisateurs de types porteurs de certificats et des composantes logicielles de la TOE peuvent avoir ce type d'attribut de sécurité ;

- Données d'identification : ou des données d'identification seules (adresses IP par exemples). Seules des composantes logicielles de la TOE ont ce type d'attribut de sécurité pour communiquer avec des machines de l'environnement IT de la TOE.

4.1.5 Utilisateurs

Les utilisateurs sont décrits au § 2.2.1 « Utilisateurs de la TOE ».

4.1.6 Règles de contrôles d'accès

Fonctions permises par la règle de contrôles d'accès	Sujet accédants	Objets accédés	Opérations	Autorisation d'accès si :
Trust.Center®_Domaine de confiance	Administrateur ; Administrateur Root ;	BTOE 13 BTOE 29	L/M/E/I/C	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
Trust.Center®_Administration des AC	Administrateur ; Administrateur Root ;	BTOE 1 BTOE 17 BTOE 19	L/M/E/I	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
Trust.Center®_XRMP	Trust.Center®	BTOE 2	L/E/I	Possède l'attribut de sécurité nécessaire pour accéder au proxy XRMP.
Trust.Center®_XRMP	HSS	BTOE 28	M/C/E	Possède l'attribut de sécurité nécessaire pour accéder au HSS.
Trust.Center®_Rôles de confiance	Administrateur ; Administrateur Root ;	BTOE 3	L/E/I	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
Trust.Center®_Rôles de confiance	Administrateur ; Administrateur Root ;	BTOE 20	L/M/C	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
Trust.Center®_Cycle de vie des certificats et des LCR	Administrateur ; Administrateur Root ;	BTOE 2	L/I	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
Trust.Center®_Cycle de vie	Administrateur ;	BTOE 22	L/C/I/M	- Le certificat est

des certificats et des LCR	Administrateur Root ;	BTOE 23		valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
Trust.Center®_Cycle de vie des certificats et des LCR	Opérateur	BTOE 2	L/I	- Le certificat est valide ; - Le certificat est associé au droit Opérateur sur le domaine de confiance.
Trust.Center®_Cycle de vie des certificats et des LCR	Opérateur	BTOE 22 BTOE 23	L/C/I/M	- Le certificat est valide ; - Le certificat est associé au droit Opérateur sur le domaine de confiance.
Trust.Center®_Cycle de vie des certificats et des LCR	Proxy d'AE	BTOE 8	L	- Le certificat est valide ; - Le certificat est associé au droit opérateur sur le domaine de confiance.
Trust.Center®_Cycle de vie des certificats et des LCR	Système d'information Client ; SA - Trust.Center® ;	BTOE 35	L/E	Possède l'attribut de sécurité nécessaire pour accéder au SA – Trust.Center®.
Trust.Center®_Journalisation et audit	Administrateur ; Administrateur Root ;	BTOE 2 BTOE 10	L	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
Trust.Center®_Journalisation et audit	Auditeur ;	BTOE 2 BTOE 10	L	- Le certificat est valide ; - Le certificat est associé au droit auditeur sur le domaine de confiance.
Trust.Center®_Gestion site web	Administrateur ; Administrateur Root ;	BTOE 9 BTOE 37	L	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
Trust.Center®_Gestion site web	Auditeur ;	BTOE 9 BTOE 36 BTOE 37	L	- Le certificat est valide ; - Le certificat est associé au droit auditeur sur le domaine de confiance.
Trust.Center®_Gestion site web	Opérateur ;	BTOE 9 BTOE 36	L	- Le certificat est valide ; - Le certificat est associé au droit oprateur sur le

				domaine de confiance.
HSS_Profil de donnée à signer	Administrateur système de l'environnement de la TOE	BTOE 1	C	Autorisé par le Responsable de sécurité. Possède l'attribut de sécurité nécessaire pour accéder au HSS.
HSS_Traitement des requêtes de signature	HSS	BTOE 1 BTOE 2 BTOE 35	L/M/E/I	Possède l'attribut de sécurité nécessaire pour accéder au HSM.
HSS_Traitement des requêtes de signature	Administrateur système	BTOE 33	L/E/I/M/C	Autorisé par le Responsable de sécurité. Possède l'attribut de sécurité nécessaire pour accéder la machine hôte du HSS.
HSS_Traitement des requêtes de signature	HSS	BTOE 33	L	Sans objet.
HSS_Journalisation et audit	Administrateur système de l'environnement de la TOE	BTOE 11	L	Autorisé par le Responsable de sécurité. Possède l'attribut de sécurité nécessaire pour accéder au HSS.
K.Registration®_Domaine de confiance	Administrateur ; Administrateur Root ;	BTOE 14 BTOE 30	L/M/E/I/C	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
K.Registration®_Offre de certification	Administrateur ; Administrateur Root ;	BTOE 15 BTOE 18	L/E/I	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
K.Registration®_Rôle de confiance	Administrateur ; Administrateur Root ;	BTOE 4	L/I/E	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
K.Registration®_Rôle de confiance	Administrateur ; Administrateur Root ;	BTOE 21	L/C/M	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
K.Registration®_Mise en œuvre d'une offre de certification	Administrateur ; Administrateur Root ;	BTOE 4	L/I/C	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
K.Registration®_Mise en œuvre d'une offre de	Administrateur ; Administrateur	BTOE 24	L/M/E/I/C	- Le certificat est valide ;

certification	Root ;			- Le certificat est associé au droit administrateur sur le domaine de confiance.
K.Registration®_Mise en œuvre d'une offre de certification	Opérateur ;	BTOE 2 BTOE 24 BTOE 26	L/M/E/I/C (au choix en fonction du profil opérateur attribué à l'utilisateur)	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
K.Registration®_Mise en œuvre d'une offre de certification	Proxy d'AE ;	BTOE 24	L/I	Dans le cadre de la mise en œuvre du protocole XRMP.
K.Registration®_Mise en œuvre d'une offre de certification	Utilisateur ;	BTOE 2 BTOE 24 BTOE 26	L/E/I/C/M	- Le certificat est valide ; - Le certificat est associé au droit utilisateur sur le domaine de confiance. - Possède l'attribut de sécurité nécessaire pour accéder au SA – K.Registration®.
K.Registration®_Mise en œuvre d'une offre de certification	Utilisateur ;	BTOE 32	L/E	- Possède l'attribut de sécurité nécessaire pour accéder au SA – K.Registration®.
K.Registration®_Mise en œuvre d'une offre de certification	Proxy d'AE	BTOE 5 BTOE 24 BTOE 26	L/I	Dans le cadre de la mise en œuvre du protocole XRMP.
K.Registration®_Journalisation et audit	Administrateur ; Administrateur Root ;	BTOE 12	L	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
K.Registration®_Journalisation et audit	Auditeur ;	BTOE 12	L	- Le certificat est valide ; - Le certificat est associé au droit auditeur sur le domaine de confiance.
K.Registration®_Gestion site web	Administrateur ; Administrateur Root ;	BTOE 7 BTOE 38	L	- Le certificat est valide ; - Le certificat est associé au droit administrateur sur le domaine de confiance.
K.Registration®_Gestion site web	Auditeur ;	BTOE 7 BTOE 38	L	- Le certificat est valide ; - Le certificat est associé au droit auditeur sur le domaine de confiance.
K.Registration®_Gestion site web	Opérateur	BTOE 7 BTOE 39	L	- Le certificat est valide ;

				- Le certificat est associé au droit Opérateur sur le domaine de confiance.
K.Registration®_Gestion site web	Utilisateur	BTOE 7 BTOE 40	L	- Le certificat est valide ; - Le certificat est associé au droit utilisateur sur le domaine de confiance.
K.Registration®_Gestion site web	Système d'information Client	BTOE 7 BTOE 41	L	- Le certificat est valide ; - Le certificat est associé au droit utilisateur sur le domaine de confiance.
Proxy d'AE	Proxy d'AE	BTOE 25 BTOE 27	L/E/I/M/C	Sans objet.
Proxy d'AE	Administrateur système	BTOE 33	L/E/I/M/C	Autorisé par le Responsable de sécurité. Possède l'attribut de sécurité nécessaire pour accéder la machine hôte du proxy d'AE.
Proxy d'AE	Proxy d'AE	BTOE 33	L	Sans objet.
Proxy d'AE	SA - K.Registration® SA – Trust.Center®	BTOE 6	L/I	Possède l'attribut de sécurité nécessaire pour accéder au Proxy d'AE.
Proxy d'AE	SA – Trust.Center®	BTOE 25 BTOE 27	L/I	Possède l'attribut de sécurité nécessaire pour accéder au Proxy d'AE.
Keyseed®_Mise en œuvre de script	Opérateur	BTOE 16	L/E/I/M	Autorisé par le Responsable de sécurité. Possède l'attribut de sécurité nécessaire pour accéder la machine hôte de Keyseed®.
Keyseed®_Mise en œuvre de script	Administrateur système	BTOE 31	L/E/I/M/C	Autorisé par le Responsable de sécurité. Possède l'attribut de sécurité nécessaire pour accéder la machine hôte de Keyseed®.

4.2 Exigences fonctionnelles de sécurité

Les exigences fonctionnelles de sécurité retenues pour l'IGC sont présentées aux paragraphes ci-dessous. L'instanciation des exigences décrite dans ce chapitre se fera par la description des fonctions de sécurité au regard des exigences fonctionnelles de sécurité comme décrite au § 6.5.1.

Toutes les exigences fonctionnelles de sécurité pour la TOE sont extraites de la partie 2 des Critères Communs dans leur version 3.1.

Les exigences fonctionnelles de sécurité sont données pour toutes les configurations possibles de la TOE.

4.2.1 Class FAU: Security audit

4.2.1.1 FAU_GEN.1 Audit data generation

Refinement: Cette exigence de sécurité fonctionnelle s'applique SA - K.Registration® et au SA - Trust.Center®.

4.2.1.1.1 FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [detailed] level of audit; and
c) [BTOE 10, BTOE 11 et BTOE 12].

4.2.1.1.2 FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [le type d'action réalisée (Créer/Activer/Désactiver/Détruire/Lire), l'identité du rôle qui initie l'action, l'identifiant du domaine de confiance utilisé, l'identification de la donnée sur laquelle porte l'action et parfois le contenu exacte de la donnée. De plus, les traces d'audits ne doivent pas inclure des traces d'éléments sensibles (clés privées, …)].

4.2.1.2 FAU_GEN.2 User identity association

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.1.2.1 FAU_GEN.2.1 User identify association

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

4.2.1.3 FAU_SAR.1 Audit review

Refinement: Cette exigence de sécurité fonctionnelle s'applique SA - K.Registration® et au SA - Trust.Center®.

4.2.1.3.1 FAU_SAR.1.1

The TSF shall provide [utilisateurs avec droits d'audit et d'administration] with the capability to read [BTOE 10, BTOE 11 et BTOE 12] from the audit records.

4.2.1.3.2 FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

4.2.1.4 FAU_SAR.2 Restricted audit review

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.1.4.1 FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

4.2.1.5 FAU_SAR.3 Selectable audit review

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.1.5.1 FAU_SAR.3.1

The TSF shall provide the ability to apply [sélection sur un domaine de confiance] of audit data based on [utilisateurs avec un certificat qui possède des droits d'audit sur un domaine de confiance].

4.2.1.6 FAU_SEL.1 Selective audit

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.1.6.1 FAU_SEL.1.1

The TSF shall be able to select the set of audited events from the set of all auditable events based on the following attributes:

a) [identité de l'utilisateur, certificat de l'utilisateur, domaine de confiance sur lequel le certificat de l'utilisateur est déclaré]

b) [aucun]

4.2.1.7 FAU_STG.1 Protected audit trail storage

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration®, au SA - Trust.Center® et au HSS.

4.2.1.7.1 FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

4.2.1.7.2 FAU_STG.1.2

The TSF shall be able to [empêcher] unauthorised modifications to the stored audit records in the audit trail.

The TSF shall be able to [détecter] unauthorised modifications to the stored audit records in the audit trail.

4.2.2 Class FCO: Communication

4.2.2.1 FCO_NRO.2 Enforced proof of origin

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration®,et au SA - Trust.Center®.

4.2.2.1.1 FCO_NRO.2.1

The TSF shall enforce the generation of evidence of origin for transmitted [données signée par un utilisateur qui possède un certificat avec des droits de type "opérateur" et l'ensemble des données générées ou

modifiées par un utilisateur ; BTOE 22, BTOE 23, BTOE 24, BTOE 25, BTOE 26, BTOE 27 et BTOE 30] at all times.

4.2.2.1.2 FCO_NRO.2.2

The TSF shall be able to relate the [identité de l'utilisateur, date et l'heure] of the originator of the information, and the [donnée, signature de la donnée] of the information to which the evidence applies.

4.2.2.1.3 FCO_NRO.2.3

The TSF shall provide a capability to verify the evidence of origin of information to [personnes identifiée par le responsable de sécurité] given [les limitations sur la preuve d'origine sont déterminées par le niveau de sécurité requis pour l'attribution des certificats aux utilisateurs et leur modes d'utilisation].

4.2.2.2 FCO_NRR.2 Enforced proof of receipt

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration®.

4.2.2.2.1 FCO_NRR.2.1

The TSF shall enforce the generation of evidence of receipt for received [envoi de courier électronique par le module SA - K.Registration® dès qu'une operation est réalisée sur la TOE conformément à la configuration de l'offre de certification] at all times.

4.2.2.2.2 FCO_NRR.2.2

The TSF shall be able to relate the [adresse de courier électronique et identité (déclarées en base de données du SA - K.Registration®) des destinataires des notifications] of the recipient of the information, and the [les couriers électroniques types definis dans l'offre de certification et les opérations de la TOE soumises à notification] of the information to which the evidence applies.

4.2.2.2.3 FCO_NRR.2.3

The TSF shall provide a capability to verify the evidence of receipt of information to [originator, recipient] given [la liste des certificats à utiliser et l'accès à la LCR pour vérifier la signature du courrier électronique].

4.2.3 Class FCS: Cryptographic support

4.2.3.1 FCS_COP.1 Cryptographic operation

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration®, Proxy d'AE, SA - Trust.Center®, HSS (hash seulement) et KeySeed® (hash seulement).

4.2.3.1.1 FCS_COP.1.1

The TSF shall perform [chiffrement, déchiffrement, signature, verification de signature et hash] in accordance with a specified cryptographic algorithm [RSA, SHA1, SHA256,] and cryptographic key sizes [2048 (RSA), 4096 (RSA), (SHA1), 256(SHA2)] that meet the following: [[RSA], [SHA1], [SHA256],].

4.2.4 Class FDP: User data protection

4.2.4.1 FDP_ACC.2 Complete access control

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.4.1.1 FDP_ACC.2.1

The TSF shall enforce the [contrôle d'accès par certificat et code de retrait] on [utilisateur avec rôle de confiance et utilisateur de type porteur de certificat pour la mise en œuvre des fonctions autorisées] and all operations among subjects and objects covered by the SFP.

4.2.4.1.2 FDP_ACC.2.2

The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

4.2.4.2 FDP_ACF.1 Security attribute based access control

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.4.2.1 FDP_ACF.1.1

The TSF shall enforce the [contrôle d'accès par certificat associé à un rôle de confiance sur un domaine de confiance et code de retrait] to objects based on the following: [avec certificat pour toutes les actions effectuées par un utilisateurs avec un rôle de confiance et par certificat ou code de retrait pour toutes les actions effectuées par un utilisateur de type porteur de certificat].

4.2.4.2.2 FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [fournir l'accès aux fonctions et aux données conformément aux règles de contrôles d'accès définies par la configuration initiale des composants].

4.2.4.2.3 FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [fournir l'accès aux fonctions et aux données conformément aux règles de contrôles d'accès définies par les utilisateurs de types « Administrateur » et « Administrateur root » sur les composants].

4.2.4.2.4 FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [certificat qui n'a pas de droits ou qui est révoqué].

4.2.4.3 FDP_DAU.2 Data Authentication with Identity of Guarantor

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.4.3.1 FDP_DAU.2.1

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [BTOE 22, BTOE 23, BTOE 24, BTOE 25, BTOE 26, BTOE 27 et BTOE 28].

4.2.4.3.2 FDP_DAU.2.2

The TSF shall provide [personne autorisée par le responsable de sécurité] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

4.2.4.4 FDP_ETC.1 Export of user data without security attributes

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration®, au SA - Trust.Center® et à Keyseed®.

4.2.4.4.1 FDP_ETC.1.1

The TSF shall enforce the [contrôle d'accès par certificat pour les utilisateurs avec un rôle de confiance prévu à cet effet] when exporting user data, controlled under the SFP(s), outside of the TOE.

The TSF shall enforce the [mise en œuvre du script de cérémonie des clés (BTOE 17)] when exporting user data, controlled under the SFP(s), outside of the TOE.

4.2.4.4.2 FDP_ETC.1.2

The TSF shall export the user data without the user data's associated security attributes

4.2.4.5 FDP_IFC.2 Complete information flow control

Refinement: Cette exigence de sécurité fonctionnelle concerne le HSS et le proxy d'AE.

4.2.4.5.1 FDP_IFC.2.1

The TSF shall enforce the [routage proxy d'AE et routage HSS] on [demande de certificat et demande de revocation pour le proxy d'AE et certificat et LCR pour le HSS] and all operations that cause that information to flow to and from subjects covered by the SFP.

4.2.4.5.2 FDP_IFC.2.2

The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

4.2.4.6 FDP_IFF.1 Simple security attributes

Refinement: Cette exigence de sécurité fonctionnelle concerne le Keyseed®, Trust.Center(r) et le K.Registration®.

4.2.4.6.1 FDP_IFF.1.1

The TSF shall enforce the [routage proxy d'AE, Keyseed® et HSS] based on the following types of subject and information security attributes: [identifiant d'AC contenue dans la demande du SA K.Registration® pour le proxy d'AE et identifiant de l'AC continue dans la demande de signature du SA Trust.Center® pour le HSS et le requête XML de KeySeed®].

4.2.4.6.2 FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [le proxy d'AE signe des requêtes (Cf. BTOE 26 et BTOE 26) pour le SA Trust.Center® avec la clé privée correspondante au certificat déclaré sur le SA -Trust.Center® avec un rôle « opérateur » au profit d'un domaine de confiance sur l'AE, le HSS déclenche la signature d'un certificat ou d'une LCR avec la clé privée de l'AC identifiée dans la requête de signature transmise par le SA Trust.Center®].

4.2.4.6.3 FDP_IFF.1.3

The TSF shall enforce the [aucun].

4.2.4.6.4 FDP_IFF.1.4

The TSF shall explicitly authorise an information flow based on the following rules: [aucun].

4.2.4.6.5 FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [aucun].

4.2.4.7 FDP_ITC.1 Import of user data without security attributes

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA – Trust.Center®.

4.2.4.7.1 FDP_ITC.1.1

The TSF shall enforce the [control d'accès par certificat] when importing user data, controlled under the SFP, from outside of the TOE.

4.2.4.7.2 FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

4.2.4.7.3 FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [aucun].

4.2.4.8 FDP_ITC.2 Import of user data with security attributes

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.4.8.1 FDP_ITC.2.1

The TSF shall enforce the [control d'accès par certificat suivant les configurations des composantes] when importing user data, controlled under the SFP, from outside of the TOE.

4.2.4.8.2 FDP_ITC.2.2

The TSF shall use the security attributes associated with the imported user data.

4.2.4.8.3 FDP_ITC.2.3

The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

4.2.4.8.4 FDP_ITC.2.4

The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

4.2.4.8.5 FDP_ITC.2.5

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [aucun].

4.2.4.9 FDP_ITT.1.1 Basic internal transfer protection

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center® mais lorsque la TOE est sur la même machine.

4.2.4.9.1 FDP_ITT.1.1

The TSF shall enforce the [contrôle d'accès par certificat et signature des données échangées entre le SA - K.Registration® et proxy d'AE et entre le proxy d'AE et SA - Trust.Center® (proxy XRMP)] to prevent the [disclosure, modification, loss of use] of user data when it is transmitted between physically-separated parts of the TOE.

4.2.4.10 FDP_UCT.1 Basic data exchange confidentiality

Refinement: Cette exigence de sécurité fonctionnelle s'applique au K.Registration® et au SA - Trust.Center®.

4.2.4.10.1 FDP_UCT.1.1

The TSF shall enforce the [chiffrement des données entre le proxy d'AE et SA - Trust.Center® (proxy XRMP)] to be able to [transmettre, recevoir] user data in a manner protected from unauthorised disclosure.

4.2.4.11 FDP_UIT.1 Data exchange integrity

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.4.11.1 FDP_UIT.1.1

The TSF shall enforce the [verification de la signature par les SA-K.Registration®, le porxy d'AE et SA - Trust.Center® (proxy XRMP)] to be able to [transmettre, recevoir] user data in a manner protected from [modification, re-jeu] errors.

4.2.4.11.2 FDP_UIT.1.2

The TSF shall be able to determine on receipt of user data, whether [modification, re-jeu] has occurred.

4.2.5 Class FIA: Identification and authentication

4.2.5.1 FIA_AFL.1 Authentication failure handling

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration®.

4.2.5.1.1 FIA_AFL.1.1

The TSF shall detect when [nombre de tentative de saisie de code de retrait supérieure à un nombre configuré sur le SA - K.Registration®], an administrator configurable positive integer within [code de retrait] unsuccessful authentication attempts occur related to [retrait de certificat].

4.2.5.1.2 FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [selection: *met*], the TSF shall [bloquer le retrait du certificat].

Le certificat ne peut plus être retiré.

4.2.5.2 FIA_ATD.1 User attribute definition

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.5.2.1 FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [certificat lié à un rôle de confiance sur le SA - K.Registration® et le SA - Trust.Center®, domaine de confiance sur lequel l'utilisateur est déclaré et la liste des actions possibles par type de rôle (uniquement pour le SA - K.Registration®)].

4.2.5.3 FIA_SOS.2 TSF Generation of secrets

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration®.

4.2.5.3.1 FIA_SOS.2.1

The TSF shall provide a mechanism to generate secrets that meet [longueur minimale et caractères aléatoires].

4.2.5.3.2 FIA_SOS.2.2

The TSF shall be able to enforce the use of TSF generated secrets for [retrait de certificat].

4.2.5.4 FIA_UAU.1 Timing of authentication

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration®.

4.2.5.4.1 FIA_UAU.1.1

The TSF shall allow [déposer une demande de certificat] on behalf of the user to be performed before the user is authenticated.

4.2.5.4.2 FIA_UAU.1.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

4.2.5.5 FIA_UAU.2 User authentication before any action

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.5.5.1 FIA_UAU.2.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

4.2.5.6 FIA_UID.2 User identification before any action

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration®, proxy d'AE, et au SA - Trust.Center®.

4.2.5.6.1 FIA_UID.2.1

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

4.2.5.7 FIA_USB.1 User-subject binding

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.5.7.1 FIA_USB.1.1

The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [certificat].

4.2.5.7.2 FIA_USB.1.2

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [vérifier que l'affectation d'un certificat à un rôle est effectué par un rôle autorisé].

4.2.5.7.3 FIA_USB.1.3

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [tracer l'affectation de roles à des certificats].

4.2.6 Class FMT: Security management

4.2.6.1 FMT_MOF.1 Management of security functions behaviour

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.6.1.1 FMT_MOF.1.1

The TSF shall restrict the ability to [activer, désactiver et utiliser] the functions [Trust.Center®_Domaine de confiance, Trust.Center®_Admisnistration des AC, Trust.Center®_Rôles de confiance, Trust.Center®_Cycle de vie des certificats et des LCR (utilisation par IHM seulement), Trust.Center®_Journalisation et audit (consultation seulement), K.Registration®_Domaine de confiance, K.Registration®_Offre de certification, K.Registration®_Rôle de confiance, K.Registration®_Mise en œuvre d'une offre de certification (utilisation par IHM seulement), K.Registration®_Journalisation et audit (consultation seulement) et KeySeed®_Mise en œuvre de script] to [assignment: par des rôles autorisés de type « Administrateur » et « Administrateur root »].

4.2.6.2 FMT_MSA.1 Management of security attributes

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.6.2.1 FMT_MSA.1.1

The TSF shall enforce the [contrôle d'accès par certificat associé à un rôle de confiance de type « Administrateur » ou « Admisnitrateur root »] to restrict the ability to [définir, affecter, retirer, supprimer] the security attributes [les rôles de confiance et les profils associés] to [les rôles de confiance sur les composants de la TOE ayant un profil type « Administrateur » ou « Administrateur root »].

4.2.6.3 FMT_MSA.2 Secure security attributes

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.6.3.1 FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for [certificat].

4.2.6.4 FMT_MSA.3 Static attribute initialisation

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.6.4.1 FMT_MSA.3.1

The TSF shall enforce the [aucun] to provide [aucun] default values for security attributes that are used to enforce the SFP.

Il n'y a pas de valeur par défaut à initialiser sur les composants de la TOE. Les premiers certificats des utilisateurs ayant des rôles de confiance sont introduits dans la base de données de chaque composant de la TOE sur lesquels il possède un rôle de confiance. Il n'y a pas de valeur par défaut à changer.

Les certificats pour les autres rôles de confiance sont introduits et paramétrés dans le composant ou le rôle doit être actif. Cette opération ne peut être effectuée que par des utilisateurs de la TOE ayant un rôle de confiance de type « Administrateur » sur le composant de la TOE sur lequel le certificat de l'utilisateur doit être déclaré.

4.2.6.4.2 FMT_MSA.3.2

The TSF shall allow the [les roles autorisés et identifiés] to specify alternative initial values to override the default values when an object or information is created.

Les utilisateurs ayant un rôle de confiance sont authentifiés à l'aide de leur certificat.

4.2.6.5 FMT_MTD.1 Management of TSF data

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.6.5.1 FMT_MTD.1.1

The TSF shall restrict the ability to [Lecture, Ecriture, Modification, Copier, Importer] the [tous les biens de BTOE1 à BTOE 42] to [par les utilisateurs qui possède un rôle de confiance prévu à cet effet sur le composant et sur la donnée comme décrit dans le tableau « des règles de contrôle d'accès].

4.2.6.6 FMT_MTD.3 Secure TSF data

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.6.6.1 FMT_MTD.3.1

The TSF shall ensure that only secure values are accepted for [BTOE 15, BTOE 16, BTOE 17, BTOE 18, BTOE 19, BTOE 22, BTOE 23, BTOE 24, BTOE 25, BTOE 26, BTOE 27, BTOE 28 et BTOE 32].

4.2.6.7 FMT_REV.1 Revocation

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.6.7.1 FMT_REV.1.1

The TSF shall restrict the ability to revoke [certificat] associated with the [porteur et roles autorisés] under the control of the TSF to [seulements les porteurs et les roles autorisés en function de la configuration].

Les utilisateurs ayant un rôle de confiance de type « administrateur » sur un composant de la TOE peuvent révoqués les certificats des utilisateurs ayant un rôle de confiance. La révocation du certificat empêche l'utilisateur de pouvoir utiliser la TOE. De même, les rôles de confiance de type « Administrateur » et « Administrateur Root » peuvent aussi être révoqué par les rôles de confiance de type « Administrateur Root ».

4.2.6.7.2 FMT_REV.1.2

The TSF shall enforce the rules [contrôle de l'état des certificats des roles de confiances qui s'authentifient sur le SA - K.Registration® et SA - Trust.Center®].

4.2.6.8 FMT_SMF.1 Specification of Management Functions

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration®, au SA - Trust.Center® et KeySeed®.

4.2.6.8.1 FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [Trust.Center®_Domaine de confiance, Trust.Center®_Admisnistration des AC, Trust.Center®_XRMP, Trust.Center®_Rôles de confiance, Trust.Center®_Cycle de vie des certificats et des LCR, Trust.Center®_Journalisation et audit, Trust.Center®_Gestion site web, HSS_Profil de donnée à signer, HSS_Traitement des requêtes de signature, HSS_Journalisation et audit, K.Registration®_Domaine de confiance, K.Registration®_Proxy d'AE, K.Registration®_Offre de certification, K.Registration®_Rôle de confiance, K.Registration®_Mise en œuvre d'une offre de certification, K.Registration®_Journalisation et audit, K.Registration®_Gestion site web, KeySeed®_Mise en œuvre de script].

4.2.6.9 FMT_SMR.2 Restrictions on security roles

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.6.9.1 FMT_SMR.2.1

The TSF shall maintain the roles: [roles autorisés].

Les composants de la TOE distinguent 4 types de rôles :

- « Administrateur root » : insérer dans le système à l'initialisation du composant ;
- « Administrateur » : administre le composant de la TOE en fonction de ses droits ;
- « Opérateur » : met en œuvre des fonctions de la TOE en fonction de ses droits ;
- « Auditeur » : consulte les fichiers d'audit du composant de la TOE.

4.2.6.9.2 FMT_SMR.2.2

The TSF shall be able to associate users with roles.

4.2.6.9.3 FMT_SMR.2.3

The TSF shall ensure that the conditions [un « Auditeur » ne peut être qu' « Auditeur » sur un domaine de confiance, un « Opérateur » ne peut être qu' « Opérateur » sur un domaine de confiance et un « Administrateur » et un « Administrateur root » ne peuvent être qu' « Administrateur » et qu'« Administrateur root » sur un domaine de confiance] are satisfied.

4.2.7 Class FPT: Protection of the TSF

4.2.7.1 FPT_ITT.1 Basic internal TSF data transfer protection

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® (proxy d'AE) et au SA - Trust.Center®.

4.2.7.1.1 FPT_ITT.1.1

The TSF shall protect TSF data from [modification] when it is transmitted between separate parts of the TOE.

4.2.7.2 FPT_RPL.1 Replay detection

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.7.2.1 FPT_RPL.1.1

The TSF shall detect replay for the following entities: [demande de certificat identique pour un même utilisateur].

4.2.7.2.2 FPT_RPL.1.2

The TSF shall perform [rejeter la demande de certificat] when replay is detected.

Les demandes de certificats sont rejetées.

4.2.8 FPT_STM Time stamps

4.2.8.1 FPT_STM.1 Reliable time stamps

Refinement: Cette exigence de sécurité fonctionnelle s'applique aux SA - K.Registration®, HSS et au SA - Trust.Center®.

4.2.8.1.1 FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

4.2.9 FPT_TDC Inter-TSF TSF data consistency

4.2.9.1 FPT_TDC.1 Inter-TSF basic TSF data consistency

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration®, au SA - Trust.Center®. et KeySeed®, HSS, proxy d'AE, et Trust.Center®.

4.2.9.1.1 FPT_TDC.1.1

The TSF shall provide the capability to consistently interpret [BTOE 16, BTOE 18, BTOE 19 et BTOE 20] when shared between the TSF and another trusted IT product.

4.2.9.1.2 FPT_TDC.1.2

The TSF shall use [si le format de demande de certificat transmis par le SA - K Registration® (proxy d'AE) n'est pas correcte alors le HSS rejette la demande, si les demandes transmises par le SA - K Registration® (proxy d'AE) ne sont pas correctes, alors le SA - Trust.Center® rejette la demande et le composant KeySeed® contrôle le format de la donnée à signer et émet une donnée à signer conforme à un contenu pré-défini] when interpreting the TSF data from another trusted IT product.

4.2.10 Class FTA: TOE access

4.2.11 FTA_LSA Limitation on scope of selectable attributes

4.2.11.1 FTA_LSA.1 Limitation on scope of selectable attributes

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.11.1.1 FTA_LSA.1.1

The TSF shall restrict the scope of the session security attributes [certificat rôle de confiance qui permet d'avoir accès à des IHM dédiées en fonction de la configuration de la composante et des droits associés au certificat (BTOE 36, BTOE 37, BTOE 38, BTOE 39, BTOE 40 et BTOE 41)], based on [URL du site utilisé sur les composants et certificat associé à un rôle de confiance et des droits sur un domaine de confiance de la composants].

4.2.12 FTA_SSL Session locking and termination

4.2.12.1 FTA_SSL.1 TSF-initiated session locking

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® (pour BTOE 38, BTOE 39, BTOE 40 et BTOE 41) et au SA - Trust.Center® (pour BTOE 36 et BTOE 38).

4.2.12.1.1 FTA_SSL.1.1

The TSF shall lock an interactive session after [30 minutes] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

4.2.12.1.2 FTA_SSL.1.2

The TSF shall require the following events to occur prior to unlocking the session: [action de la part de l'utilisateur pour fermer la session ou un temps de non utilisation pendant 30 minutes].

4.2.12.2 FTA_SSL.2 User-initiated locking

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® (pour BTOE 38, BTOE 39, BTOE 40 et BTOE 41) et au SA - Trust.Center® (pour BTOE 36 et BTOE 37).

4.2.12.2.1 FTA_SSL.2.1

The TSF shall allow user-initiated locking of the user's own interactive session, by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

4.2.12.2.2 FTA_SSL.2.2

The TSF shall require the following events to occur prior to unlocking the session: [nouvelle authentification réussie].

4.2.12.3 FTA_SSL.3 TSF-initiated termination

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® (pour BTOE 38, BTOE 39, BTOE 40 et BTOE 41) et au SA - Trust.Center® (pour BTOE 36 et BTOE 37).

4.2.12.3.1 FTA_SSL.3.1

The TSF shall terminate an interactive session after a [temps de 30 minutes pendant laquelle la session n'est plus utilisée par l'utilisateur].

4.2.12.4 FTA_SSL.4 User-initiated termination

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® (pour BTOE 38, BTOE 39, BTOE 40 et BTOE 41) et au SA - Trust.Center® (pour BTOE 36 et BTOE 37).

4.2.12.4.1 FTA_SSL.4.1

The TSF shall allow user-initiated termination of the user's own interactive session.

4.2.13 FTA_TSE TOE session establishment

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.13.1 FTA_TSE.1 TOE session establishment

The TSF shall be able to deny session establishment based on [URL du site utilisé sur les composants (BTOE 36, BTOE 37, BTOE 38, BTOE 39, BTOE 40 et BTOE 41) et statut du certificat associé au rôle de confiance dans un domaine de confiance].

4.2.14 Class FTP: Trusted path/channels

4.2.14.1 FTP_ITC.1 Inter-TSF trusted channel

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.14.1.1 FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

4.2.14.1.2 FTP_ITC.1.2

The TSF shall permit [accès distant sécurisé] to initiate communication via the trusted channel.

SA - K.Registration® et au SA - Trust.Center® mettent en œuvre un chemin de confiance avec des utilisateurs de type rôles de confiance qui utilise un poste informatique ou serveur.

4.2.14.1.3 FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [Trust.Center®_XRMP et K.Registration®_Mise en œuvre d'une offre de certification (uniquement demande de certificat et de révocation et renvoi d'information sur les demandes de certificat en cours)].

4.2.15 FTP_TRP Trusted path

4.2.15.1 FTP_TRP.1 Trusted path

Refinement: Cette exigence de sécurité fonctionnelle s'applique au SA - K.Registration® et au SA - Trust.Center®.

4.2.15.1.1 FTP_TRP.1.1

The TSF shall provide a communication path between itself and [distant et local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification et divulgation].

Le SA - Trust.Center® réalise un chemin de confiance avec les utilisateurs (personne) qui ont un rôle de confiance sur le SA - Trust.Center®. Les utilisateurs peuvent utiliser une signature électronique sur les données qu'ils transmettent à partir des interfaces fournit lors des connexions SSL avec le composant.

Le SA - K.Registration® réalise un chemin de confiance avec les utilisateurs (personne) qui ont un rôle de confiance sur le SA - K.Registration®. Les utilisateurs (personne) peuvent utiliser une signature électronique sur les données qu'ils transmettent à partir des interfaces fournit lors des connexions SSL avec le composant.

4.2.15.1.2 FTP_TRP.1.2

The TSF shall permit [distant et local] to initiate communication via the trusted path.

Le SA - Trust.Center® réalise un chemin de confiance avec les utilisateurs qui ont un rôle de confiance sur le SA - Trust.Center®. Les utilisateurs peuvent utiliser une signature électronique sur les données qu'ils transmettent à partir des interfaces fournit lors des connexions avec le composant.

Le SA - K.Registration® réalise un chemin de confiance avec les utilisateurs qui ont un rôle de confiance sur le SA -K.Registration®. Les utilisateurs (personne) peuvent utiliser une signature électronique sur les données qu'ils transmettent à partir des interfaces fournit lors des connexions SSL avec le composant.

4.2.15.1.3 FTP_TRP.1.3

The TSF shall require the use of the trusted path for [Trust.Center®_Domaine de confiance, Trust.Center®_Admisnistration des AC, Trust.Center®_Rôles de confiance, Trust.Center®_Cycle de vie des certificats et des LCR, Trust.Center®_Journalisation et audit, K.Registration®_Mise en œuvre d'une offre de certification, K.Registration®_Domaine de confiance, K.Registration®_Offre de certification, K.Registration®_Rôle de confiance et K.Registration®_Journalisation et audit].
Les fonctions impactées dépendent de la configuration de K.Registration® et du Trust.Center® (hors HSS) qui requière ou non la mise en œuvre de la signature électronique.

4.3 Exigences d'assurance

La cible de sécurité est réalisée par référence au niveau EAL4 augmenté du composant ALC_FLR.3 comme définit dans la version 3.1 des [CC] partie 3. Le choix des packages d'assurances est effectué à partir du

référentiel de qualification standard [QS] définit par l'ANSSI et de certain package d'assurance issu du profil de protection [PP_CIMC].

Classe d'assurance	Famille d'assurance	
Développement	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.3	Systematic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample

Classe d'assurance	Famille d'assurance	
Estimation des vulnérabilités	AVA_VAN.3	Focused vulnerability analysis

Toutes les exigences d'assurance pour la TOE sont extraites de la partie 3 des Critères communs **[CC]**.

Ce niveau d'assurance couvre les exigences du niveau de sécurité 3 défini dans le profil de protection : « Certificate Issuing and Management Components Family of Protection Profiles Version 1.0 » (Cf. § « 8.1.3 Security Level 3 Security Assurance »). Ce document est cité par la politique de certification de l'OTAN [OTAN] afin de déterminer le périmètre et le niveau d'évaluation d'une cible de sécurité d'une solution IGC.

De plus, il correspond au niveau de risque qui s'applique aux applications qui utilisent les services de la suite logicielle Sequoia®.

5 FONCTION DE SECURITE

Les fonctions de sécurité de la TOE sont données sans détailler toutes les fonctions techniques de la cible de sécurité. La correspondance entre les fonctions techniques détaillées de la cible de sécurité et les fonctions macroscopiques ci-dessous est donnée dans des documents annexes, dédiés à chaque composante de la TOE, qui servent à l'évaluation de la TOE. Le regroupement des fonctions est effectué par groupes : administration, gestion des rôles de confiance, journalisation et audit, configuration, mise en œuvre et communication avec les composantes de la TOE.

5.1.1 Trust.Center®

5.1.1.1 SA – Trust.Center®

5.1.1.1.1 Trust.Center® _ Domaine de confiance

Cette fonction permet :

- De créer un domaine de confiance pour cloisonner les données d'un client à l'autre ;
- D'activer un domaine de confiance ;
- De désactiver un domaine de confiance ;
- De gérer l'unicité des identités introduites dans les certificats.

5.1.1.1.2 Trust.Center® _ Administration des AC

Cette fonction permet :

- D'insérer un certificat d'AC dans un domaine de confiance ;
- De retirer un certificat d'AC pour que Trust.Center® n'utilise plus le certificat en question pour les signatures (certificats et LCR) ;
- De recherche d'un certificat d'AC dans des domaines de confiance ;
- De consulter un certificat d'AC d'un domaine de confiance ;
- De publier un certificat d'AC ou la Chaîne de confiance, sur les sites public et d'administration ;
- D'activer et de désactiver un certificat d'AC pour que Trust.Center® puisse ou non utiliser le certificat en question pour les signatures des éléments de confiance ;
- D'ajouter un profil dans un domaine de confiance pour une AC donnée. Le profil décrit le format (et ses paramètres) de l'élément à produire (certificat ou LCR) ;
- De rechercher un profil dans un domaine de confiance ;
- De consulter un profil (certificat ou LCR) dans un domaine de confiance ;
- D'activer ou désactiver un profil dans un domaine de confiance afin qu'il puisse ou non être utilisé pour produire un certificat ou une LCR ;

- De créer un type demande en indiquant le profil (certificat ou LCR) à utiliser pour la génération de l'élément demandé (certificat ou LCR), les rôles de confiance requis et les AC au sein d'un domaine de confiance à utiliser ;
- De rechercher un type de demande dans le service d'application ;
- De consulter un type de demande ;
- De modifier les paramètres d'un type de demande ;
- D'authentifier et d'autoriser un rôle de confiance ;
- D'activer ou désactiver un type de demande pour que le service d'application puisse ou non utiliser les types de demande en question pour traiter les requêtes provenant des rôles de confiance reconnus.

5.1.1.1.3 Trust.Center® _XRMP

Cette fonction permet :

- D'authentifier les demandes de révocation émises par un rôle de confiance qui utilise le protocole XRMP (Système d'information Client ou au proxy d'AE) ;
- D'authentifier les demandes de retrait de certificats émises par un rôle de confiance qui utilise le protocole XRMP (système d'information Client ou au proxy d'AE) ;
- De transmettre des certificats à un système d'information Client ou au proxy d'AE.

5.1.1.1.4 Trust.Center® _Rôles de confiance

Cette fonction permet :

- De créer un rôle de confiance pour un domaine de confiance (administrateur, opérateur ou auditeur). Un rôle de confiance est associé à un certificat qui permettra d'authentifier l'acteur qui souhaite mettre en œuvre des fonctions à l'aide de son rôle de confiance ;
- De rechercher un rôle de confiance et son certificat associé ;
- De consulter les caractéristiques d'un rôle de confiance ;
- De révoquer un rôle de confiance à un acteur de la TOE en lui révoquant son certificat associé au rôle qu'on lui retire.

5.1.1.1.5 Trust.Center® _Cycle de vie des certificats et des LCR

Cette fonction permet :

- D'authentifier et d'autoriser un rôle de confiance ;
- De générer un certificat, suite à une demande de certificat venant de Trust.Center® _XRMP sur Trust.Center®, en créant la requête de demande de signature de certificat pour le service cryptographique ;
- De recevoir le certificat au format PKCS#7 transmis par le HSS ;
- De rechercher : rechercher un certificat d'un porteur de certificat à partir de paramètre tel que le DN ;
- De consulter un certificat d'un porteur de certificat ;
- De révoquer un certificat, suite à une demande de révocation venant d'un client XRMP ou d'un proxy d'AE, en enregistrant l'identifiant du certificat à révoquer pour qu'il soit contenu dans la futur LCR générée ;
- De générer une LCR, à partir des profils de LCR définit au sein du service d'application pour le domaine de confiance et des identifiants des certificats porteurs révoqués, en créant la requête de demande de signature de LCR pour le HSS ;
- De recevoir ensuite la LCR transmis par le HSS ;
- De stocker les certificats et les LCR à publier au sein du service d'application en attendant leur publication ;
- De publier au profit des clients du service de publication les certificats et les LCR par l'intermédiaire du service de publication qui vient récupérer les informations sur le service d'application et les publie ;
-

5.1.1.1.6 Trust.Center® _Journalisation et audit

Cette fonction permet :

- De journaliser l'activation d'une action a sein d'une fonction de sécurité de la TOE en enregistrant dans le service de base de données tous les évènements relatifs au résultat de l'exécution de cette fonction. Un enregistrement du journal contient les informations suivantes :
    - La date de l'événement ;
    - Le type d'événement (Information, Avertissement, Erreur, Debug …) ;
    - Le module d'exécution ;
    - L'acteur générant l'événement ;
    - Le domaine de confiance dans lequel l'évènement a lieu ;
    - L'identifiant de l'objet subissant l'événement (ex : N° certificat) ;
    - Des informations complémentaires spécifiques a l'événement.
- De consulter des évènements relatifs à une fonction à l'aide du rôle de confiance « auditeur » pour un domaine de confiance identifié. Le mode de consultation permet d'avoir de mettre en place des filtres pour la consultation.

5.1.1.1.7 Trust.Center® _Gestion site web

Cette fonction permet :

- De gérer les IHM du site AET ;
- De gérer les IHM du site ATC ;
- De gérer les interfaces du site service web.

5.1.1.2 Service de signature (HSS)

5.1.1.2.1 HSS_Profil de donnée à signer

Cette fonction permet :

- De définir et de paramétrer le contenu d'une donnée à signer (certificat, LCR, contremarque de temps, …) et à formater en fonction des requêtes que reçoit le SC de la part d'un module Client (Service applicatif Trust.Center®, …).

5.1.1.2.2 HSS_Traitement des requêtes de signature

Cette fonction permet :

- De recevoir les requêtes par son module réseau d'un module Client (Service d'application, …) et d'en vérifier le contenu au regard des formats prédéfinis ;
- De formater les données à signer envoyées par le service d'application de Trust.Center® en garantissant l'unicité des requêtes ;
- De transmettre vers le HSM la donnée à faire signer par l'AC identifiée et de récupérer la donnée signée (PKCS#11) ;
- De router vers le HSM la donnée à faire signer par l'AC identifiée ;
- De renvoyer les données signée et formatées au module Client (service d'application de Trust.Center®, …).

5.1.2 K.Registration®

5.1.2.1 SA – K.Registration®

5.1.2.1.1 K.Registration® _Domaine de confiance

Cette fonction permet :

- De créer un domaine de confiance pour cloisonner les données d'un Client à l'autre ;
- D'activer un domaine un domaine de confiance ;
- De désactiver un domaine de confiance ;
- D'affecter un certificat au domaine de confiance pour sécuriser les communications vers le proxy d'AE (K.Registration_Proxy d'AE).

5.1.2.1.2 K.Registration® _Offre de certification

Cette fonction permet :

- De créer une offre en définissant l'ensemble des paramètres qui constitue une offre de certification (profil de certificat, profil de LCR, profils des opérateurs, AC destinatrice, mode d'authentification, …) ;
- De rechercher une offre au sein de K.Registration® ;
- De consulter une offre au sein de K.Registration® ;
- De modifier une offre au sein de K.Registration® ;
- D'activer ou de désactiver une offre au sein d'un domaine de confiance de K.Registration® ;
- De supprimer une offre au sein d'un domaine de confiance de K.Registration®.

5.1.2.1.3 K.Registration® _Rôle de confiance

Cette fonction permet :

- De créer un rôle de confiance (administrateur ou opérateur). Un rôle de confiance est associé à un certificat qui permettra d'authentifier l'acteur qui souhaite mettre en œuvre des fonctions à l'aide de son rôle de confiance ;
- De définir les droits d'un rôle de confiance (offre de certification, type d'action, …) ;
- De rechercher un rôle de confiance et son certificat associé ;
- De consulter les caractéristiques d'un rôle de confiance ;
- De révoquer un rôle de confiance à un acteur de la TOE (par révocation du certificat associé au rôle qu'on lui retire).

5.1.2.1.4 K.Registration® _Mise en œuvre d'une offre de certification

Cette fonction permet :

- De demander un certificat en fonction du profil de l'acteur (opérateur ou porteur de certificat) ;
- De supprimer une demande de certificat ;
- D'affecter une demande de certificat ;
- De valider une demande de certificat en cours (opérateur de certificat) ;
- D'authentifier et d'autoriser un rôle de confiance ;
- De révoquer un certificat en fonction du profil de l'acteur (opérateur ou porteur de certificat) ;
- De renouveler de certificat en fonction du profil de l'acteur (opérateur ou porteur de certificat) ;
- De retirer un certificat en fonction du profil de l'acteur (opérateur ou porteur de certificat) ;
- De suspendre un certificat en fonction du profil de l'acteur (opérateur ou porteur de certificat) ;
- D'authentifier et d'autoriser un rôle de confiance ;
- De transmettre des demande de certificat et de révocation signé au proxy d'AE ;
- De recevoir les certificats venant du proxy d'AE ;
- De notifier de la réalisation des actions demande, génération, renouvellement et révocation d'un certificat, si cela est souhaité, en envoyant un mail. Le mail est crée et envoyé au service de notification.

5.1.2.1.5 K.Registration® _Journalisation et audit

Cette fonction permet :

- De journaliser l'activation d'une fonction en enregistrant dans le service de base de données tous les évènements relatifs à l'exécution d'une fonction. Un enregistrement du journal contient les informations suivantes :
  - La date de l'événement ;
  - Le type d'événement (Information, Avertissement, Erreur, Debug …) ;
  - Le module d'exécution ;
  - L'acteur générant l'événement ;
  - Le domaine de confiance dans lequel l'évènement a lieu ;
  - Des informations complémentaires spécifiques a l'événement ;
- De consulter des évènements relatifs à une fonction à l'aide du rôle de confiance « auditeur » pour une ou plusieurs offres de certification. Le mode de consultation permet d'avoir de mettre en place des filtres pour la consultation.

5.1.2.1.6 K.Registration® _Gestion site web

Cette fonction permet :

- De gérer les IHM du site Administration ;
- De gérer les IHM du site Opérateur ;
- De gérer les IHM du site Utilisateur ;
- De gérer les interfaces du site services web.

5.1.2.2 Proxy d'AE

Cette fonction permet :

- De recevoir les demandes de certificat et de révocation venant du SA - K.Registration® ;
- De créer des requêtes de demande de certificats à destination de Trust.Center® ;
- De créer des requêtes de demande de révocation à destination de Trust.Center® ;
- De router des requêtes de demandes de certificats à destination de Trust.Center® ;
- De router des requêtes de demande de révocation à destination de Trust.Center®
- De recevoir les certificats émis par le Trust.Center® ;
- D'envoyer les certificats vers le SA - K.Registration®.

5.1.3 Keyseed®

5.1.3.1 Keyseed® _Mise en œuvre de script

Cette fonction permet :

- De définir et de paramétrer le contenu d'une donnée à signer (certificat AC et ACR, LAR et certificat rôles de confiance) ;
- De gérer le cycle de vie des clés cryptographiques des AC hébergées sur le module cryptographique (génération, destruction, importation, exportation, activation, désactivation, révocation et reconstitution) via les commandes Pkcs#11 utilisé pour communiquer avec le HSM ;
- De créer des demande de certificat d'AC, d'ACR et de certificat rôle de confiance ;
- De créer des demandes de LAR ;
- De créer des certificat d'AC, d'ACR, des LAR et rôle de confiance ;
- Impression d'un procès verbale ;
- Export de clé du HSM.

6 ARGUMENTAIRE

6.1 Couverture des menaces par les objectifs de sécurité

6.1.1 Tableau de croisement Menace/Objectif

	M_Rôle de confiance	M_Journalisation	M_Erreur d'utilisation	M_Altération des biens	M_Rôle de confiance autorisé	M_Autorisation	M_Divulgation
O.SERVICES	♦	♦	♦	♦	♦	♦	♦
O.ADMINISTRATION	♦	♦	♦	♦	♦	♦	♦
O.AUDIT	♦	♦	♦	♦	♦	♦	♦
O.AUTHENTIFICATION	♦	♦	♦	♦	♦	♦	♦
O.AUTORISATION	♦	♦	♦	♦	♦	♦	♦
O.PROTECT_DONNEES	♦	♦	♦	♦	♦	♦	♦
O.TRANS_DATA	♦	♦	♦	♦	♦	♦	♦
O.ESPIONNAGE_DISTANT	♦					♦	♦
O.TEMPSREF	♦	♦		♦	♦	♦	
O.CRYPTO	♦	♦		♦	♦	♦	♦
OE_RETOUR_ETAT_SUR	♦	♦	♦	♦	♦	♦	♦
OE_Administrateur système	♦	♦	♦	♦	♦	♦	♦
OE_Porteur de données d'activation			♦	♦	♦	♦	♦

OE_Attribution de rôle	♦		♦	♦		♦	♦
OE_Machines hôtes	♦	♦	♦	♦		♦	♦
OE_Réseau	♦	♦	♦	♦	♦	♦	♦
OE_Sauvgarde		♦		♦		♦	
OE_machine hôte Keyseed®	♦	♦	♦	♦		♦	♦
OE_machine hôte Trust.Center®	♦	♦	♦	♦		♦	♦
OE_machine hôte K.Registration®	♦	♦	♦	♦		♦	♦
OE_Client XRMP	♦		♦	♦		♦	♦
OE_SI Client	♦	♦	♦	♦	♦	♦	♦
OE_Temps de référence		♦		♦			♦
OE_ Service cryptographique_AC (HSM)		♦		♦			♦
OE_bi-clés_Rôle de confiance	♦			♦			♦
OE_Protection d'une clé privée associée à un certificat				♦			♦
OE_Politique de certification		♦	♦	♦	♦	♦	♦
OE_Protection_physique				♦			♦

6.2 Couverture des politiques de sécurité organisationnelle par les objectifs

6.2.1 Tableau de croisement Objectifs/Politiques

	OSP_Services de	OSP_Cloisonnemen	OSP_Rôles	OSP_Admin	OSP_Audit_admin	OSP_Audit_flux	OSP_Configuration_	OSP_Sauvegarde	OSP_Rôles de		OSP_Service		OSP_Crypto

	certification	t					sûre		confiance		cryptographique TOE		
O.SERVICES	♦	♦	♦		♦	♦			♦		♦		
O.ADMINISTRATION	♦	♦	♦	♦	♦				♦				
O.AUDIT	♦		♦		♦	♦		♦					
O.AUTHENTIFICATION	♦	♦	♦	♦	♦				♦				
O.AUTORISATION	♦	♦	♦	♦	♦				♦				
O.PROTECT_DONNEES	♦	♦		♦	♦	♦	♦	♦	♦		♦		
O.TRANS_DATA	♦	♦		♦	♦								
O.ESPIONNAGE_DISTANT	♦	♦		♦									
O.TEMPSREF	♦					♦							
O.CRYPTO	♦	♦									♦		♦

6.3 Couverture des hypothèses par les objectifs sur l'environnement

6.3.1 Tableau de croisement Hypothèse/Objectifs

	H_Administrateur système	H_Porteur de données d'activation		H_Attribution de rôle	H_Machines hôtes	H_Réseau	H_Sauvgarde	H_machine hôte Keyseed®	H_machine hôte Trust.Center®	H_machine hôte K.Registration®	H_Client XRMP	H_SI Client	H_Temps de référence	H_Service cryptographique_AC (HSM)	H_bi-clés_Rôle de confiance	H_Protection d'une clé privée associée à un certificat	H_Politique de certification	H_Protection physique de la TOE
OE_Administrateur système	♦																	
OE_Porteur de		♦																

données d'activation																	
OE_Attribution de rôle				♦													
OE_Machines hôtes					♦												
OE_Réseau						♦											
OE_Sauvgarde							♦										
OE_machine hôte Keyseed®								♦									
OE_machine hôte Trust.Center®									♦								
OE_machine hôte K.Registration®										♦							
OE_Client XRMP											♦						
OE_SI Client												♦					
OE_Temps de référence													♦				
OE_Service cryptographique_AC (HSM)														♦			
OE_bi-clés_Rôle de confiance															♦		
OE_Protection																♦	

d'une clé privée associée à un certificat																		
OE_RETOUR_ETAT_SUR							♦											
OE_Politique de certification	♦	♦		♦	♦	♦	♦	♦	♦	♦			♦	♦	♦	♦	♦	♦
OE_Protection_physique																		♦

6.4 Couverture des objectifs par les exigences de sécurité

6.4.1 Tableau de croisement Exigences fonctionnelles de sécurité/Objectifs

	O.SERVICES	O.ADMINISTRATION	O.AUDIT	O.AUTHENTIFICATION	O.AUTORISATION	O.PROTECT_DONNEES	O.TRANS_DATA	O.ESPIONNAGE_DISTANT		O.TEMPSREF	O.CRYPTO
FAU_GEN.1			♦								
FAU_GEN.2			♦								
FAU_SAR.1			♦								
FAU_SAR.2			♦								
FAU_SAR.3			♦								
FAU_SEL.1			♦								
FAU_STG.1			♦			♦					
FCO_NRO.2			♦				♦				
FCO_NNR.2	♦			♦			♦				
FCS_COP.1											♦
FDP_ACC.2					♦						

FDP_ACF.1					♦						
FDP_DAU.2				♦	♦	♦	♦				
FDP_ETC.1		♦			♦	♦	♦				
FDP_IFC.2	♦						♦				
FDP_IFF.1	♦						♦				
FDP_ITC.1							♦				
FDP_ITC.2							♦				
FDP_ITT.1							♦				
FDP_UCT							♦				
FDP_UIT.1							♦				
FIA_AFL.1				♦	♦						
FIA_ATD.1		♦			♦						
FIA_SOS.2				♦							
FIA_UAU.1				♦							
FIA_UAU.2				♦				♦			
FIA_UID.2				♦	♦						
FIA_USB.1		♦			♦						
FMT_MOF.1		♦									
FMT_MSA.1		♦				♦					
FMT_MSA.2		♦				♦					
FMT_MSA.3		♦				♦					
FMT_MTD.1		♦				♦					
FMT_MTD.3		♦				♦					
FMT_REV.1		♦									
FMT_SMF.1		♦									
FMT_SMR.2		♦			♦						
FPT_RPL.1							♦				
FPT_STM.1			♦							♦	
FPT_TDC.1						♦					
FPT_ITT.1							♦				

FTA_LSA.1						♦					
FTA_SSL.1				♦							
FTA_SSL.2				♦							
FTA_SSL.3				♦							
FTA_SSL.4				♦							
FTA_TSE.1				♦	♦		♦				
FTP_ITC.1							♦				
FTP_TRP.1							♦				

6.5 Couverture

6.5.1 Tableau de croisement Exigences fonctionnelles de sécurité/Fonctions Sequoia®

	Trust.Center®_Domaine de confiance	Trust.Center®_Administration des AC	Trust.Center®_XRMP	Trust.Center®_Rôles de confiance	Trust.Center®_Cycle de vie des certificats et des LCR	Trust.Center®_Journalisation et audit	Trust.Center®_Gestion site web	HSS_Profil de donnée à signer	HSS_Traitement des requêtes de signature	HSS_Journalisation et audit	K.Registration®_Gestion site web	K.Registration®_Domaine de confiance	K.Registration®_ proxy d'AE	K.Registration®_Offre de certification	K.Registration®_Rôle de confiance	K.Registration®_Mise en œuvre d'une offre de certification	K.Registration®_Journalisation et audit	KeySeed®_Mise en œuvre de script	
FAU_GEN.1						♦				♦							♦		
FAU_GEN.2						♦				♦							♦		
FAU_SAR.1						♦											♦		
FAU_SAR.2						♦											♦		
FAU_SAR.3						♦											♦		
FAU_SEL.1						♦											♦		
FAU_STG.1						♦											♦		
FCO_NRO.2			♦		♦											♦			
FCO_NRR.2														♦		♦			

FCS_COP.1			♦		♦				♦				♦			♦		♦	
FDP_ACC.2					♦											♦			
FDP_ACF.1	♦											♦		♦					
FDP_DAU.2			♦		♦								♦			♦			
FDP_ETC.1					♦											♦		♦	
FDP_IFC.2									♦				♦						
FDP_IFF.1									♦				♦					♦	
FDP_ITC.1			♦		♦											♦			
FDP_ITC.2			♦		♦											♦			
FDP_ITT.1			♦										♦			♦			
FDP_UCT			♦										♦			♦			
FDP_UIT.1			♦										♦			♦			
FIA_AFL.1																♦			
FIA_ATD.1	♦			♦								♦			♦				
FIA_SOS.2																♦			
FIA_UAU.1											♦					♦			
FIA_UAU.2					♦		♦				♦					♦			
FIA_UID.2					♦											♦			
FIA_USB.1	♦			♦								♦		♦	♦				
FMT_MOF.1					♦											♦			
FMT_MSA.1	♦			♦								♦		♦	♦				
FMT_MSA.2	♦			♦								♦		♦	♦				
FMT_MSA.3	♦			♦								♦		♦	♦				

FMT_MTD.1				♦										♦	♦			
FMT_MTD.3		♦	♦					♦					♦	♦				
FMT_REV.1					♦											♦		
FMT_SMF.1					♦											♦		♦
FMT_SMR.2	♦			♦								♦		♦	♦			
FPT_ITT.1			♦										♦			♦		
FPT_RPL.1		♦												♦				
FPT_STM.1					♦	♦			♦	♦							♦	
FPT_TDC.1		♦						♦						♦				♦
FTA_LSA.1	♦	♦		♦	♦	♦	♦				♦	♦		♦	♦	♦	♦	
FTA_SSL.1					♦											♦		
FTA_SSL.2					♦											♦		
FTA_SSL.3					♦											♦		
FTA_SSL.4					♦											♦		
FTA_TSE.1	♦	♦		♦	♦	♦	♦				♦	♦		♦	♦	♦	♦	
FTP_ITC.1			♦													♦		
FTP_TRP.1					♦											♦		

6.6 Dépendances

6.6.1 Trust.Center®

Composant	Intitulé	Dépendances requises	Dépendance	Commentaires

			satisfaite	
FAU_GEN.1	Audit data generation	FPT_STM.1	Oui	
FAU_GEN.2	User identity association	FAU_GEN.1 et FIA_UID.1	Oui (FIA_UID.2)	FIA_UID.2 est supérieurement hiérarchique et est donc pris à la place.
FAU_SAR.1	Audit review	FAU_GEN.1	Oui	
FAU_SAR.2	Restricted audit review	FAU_SAR.1	Oui	
FAU_SAR.3	Selectable audit review	FAU_SAR.1	Oui	
FAU_SEL.1	Selective audit	FAU_GEN.1	Oui	
		FMT_MTD.1	Oui	
FAU_STG.1	Protected audit trail storage	FAU_GEN.1	Oui	
FCO_NRO.2	Selective proof of origin	FIA_UID.1	Oui (FIA_UID.2)	FIA_UID.2 est supérieurement hiérarchique et est donc pris à la place.
FCS_COP.1	Cryptographic operation	(FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1) et FCS_CKM.4	Partiel (FDP_ITC.1 et FDP_ITC.2)	FCS_CKM.4 n'est pas satisfait car les clés sont stockées dans le HSM et c'est ce dernier qui est responsable de leur destruction.
FDP_ACC.2	Complete access control	FDP_ACF.1	Oui	
FDP_ACF.1	Security attribute based access control	FDP_ACC.1 et FMT_MSA.3	Oui (FDP_ACC.2)	
FDP_DAU.2	Data authentication with identity of Guarantor	FIA_UID.1	Oui (FIA_UID.2)	FIA_UID.2 est supérieurement hiérarchique et est donc pris à la place.
FDP_ETC.1	Export of user data without security attribute	FDP_ACC.1 ou FDP_IFC.1	Oui	FDP_ACC.2 est supérieurement hiérarchique et est donc pris à la place.
FDP_IFC.2	Complete information flow control	FDP_IFF.1	Oui	
FDP_IFF.1	Simple security attributes	FDP_IFC.1 et FMT_MSA.3	Oui (FDP_IFC.2)	FDP_IFC.2 est supérieurement hiérarchique et est donc pris à la place.
FDP_ITC.1	Import of user data without security attributes	(FDP_IFC.1 ou FDP_ACC.1) et FMT_MSA.3	Oui (FDP_ACC.2)	Quelque soient les flus, tous depend des règles de contrôle d'accès et de plus il n'y a pas d'échange entre

				composantes de ce type de données.
FDP_ITC.2	Import of user data with security attributes	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1) et FPT_TDC.1	Oui (FDP_ACC.2, FTP_TRP.1)	FDP_ACC.2 est supérieurement hiérarchique et est donc pris à la place. Quelque soient les flus, tous depend des règles de contrôle d'accès et de plus il n'y a pas d'échange de ce type de données. Il n'y a pas de circulation d'information (security attribute) entre composantes.
FDP_ITT.1	Basic internal transfer protection	(FDP_ACC.1 ou FDP_IFC.1)	Oui (FDP_ACC.2)	FDP_ACC.2 est supérieurement hiérarchique et est donc pris à la place. Quelque soient les flus, tous depend des règles de contrôle d'accès.
FDP_UCT.1	Basic data exchange confidentiality	(FTP_ITC.1 ou FTP_TRP.1) et (FDP_ACC.1 ou FDP_IFC.1)	Oui (FDP_ACC.2, FTP_TRP.1)	FDP_ACC.2 est supérieurement hiérarchique et est donc pris à la place. Quelque soient les flus, tous depend des règles de contrôle d'accès. Quelque soient les flus, tous depend des règles de contrôle d'accès.
FDP_UIT.1	Data exchange integrity	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	Oui (FDP_ACC.2, FTP_TRP.1)	Quelque soient les flus, tous depend des règles de contrôle d'accès.
				Quelque soient les flus, tous depend des règles de contrôle d'accès.
FIA_ATD.1	User attribute definition	Aucune	Oui	
FIA_UAU.2	User authentication before any action	FIA_UID.1	Oui (FIA_UID.2)	FIA_UID.1 est supérieurement hiérarchique et est donc pris à la place.
FIA_UID.2	User identification before any action	Aucune	Oui	
FIA_USB.1	User-subject binding	FIA_ATD.1	Oui	
FMT_MOF.1	Management of security functions behaviour	FMT_SMR.1 et FMT_SMF.1	Oui (FMT_SMR	FMT_SMR.2 est supérieurement hiérarchique et est donc pris à la

			.2)	place.
FMT_MSA.1	Management of security attributes	(FDP_ACC.1 ou FDP_IFC.1) et FMT_SMR.1 et FMT_SMF.1	Oui (FDP_ACC .2, FMT_SMR. 2 et FMT_SMF. 1)	FDP_ACC.2 est supérieurement hiérarchique et est donc pris à la place. Quelque soient les flus, tous depend des règles de contrôle d'accès. FMT_SMR.2 est supérieurement hiérarchique et est donc pris à la place.
FMT_MSA.2	Secure security attributes	(FDP_ACC.1 ou FDP_IFC.1) et FMT_SMR.1 et FMT_MAS.1	Oui (FDP_ACC .2, FMT_SMR. 2)	FDP_ACC.2 est supérieurement hiérarchique et est donc pris à la place. FMT_SMR.2 est supérieurement hiérarchique et est donc pris à la place.
FMT_MSA.3	Static attribute initialisation	FMT_MSA.1 et FMT_SMR.1	Oui (FMT_SMR .2)	FMT_SMR.2 est supérieurement hiérarchique et est donc pris à la place.
FMT_MTD.1	Management of TSF data	FMT_SMR.1 et FMT_SMF.1	Oui (FMT_SMR .2)	FMT_SMR.2 est supérieurement hiérarchique et est donc pris à la place.
FMT_MTD.3	Secure TSF data	FMT_MTD.1	Oui	
FMT_REV.1	Revocation	FMT_SMR.1	Oui (FMT_SMR .2)	FMT_SMR.2 est supérieurement hiérarchique et est donc pris à la place.
FMT_SMF.1	Specification of Management Functions	Aucune	Oui	
FMT_SMR.2	Restrictions on security roles	FIA_UID.1	Oui (FIA_UID.2)	FIA_UID.2 est supérieurement hiérarchique et est donc pris à la place.
FPT_ITT.1	Basic internal TSF data transfer protection	Aucune	Oui	
FPT_RPL.1	Replay detection	Aucune	Oui	
FPT_STM.1	Reliable time stamps	Aucune	Oui	
FPT_TDC.1	Inter-TSF basic TSF data consistency	Aucune	Oui	
FTA_LSA.1	Limitation on scope of selectable attributes	Aucune	Oui	
FTA_SSL.1	TSF-initiated session locking	FIA_UAU.1	Oui (FIA_UAU. 2)	FIA_UAU.1 ne s'applique à la composante et FIA_UAU.2 est supérieurement hiérarchique et est

				donc pris à la place.
FTA_SSL.2	User-initiated locking	FIA_UAU.1	Oui (FIA_UAU.2)	FIA_UAU.1 ne s'applique à la composante et FIA_UAU.2 est supérieurement hiérarchique et est donc pris à la place.
FTA_SSL.3	TSF-initiated termination	Aucune	Oui	
FTA_SSL.4	User-initiated termination	Aucune	Oui	
FTA_TSE.1	TOE session establishment	Aucune	Oui	
FTP_ITC.1	Inter-TSF trusted channel	Aucune	Oui	
FTP_TRP.1	Trusted path	Aucune	Oui	

6.6.2 K.Registration®

Composant	Intitulé	Dépendances requises	Dépendance satisfaite	Commentaires
FAU_GEN.1	Audit data generation	FPT_STM.1	Oui	
FAU_GEN.2	User identity association	FAU_GEN.1 et FIA_UID.1	Oui (FIA_UID.2)	FIA_UID.2 est supérieurement hiérarchique et est donc pris à la place.
FAU_SAR.1	Audit review	FAU_GEN.1	Oui	
FAU_SAR.2	Restricted audit review	FAU_SAR.1	Oui	
FAU_SAR.3	Selectable audit review	FAU_SAR.1	Oui	
FAU_SEL.1	Selective audit	FAU_GEN.1	Oui	
		FMT_MTD.1	Oui	
FAU_STG.1	Protected audit trail storage	FAU_GEN.1	Oui	
FCO_NRO.2	Selective proof of origin	FIA_UID.1	Non	FIA_UID.2 est supérieurement hiérarchique et est donc pris à la place.
		FIA_UID.2	Oui	
FCO_NRR.2	Enforced proof of receipt	FIA_UID.1	Oui (FIA_UID.2)	
FCS_COP.1	Cryptographic operation	(FDP_ITC.1 ou	Partiel	FCS_CKM.4 n'est pas satisfait car les

		FDP_ITC.2 ou FCS_CKM.1) et FCS_CKM.4	(FDP_ITC.1 et FDP_ITC.2)	clés sont stockées dans le HSM, ou dans le serveur support au logiciel K.Registration®, et c'est ce dernier qui est responsable de leur destruction.
FDP_ACC.2	Complete access control	FDP_ACF.1	Oui	
FDP_ACF.1	Security attribute based access control	FDP_ACC.1 et FMT_MSA.3	Oui (FDP_ACC.2)	
FDP_DAU.2	Data authentication with identity of Guarantor	FIA_UID.1	Oui (FIA_UID.2)	FIA_UID.2 est supérieurement hiérarchique et est donc pris à la place.
FDP_ETC.1	Export of user data without security attribute	FDP_ACC.1 ou FDP_IFC.1	Oui	FDP_ACC.2 est supérieurement hiérarchique et est donc pris à la place.
FDP_IFC.2	Complete information flow control	FDP_IFF.1	Oui	
FDP_IFF.1	Simple security attributes	FDP_IFC.1 et FMT_MSA.3	Oui (FDP_IFC.2)	FDP_IFC.2 est supérieurement hiérarchique et est donc pris à la place.
FDP_ITC.1	Import of user data without security attributes	(FDP_IFC.1 ou FDP_ACC.1) et FMT_MSA.3	Oui (FDP_ACC.2)	Quelque soient les flus, tous depend des règles de contrôle d'accès et de plus il n'y a pas d'échange entre composantes de ce type de données.
FDP_ITC.2	Import of user data with security attributes	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1) et FPT_TDC.1	Oui (FDP_ACC.2, FTP_TRP.1)	FDP_ACC.2 est supérieurement hiérarchique et est donc pris à la place. Quelque soient les flus, tous depend des règles de contrôle d'accès et de plus il n'y a pas d'échange de ce type de données. Il n'y a pas de circulation d'information (security attribute) entre composantes.
FDP_ITT.1	Basic internal transfer protection	(FDP_ACC.1 ou FDP_IFC.1)	Oui (FDP_ACC.2)	FDP_ACC.2 est supérieurement hiérarchique et est donc pris à la place. Quelque soient les flus, tous depend des règles de contrôle d'accès.
FDP_UCT.1	Basic data exchange confidentiality	(FTP_ITC.1 ou	Oui	FDP_ACC.2 est supérieurement

		FTP_TRP.1) et (FDP_ACC.1 ou FDP_IFC.1)	(FDP_ACC.2, FTP_TRP.1)	hiérarchique et est donc pris à la place. Quelque soient les flus, tous depend des règles de contrôle d'accès. Quelque soient les flus, tous depend des règles de contrôle d'accès.
FDP_UIT.1	Data exchange integrity	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	Oui (FDP_ACC.2, FTP_TRP.1)	Quelque soient les flus, tous depend des règles de contrôle d'accès.
FIA_AFL.1	Authentication failure handling	FIA_UAU.1	Oui (FIA_UAU.2)	FIA_UAU.2 est supérieurement hiérarchique et est donc pris à la place.
FIA_ATD.1	User attribute definition	Aucune	Oui	
FIA_SOS.2	Generation of secrets	Aucune	Oui	
FIA_UAU.1	Timing of authentication	FIA_UID.1	Oui (FIA_UID.2)	FIA_UID.2 est supérieurement hiérarchique et est donc pris à la place.
FIA_UAU.2	User authentication before any action	FIA_UID.1	Oui (FIA_UID.2)	FIA_UID.2 est supérieurement hiérarchique et est donc pris à la place.
FIA_UID.2	User identification before any action	Aucune	Oui	
FIA_USB.1	User-subject binding	FIA_ATD.1	Oui	
FMT_MOF.1	Management of security functions behaviour	FMT_SMR.1 et FMT_SMF.1	Oui (FMT_SMR.2)	FMT_SMR.2 est supérieurement hiérarchique et est donc pris à la place.
FMT_MSA.1	Management of security attributes	(FDP_ACC.1 ou FDP_IFC.1) et FMT_SMR.1 et FMT_SMF.1	Oui (FDP_ACC.2, FMT_SMR.2 et FMT_SMF.1)	FDP_ACC.2 est supérieurement hiérarchique et est donc pris à la place. Quelque soient les flus, tous depend des règles de contrôle d'accès. FMT_SMR.2 est supérieurement hiérarchique et est donc pris à la place.
FMT_MSA.2	Secure security attributes	(FDP_ACC.1 ou FDP_IFC.1) et	Oui (FDP_ACC	FDP_ACC.2 est supérieurement hiérarchique et est donc pris à la

		FMT_SMR.1 et FMT_MAS.1	.2, FMT_SMR.2)	place. FMT_SMR.2 est supérieurement hiérarchique et est donc pris à la place.
FMT_MSA.3	Static attribute initialisation	FMT_MSA.1 et FMT_SMR.1	Oui (FMT_SMR.2)	FMT_SMR.2 est supérieurement hiérarchique et est donc pris à la place.
FMT_MTD.1	Management of TSF data	FMT_SMR.1 et FMT_SMF.1	Oui (FMT_SMR.2)	FMT_SMR.2 est supérieurement hiérarchique et est donc pris à la place.
FMT_MTD.3	Secure TSF data	FMT_MTD.1	Oui	
FMT_REV.1	Revocation	FMT_SMR.1	Oui (FMT_SMR.2)	FMT_SMR.2 est supérieurement hiérarchique et est donc pris à la place.
FMT_SMF.1	Specification of Management Functions	Aucune	Oui	
FMT_SMR.2	Restrictions on security roles	FIA_UID.1	Oui (FIA_UID.2)	FIA_UID.2 est supérieurement hiérarchique et est donc pris à la place.
FPT_ITT.1	Basic internal TSF data transfer protection	Aucune	Oui	
FPT_RPL.1	Replay detection	Aucune	Oui	
FPT_STM.1	Reliable time stamps	Aucune	Oui	
FPT_TDC.1	Inter-TSF basic TSF data consistency	Aucune	Oui	
FTA_LSA.1	Limitation on scope of selectable attributes	Aucune	Oui	
FTA_SSL.1	TSF-initiated session locking	FIA_UAU.1	Oui	
FTA_SSL.2	User-initiated locking	FIA_UAU.1	Oui	
FTA_SSL.3	TSF-initiated termination	Aucune	Oui	
FTA_SSL.4	User-initiated termination	Aucune	Oui	
FTA_TSE.1	TOE session establishment	Aucune	Oui	
FTP_ITC.1	Inter-TSF trusted channel	Aucune	Oui	
FTP_TRP.1	Trusted path	Aucune	Oui	

6.6.3 Keyseed®

Les dépendances pour les composants fonctionnels de sécurité sont les suivants :

Composant	Intitulé	Dépendances requises	Dépendance satisfaite	Commentaires

FAU_GEN.1	Audit data generation			Non retenu pour la composante.
FAU_GEN.2	User identity association			Non retenu pour la composante.
FAU_SAR.1	Audit review			Non retenu pour la composante.
FAU_SAR.2	Restricted audit review			Non retenu pour la composante.
FAU_SAR.3	Selectable audit review			Non retenu pour la composante.
FAU_SEL.1	Selective audit			Non retenu pour la composante.
FAU_STG.1	Protected audit trail storage			Non retenu pour la composante.
FCO_NRO.2	Selective proof of origin			Non retenu pour la composante.
FCO_NRR.2	Enforced proof of receipt			Non retenu pour la composante.
FCS_COP.1	Cryptographic operation	FDP_ITC.2	Non	FDP_ITC.2 n'est pas satisifait car c'est le HSM qui choisit la clé pour signer en fonction des informations transmis par Keyseed®.
		FCS_CKM.1	Non	FCS_CKM.1 n'est pas satisfait car les clés sont stockées dans le HSM et c'est ce dernier qui est responsable de leur génération.
		FCS_CKM.4	Non	FCS_CKM.4 n'est pas satisfait car les clés sont stockées dans le HSM et c'est ce dernier qui est responsable de leur destruction.
FDP_ACC.2	Complete access control			Non retenu pour la composante.
FDP_ACF.1	Security attribute based access control			Non retenu pour la composante.
FDP_DAU.2	Data authentication with identity of Guarantor			Non retenu pour la composante.
FDP_ETC.1	Export of user data without security attribute			Non retenu pour la composante.
FDP_IFC.2	Complete information flow control			Non retenu pour la composante.
FDP_IFF.1	Simple security attributes			Non retenu pour la composante.
FDP_ITC.1	Import of user data without security attributes			Non retenu pour la composante.
FDP_ITC.2	Import of user data with security attributes			Non retenu pour la composante.
FDP_ITT.1	Basic internal transfer protection			Non retenu pour la composante.
FDP_UCT.1	Basic data exchange confidentiality			Non retenu pour la composante.
FDP_UIT.1	Data exchange integrity			Non retenu pour la composante.
FIA_AFL.1	Authentication failure handling			Non retenu pour la composante.
FIA_ATD.1	User attribute definition			Non retenu pour la composante.
FIA_SOS.2	Generation of secrets			Non retenu pour la composante.

FIA_UAU.1	Timing of authentication			Non retenu pour la composante.
FIA_UAU.2	User authentication before any action			Non retenu pour la composante.
FIA_UID.2	User identification before any action			Non retenu pour la composante.
FIA_USB.1	User-subject binding			Non retenu pour la composante.
FMT_MOF.1	Management of security functions behaviour			Non retenu pour la composante.
FMT_MSA.1	Management of security attributes			Non retenu pour la composante.
FMT_MSA.2	Secure security attributes			Non retenu pour la composante.
FMT_MSA.3	Static attribute initialisation			Non retenu pour la composante.
FMT_MTD.1	Management of TSF data			Non retenu pour la composante.
FMT_MTD.3	Secure TSF data			Non retenu pour la composante.
FMT_REV.1	Revocation			Non retenu pour la composante.
FMT_SMF.1	Specification of Management Functions	Aucune	Oui	
FMT_SMR.2	Restrictions on security roles			Non retenu pour la composante.
FPT_ITT.1	Basic internal TSF data transfer protection			Non retenu pour la composante.
FPT_RPL.1	Replay detection			Non retenu pour la composante.
FPT_STM.1	Reliable time stamps			Non retenu pour la composante.
FPT_TDC.1	Inter-TSF basic TSF data consistency	Aucune	Oui	
FTA_LSA.1	Limitation on scope of selectable attributes			Non retenu pour la composante.
FTA_SSL.1	TSF-initiated session locking			Non retenu pour la composante.
FTA_SSL.2	User-initiated locking			Non retenu pour la composante.
FTA_SSL.3	TSF-initiated termination			Non retenu pour la composante.
FTA_SSL.4	User-initiated termination			Non retenu pour la composante.
FTA_TSE.1	TOE session establishment			Non retenu pour la composante.
FTP_ITC.1	Inter-TSF trusted channel			Non retenu pour la composante.
FTP_TRP.1	Trusted path			Non retenu pour la composante.

7 ANNEXE A : COMPLEMENTS DE DESCRIPTION DE LA TOE ET DE SON ENVIRONNEMENT

7.1 Eléments exclus du périmètre de la TOE

Seuls les logiciels précisés au paragraphe **Erreur ! Source du renvoi introuvable.** ci-dessus (Trust.Center®, K .Registration® et KeySeed®) font partie du périmètre de la TOE. Outre les logiciels non mentionnés ci-avant, sont exclus du périmètre de la TOE les éléments suivants :

- Les machines hôtes des composants logiciels et leurs interfaces ;
- Les protocoles d'interconnexion listés au § 3.3. Seule la capacité de la TOE (interfaçage avec les bons paramètres) à établir une communication à l'aide de ces protocoles sera étudiée ;
- Les services cryptographiques utilisés par les différents composants de la TOE. Les services cryptographiques de la TOE font l'objet d'une cotation cryptographique. Les HSM qui mettent en œuvre des clés privées d'AC peuvent faire l'objet d'une cotation cryptographique ;
- Les environnements logiciels utilisés pour mettre en œuvre les modules et les composants logiciels ;
- Les systèmes d'exploitation des modules logiciels ;
- Les stations de travail des administrateurs systèmes qui sont des portables connectées en mode terminal ou depuis une salle d'administration en utilisant une connexion SSH sécurisée à l'aide d'un certificat numérique.

Ces éléments ne mettent pas en œuvre des fonctions de sécurité de la TOE. Toutefois, ils concourent à la sécurité environnementale de la TOE.

7.2 Architectures matérielles de la TOE

Ce paragraphe décrit l'ensemble des architectures système physiques pour lesquelles la TOE est évaluée. Quelque soient la configuration de l'architecture matérielle, les communications entre la composantes K.Registration® et la composante Trust.Center® s'effectuent par les services web de chacune de ses composantes (SW - K.Registration® et SW - Trust.Center®).

7.2.1 Architecture matérielle 1

Dans la description ci-dessous des architectures matérielles, les DMZ et les CZ peuvent être mutualisées ou dédiées.

7.2.1.1 Trust.Center®

Le Trust.Center® se présente sous la forme d'un rack contenant :

- 1 serveurs qui hébergent le SW - Trust.Center® ;
- 1 serveur qui héberge le SA - Trust.Center® ;
- 1 serveur qui héberge le service de base de données ;
- 1 serveur qui héberge le service cryptographique (HSS) qui est relié à une ressource cryptographique ;
- 2 firewalls matériels qui permettent des séparations pour créer une DMZ Frontale ;
- Une ressource cryptographique reliée au serveur qui héberge le service cryptographique, qui protège les clés d'AC et signe les certificats et les CRL.

Trust.Center® doit être relié à un réseau pour pouvoir dialoguer avec K.Registration®, effectuer les réplications d'annuaire avec les annuaires permanents des Clients ou des envois de fichier LDIF, envoyer des mails de notification et permettre l'établissement des connexions avec les opérateurs distants qui ont des rôles de confiance sur Trust.Center®.

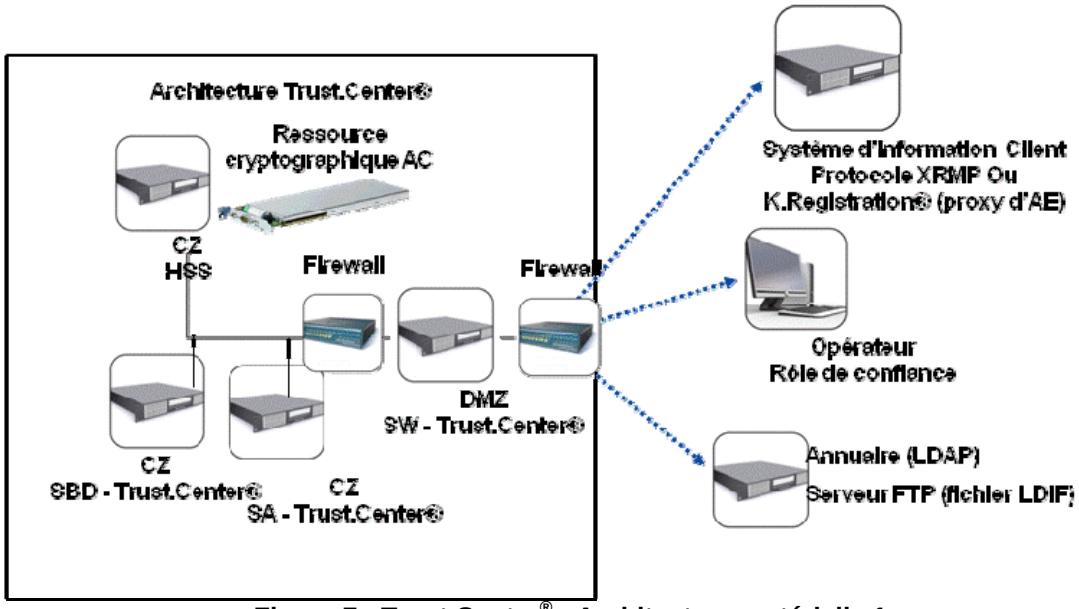


Figure 7 : Trust.Center® - Architecture matérielle 1

7.2.1.2 K.Registration®

K.Registration® se présente sous la forme d'un rack contenant :

- 1 serveurs qui hébergent le SW - K.Registration® ;
- 1 serveur qui héberge le SA - K.Registration® ;
- 1 serveur qui héberge le service de base de données ;
- 2 firewalls matériels ou logiciels qui permettent des séparations pour créer une DMZ Frontale ;
- Un module cryptographique logiciel ou une ressource cryptographique matérielle reliée au serveur qui héberge le proxy d'AE.

K.Registration® doit être relié à un réseau pour pouvoir dialoguer avec Trust.Center®, envoyer des mails de notification et permettre l'établissement des connexions avec les opérateurs distant qui ont des rôles de confiance sur K.Registration®.

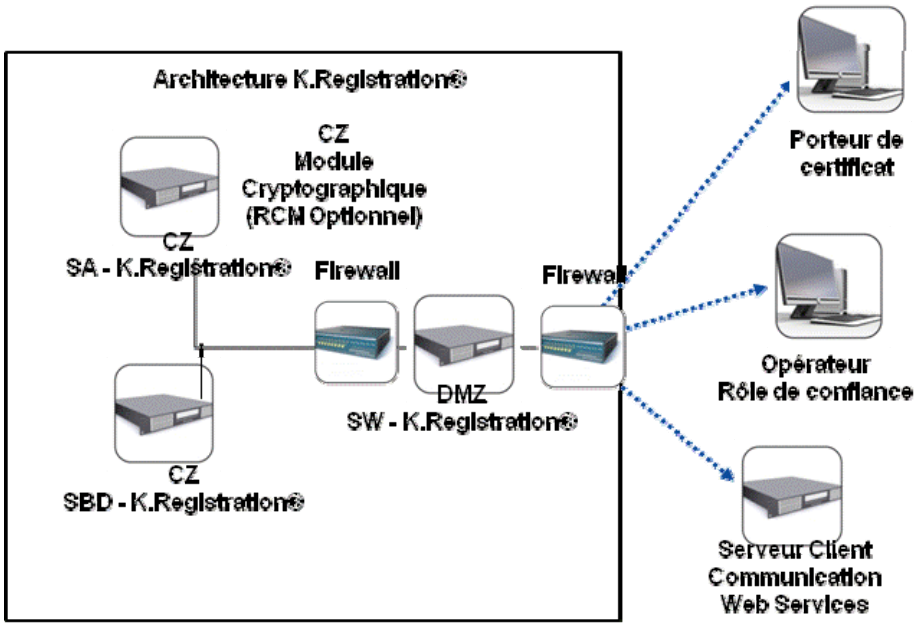


Figure 8 : K.Registration® - Architecture matérielle 1

7.2.1.3 KeySeed®

KeySeed® se présente sous la forme d'un poste informatique avec un système d'exploitation Microsoft de type Windows, ou autre de type LINUX. Le poste informatique est hors-ligne c'est-à-dire sans capacité de connexion au réseau informatique.

Figure 9 : KeySeed® - Architecture matérielle 1

7.2.2 Architecture matérielle 2

L'architecture matérielle est composée de la manière suivante :

- 1 serveur Trust.Center® qui héberge le SA - Trust.Center®, le SA - K.Registration® le HSS et le service de base de données du Trust.Center® ;
- Une ressource cryptographique reliée au serveur qui héberge le service cryptographique, qui protège les clés d'AC et signe les certificats et les CRL ;
- 1 serveur qui héberge l'ensemble des services web du Trust.Center® et de K.Registration® ;
- 1 serveur chez le Client qui communique avec le SA - Trust.Center® (en passant par le SW - Trust.Center®) avec le protocole XRMP;
- 1 ou 2 Firewall matériel(s) ou logiciel(s).

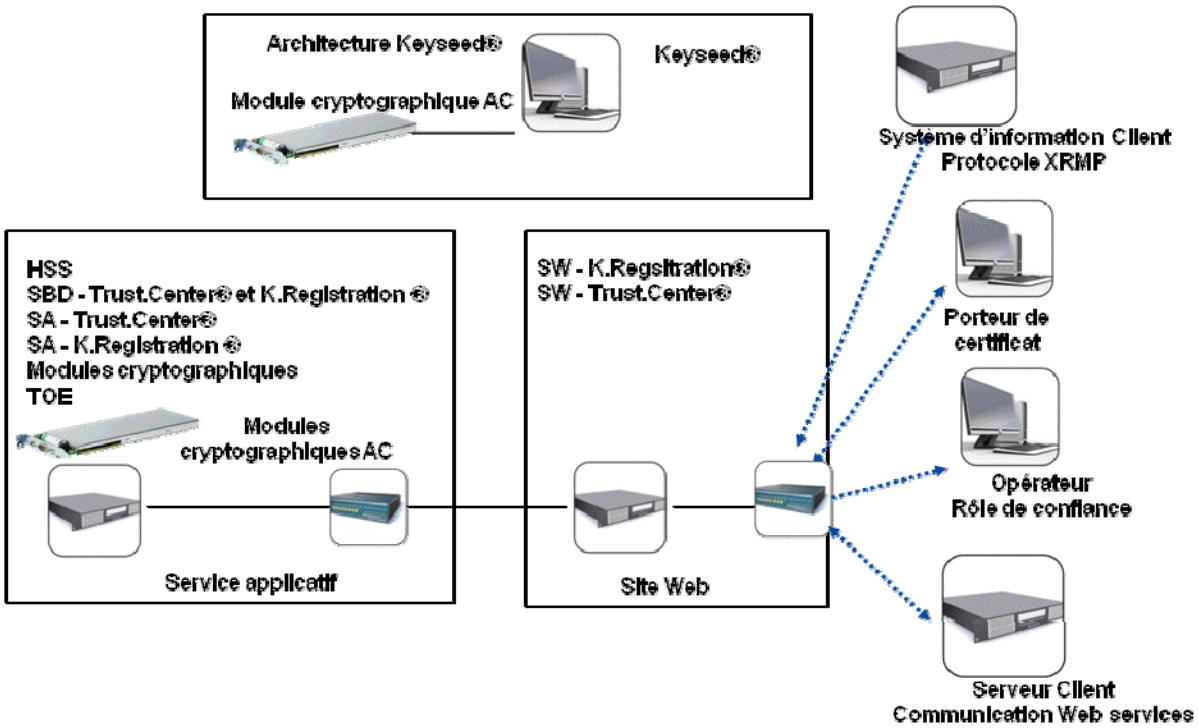
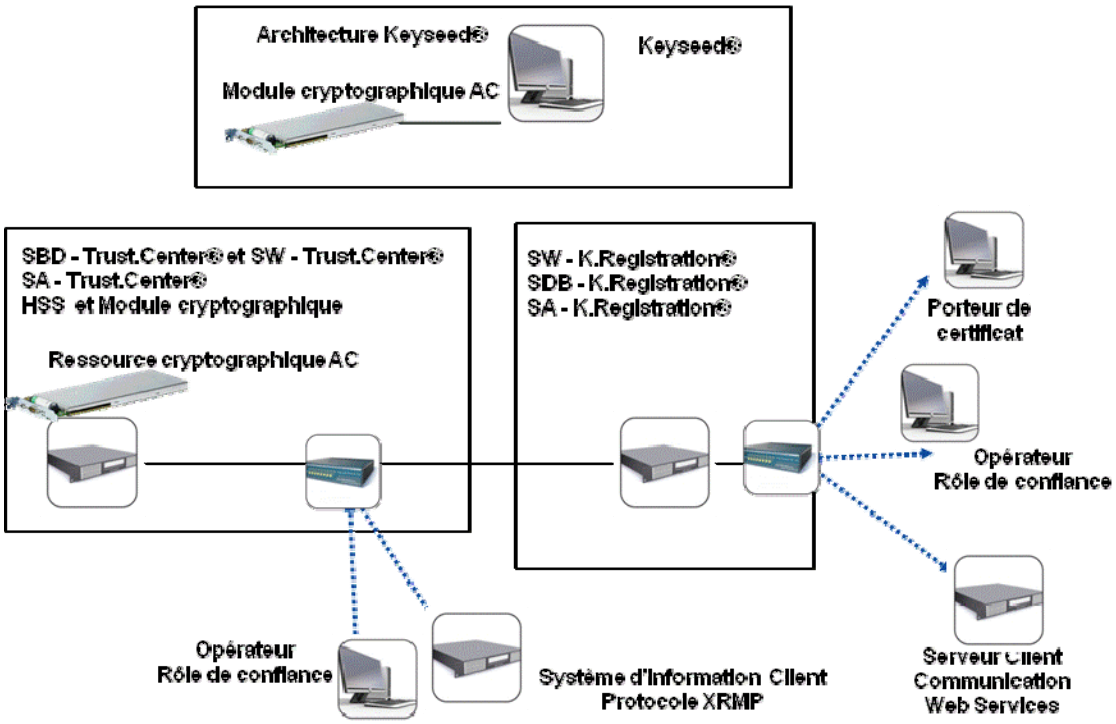


Figure 11 : Trust.Center®/K.Registration® - Architecture matérielle 2

7.2.3 Architecture matérielle et logiciel retenue pour l'évaluation certification

Le schéma ci-dessous représente l'environnement d'évaluation :



7.2.3.1 Keyseed®

7.2.3.1.1 Matériel

L'application Keyseed® est installée sur un ordinateur fixe :

- DELL VOSTRO 200
- Processeur Intel® Core™ 2 Duo CPU E4400 2.00 GHz
- 2 Go RAM Dual Channel DDR2 667MHz
- 250Go
- Lecteur Graveur DVD/DVRW

7.2.3.1.2 Logiciel : système d'exploitation

Microsoft Windows XP Professionnel Version 2002 Service Pack 3.

7.2.3.2 K.Registration®

7.2.3.2.1 Matériel

L'ensemble des composants K.Registration® est installé sur un serveur :

- HP PROLIANT DL 380 G5 Xeon E5430
- 8Go FB-DIMM ECC DDR2 PC2-5300
- Disques SAS 146,8Go 10Ktpm SFF HPL
- Lecteur/Graveur DVD+RW slimline
- Kit d'évolution PCI-X DL380 G5
- Alimentation redondé hot plug IEC 380 G5

7.2.3.2.2 Logiciel : système d'exploitation

RedHat Enterprise Linux 5 Update 3 (Default Install)

7.2.3.2.3 Logiciel : SW – K.Registration®

Logiciel	Version
apache	httpd-2.2.3-22.el5
mod_ssl	mod_ssl-2.2.3-22.el5
openSSL	0.9.8l (patch sur version openssl-0.9.8e-7.el5)
mod_jk (connecteur Apache / Jboss)	ks-mod_jk22-1.2.28-FCS

7.2.3.2.4 Logiciel : SA – K.Registration® et Proxy d'AE

Logiciel	Version
Java JDK	jdk-1.5.0_11-fcs

Les bibliothèques utilisées sont : Sequoai.security v 2.4.0 et bouncycastle (Java) v 1.43.

7.2.3.2.5 Logiciel : SDB – K.Registration®

Logiciel	Version
Oracle 11g	11.1.0.6.0 – Release 1 Installation via CD

7.2.3.3 Trust.Center®

7.2.3.3.1 Matériel

L'ensemble des composants Trust.Center® est installé sur un serveur :

- HP PROLIANT DL 380 G5 Xeon E5430
- 8Go FB-DIMM ECC DDR2 PC2-5300
- Disques SAS 146,8Go 10Ktpm SFF HPL
- Lecteur/Graveur DVD+RW slimline
- Kit d'évolution PCI-X DL380 G5
- Alimentation redondé hot plug IEC 380 G5

7.2.3.3.2 Logiciel : système d'exploitation

RedHat Enterprise Linux 5 Update 3 (Default Install)

7.2.3.3.3 Logiciel : SW – Trust.Center®

Logiciel	Version
apache	httpd-2.2.3-22.el5
mod_ssl	mod_ssl-2.2.3-22.el5
openSSL	0.9.8l (patch sur version openssl-0.9.8e-7.el5)
mod_jk (connecteur Apache / Jboss)	ks-mod_jk22-1.2.28-FCS

7.2.3.3.4 Logiciel : SA – Trust.Center® et Serveur cryptographique (HSS)

Logiciel	Version
Java JDK	jdk-1.5.0_11-fcs
Driver Bull TrustWay for Linux	1.01.01011008

Les bibliothèques utilisées sont : Sequoai.security v 2.4.0 et bouncycastle (Java) v 1.43.

7.2.3.3.5 Logiciel : SDB – Trust.Center®

Logiciel	Version
Oracle 11g	11.1.0.6.0 – Release 1 Installation via CD

7.2.3.4 Poste infomatique : Rôle de confiance et Porteur

7.2.3.4.1 Matériel

Un ordinateur fixe :

- DELL VOSTRO 200
- Processeur Intel® Core™ 2 Duo CPU E4400 2.00 GHz
- 2 Go RAM Dual Channel DDR2 667MHz
- 250Go
- Lecteur Graveur DVD/DVRW

7.2.3.4.2 Logiciel : système d'exploitation

Logiciel	Version
Mozilla Firefox	3.6

Microsoft Windows XP Professionnel Version 2002 Service Pack 3.

7.3 Environnement d'utilisation

7.3.1 K.Registration®

7.3.1.1 SW - K.Registration®

Les types de machines utilisées pour la mise en œuvre du SW - K.Registration® sont les machines suivantes :

Matériel	Description	Version Minimale
Serveur Sun	Serveur matériel	v240 ou T2000
Serveur HP	serveur matériel	ProLiant DL380 G5 ou DL360 G6

La ou les machines faisant tourner le frontal web doi(ven)t disposer des composants logiciels suivants :

Logiciel	Version recommandée
apache	httpd-2.2.3-22.el5
mod_ssl	mod_ssl-2.2.3-22.el5
openSSL	0.9.8l
mod_jk (connecteur Apache / Jboss)	ks-mod_jk22-1.2.28-FCS

7.3.1.2 SA - K.Registration® et proxy d' AE

Les types de machines utilisées pour la mise en œuvre du SA - K.Registration® et le proxy d'AE sont les suivantes :

Matériel	Description	Version Minimale
Serveur Sun	Serveur matériel	v240 ou T2000
Serveur HP	serveur matériel	ProLiant DL380 G5 ou DL360 G6

La ou les machines faisant tourner le serveur d'application doi(ven)t disposer des composants logiciels suivants :

Logiciel	Version recommandée
Java JDK	jdk-1.5.0_11-fcs

Utilisé uniquement pour l'installation et pas l'utilisation du logiciel service web.

SBD - K.Registration®

Les types de machines utilisées pour la mise en œuvre du SBD - K.Registration® sont les machines suivantes :

Matériel	Description	Version Minimale
Serveur Sun	Serveur matériel	v240 ou T2000
Serveur HP	serveur matériel	ProLiant DL380 G5 ou DL360 G6

La ou les machines faisant tourner le SGBD doi(ven)t disposer des composants logiciels suivants :

Logiciel	Description	Version Recommandée
Oracle	SBD, y compris client en ligne de commande sqlplus pour l'exécution de script sql lors de l'installation	11g
Linux RedHat	Système d'exploitation pour HP	ES5
Solaris	Système d'exploitation pour Sun	10

Il n'existe pas de contrainte sur le système d'exploitation du SBD.

7.3.1.3 Service cryptographique proxy d'AE

Les bibliothèques utilisées sont : Sequoai.security v 2.4.0 et bouncycastle (Java) v 1.43

7.3.1.4 Service cryptographique SA – K.Registration®

Les bibliothèques utilisées sont : Sequoai.security v 2.4.0 et bouncycastle (Java) v 1.43.

7.3.2 Trust.Center®

7.3.2.1 SW - Trust.Center®

Les types de machines utilisées pour la mise en œuvre du SW - ® sont les machines suivantes :

Matériel	Description	Version Minimale
Serveur Sun	Serveur matériel	v240 ou T2000
Serveur HP	serveur matériel	ProLiant DL380

		G5 ou DL360 G6

La ou les machines faisant tourner le frontal web doi(ven)t disposer des composants logiciels suivants :

Logiciel	Version recommandée
apache	httpd-2.2.3-22.el5
mod_ssl	mod_ssl-2.2.3-22.el5
openSSL	0.9.8l
mod_jk (connecteur Apache / Jboss)	ks-mod_jk22-1.2.28-FCS

7.3.2.2 SA - Trust.Center®

Les types de machines utilisées pour la mise en œuvre du SW - ® sont les machines suivantes :

Matériel	Description	Version Minimale
Serveur Sun	Serveur matériel	v240 ou T2000
Serveur HP	serveur matériel	ProLiant DL380 G5 ou DL360 G6

La ou les machines faisant tourner le serveur d'application doi(ven)t disposer des composants logiciels suivants :

Logiciel	Version
Java JDK	jdk-1.5.0_11-fcs

Utilisé uniquement pour l'installation et pas l'utilisation du logiciel service web.

SBD - Trust.Center®

Les types de machines utilisées pour la mise en œuvre du SW - K.Registration® sont les machines suivantes :

Matériel	Description	Version Minimale
Serveur Sun	Serveur matériel	v240 ou T2000
Serveur HP	serveur matériel	ProLiant DL380 G5 ou DL360 G6

La ou les machines faisant tourner le SGBD doi(ven)t disposer des composants logiciels suivants :

Logiciel	Description	Version Recommandée
Oracle	SBD, y compris client en ligne de commande sqlplus pour l'exécution de script sql lors de l'installation	11g
Linux RedHat	Système d'exploitation pour HP	ES 5
Solaris	Système d'exploitation pour Sun	10

Il n'existe pas de contrainte sur le système d'exploitation du SBD.

7.3.2.3 HSS

Les types de machines utilisées pour la mise en œuvre du SW - K.Registration® sont les machines suivantes :

Matériel	Description	Version Minimale
Serveur Sun	Serveur matériel	v240 ou T2000
Serveur HP	serveur matériel	ProLiant DL380 G5 ou DL360 G6

La ou les machines faisant tourner le HSS doi(ven)t disposer des composants logiciels suivants :

Logiciel	Description	Version Recommandée
Linux RedHat	Système d'exploitation pour HP	ES 5
Solaris	Système d'exploitation pour Sun	10

Il n'existe pas de contrainte sur le système d'exploitation du SBD.

7.3.2.4 Service cryptographique HSS

Les bibliothèques utilisées sont : Sequoai.security v 2.4.0 et bouncycastle (Java) v 1.43.

Logiciel	Version
Java JDK	jdk-1.5.0_11-fcs

7.3.2.5 Service cryptographique SA – Trust.Center®

Les bibliothèques utilisées sont : Sequoai.security v 2.4.0 et bouncycastle (Java) v 1.43.

7.3.3 KeySeed®

Les machines et logiciels supports sont les suivantes :

- Station de travail opérateur :
  - Matériel : station de travail de type PC ;
  - Logiciel : système d'exploitation Microsoft (Windows 2000, recommandé XP Professionnel Version 2002 Service Pack 3) ou Linux et lecteur de fichiers au format pdf.

7.3.4 Station de travail acteur de la TOE

Les stations de travail des acteurs sont les suivants :

- Station de travail opérateur :
  - Matériel : station de travail de type PC ;
  - Logiciel : système d'exploitation Microsoft (Windows 2000, recommandé XP Professionnel Version 2002 Service Pack 3), navigateur (Internet Explorer à partir de 7.0 ou Mozilla Firefox 3.6) ;

- Station de travail ingénieur système :
  - Matériel : station de travail de type PC ;
  - Logiciel : système d'exploitation Microsoft (Windows 2000, recommandé XP Professionnel Version 2002 Service Pack 3) ou Linux, navigateur (Internet Explorer à partir de 7.0 ou Mozilla Firefox 3.6) ;

7.3.5 Poste informatique du porteur de certificat

Les postes informatiques du porteur de certificat :

- Matériel : poste informatique bureautique ;
- Logiciel :
    - Navigateur et outil de messagerie : Lotus Notes Compatible PKCS#11 à partir de la version 6.5, Mozilla pour les versions 1.0 et supérieur, Outlook 2000 pour les versions Outlook 2000, 2002 et 2003, Outlook Express pour les versions 5 et supérieure ;
    - Système d'exploitation : Windows 2000, XP (Service Pack 3) et Vista.

7.3.6 Carte à puce

Les cartes à puces sont les suivantes :

- GemXPRESSO (TP IS v2) Gemalto ;
- Ypsid card sscd (Sagem Orga) ;
- TPC IMCY (Axalto) ;
-
- ActivCard (ActiveIdentity) ;
- AuthentIC V4 (Oberthur) ;
- ID One Cosmo (Oberthur) ;
- Instant EID IP2 Setec ;
-

7.3.7 HSM

Les modules cryptographiques sont les suivants

- Ressource matérielle :
    - Carte Trustwat ;
    - Luna SA, CA, SP et XP ;
    - Module cryptographique ANSSI (IGC/A) uniquement avec le composant KeySeed®.

7.4 Cycle de vie de la TOE

Le modèle de cycle de vie standard des Critères Communs suppose une séparation entre le développement des fonctions de sécurité et leur exploitation. KEYNECTIS met en œuvre ce principe en séparant les équipes de développement et d'exploitation des modules logiciels de la TOE.

Le cycle de vie de la TOE est résumé comme suit :

- Spécification : l'ensemble des modules logiciels fait l'objet de spécification avant d'être développés. Ces spécifications sont élaborées par KEYNECTIS et approuvées en interne KEYNECTIS ;
- Développement : l'ensemble des développements sont effectués et suivis en interne KEYNECTIS. Certains composants logiciels sont récupérés et sont modifiés selon les besoins fonctionnels ;
- Test / qualification : l'ensemble des composants logiciels est testé au moins sur le plan fonctionnel ;
- Livraison : les livraisons de tout ou partie de la TOE sont effectuées et encadrées selon des procédures de KEYNECTIS, qu'elles soient internes ou externes ;
- Intégration : l'intégration de tout ou partie de la TOE est effectuée par les équipes de KEYNECTIS et selon des procédures fournies par KEYNECTIS.

8 ANNEXE B : DEFINITION ET ACRONYMES

8.1 Acronymes

AC	Autorité de Certification
ACR	Autorité de Certification Racine
AE	Autorité d'Enregistrement
AEL	Autorité d'Enregistrement Locale
CZ	Certified Zone
ANSSI	Agence Nationnale de la Sécurité des Systèmes d'Information

DMZ	Dematerialized zone
DPC	Déclaration des Pratiques de Certification
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés
ISO	International Organization for Standardization
LAR	Liste des certificats d'AC Révoqués
LCR	Liste de Certificats Révoqués
OC	Opérateur de Certification
OID	Object Identifier
PC	Politique de Certification
PP	Profil de Protection
PSCO	Prestataire de Service de Confiance
RSA	Rivest Shamir Adelman
SHA-1	Secure Hash Algorithm version 1
SI	Système d'Information
SP	Service de Publication
UC	Utilisateur de Certificats
UF	Utilisateur Final
URL	Uniform Resource Locator

8.2 Définitions

Application : Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat.

Autorité de Certification (AC) : « Autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer les certificats. Cette autorité peut, facultativement, créer les clés d'utilisateur » [9594-8]. Elle s'appuie pour cela sur une Infrastructure de Gestion de Clés.

Autorité de Certification Racine (ACR) : AC prise comme référence par une communauté d'utilisateurs (incluant d'autres AC). Elle est un élément essentiel de la confiance qui peut lui être accordée dans un contexte donné.

Autorité d'Enregistrement (AE) : C'est une entité (personne ou machine) d'IGC utilisée pour la gestion des offres de certification. L'administration et la mise en œuvre de l'AE repose sur des rôles de confiance. L'AE réalise les demandes de certificats et de révocation auprès du centre de certification.

Autorité d'Enregistrement Locale (AEL) : C'est une entité (personne ou machine) de l'IGC utilisée pour la mise en œuvre des offres de certification gérée par l'AE. L'AEL est une personne physique qui possède un certificat délivré par une IGC afin de s'authentifier sur l'AE sur laquelle elle possède un rôle de confiance qui lui permet de mettre en œuvre une fonction de l'AE sur une offre de certification. C'est l'AEL qui enregistre et prépare les demandes de certificat des porteurs de certificat. Elle réalise les formalités nécessaires (rapport facial si exigé, vérification des pièces justificatives, …) entre le porteur de certificat et le PSCO afin de lui délivrer un certificat électronique.

Bi-clé cryptographique : Une bi-clé est un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptologie basée sur des algorithmes asymétriques. Quatre types de bi-clés interviennent dans une infrastructure de gestion de clés :

- Les bi-clés d'intégrité, dont la clé privée est utilisée à des fins de contrôle d'accès, de non répudiation et de signature et la clé publique à des fins de vérification ;
- les bi-clés de certification, nécessaires au fonctionnement d'une IGC ;
- les bi-clés de confidentialité, grâce auxquels des messages ou des données peuvent être protégés en confidentialité ;
- les bi-clés d'échange de clés qui permettent de transporter les clés (symétriques ou asymétriques).

Trust.Center® : composant d'IGC utilisée pour la gestion des AC, des certificats et des CRL au sein de domaine de confiance. L'administration et la mise en oeuvre de Trust.Center® repose sur des rôles de

confiance. Trust.Center® utilise un module cryptographique matériel (ressource cryptographique) afin de réaliser les opérations cryptographiques nécessaires à la gestion des certificats. Trust.Center® traite les demandes de certificats et de révocations émises par l'AE ou des rôles de confiance de Trust.Center®.

Cérémonie des clés : cérémonie au cours de laquelle une ou plusieurs bi-clés cryptographiques sont générées dans un module cryptographique sous le contrôle de plusieurs personnes qui détiennent les données d'activations nécessaires.

Certificat électronique : Clé publique d'un utilisateur, ainsi que certaines autres informations rendues infalsifiables par chiffrement avec la clé privée d'une autorité de certification (AC) qui l'a délivré [9594-8].
Un certificat contient des informations telles que :

- l'identité du porteur de certificat,
- la clé publique du porteur de certificat,
- la durée de vie du certificat,
- l'identité de l'autorité de certification qui l'a émis,
- la signature de l'AC qui l'a émis.

Un format standard de certificat est normalisé dans la recommandation X509 v3.

Certificat auto-signé : Certificat électronique d'une AC signé par cette même AC. Ce certificat a la particularité d'avoir le contenu de l'information « identité du porteur de certificat » identique à celle du champ « identité de l'AC qui l'a émis ».

Chemin de certification : Ensemble de certificats électroniques liés entre eux par les identités q'ils comportent et par l'identité d'un certificat auto-signé et qui sont nécessaires à la validation d'un certificat électronique.

Composant d'IGC : Plate-forme opérée par une entité (AC, AE) et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC. L'entité peut être le PSCO lui-même ou une entité externe liée au PSCO par voie contractuelle, réglementaire ou hiérarchique.

Données d'activation : Des valeurs de données, autres que des clés, qui sont nécessaires pour exploiter les modules cryptographiques ou les éléments qu'ils protègent et qui doivent être protégées (par ex. un NIP, une phrase secrète, une clé partagée manuelle).

Déclaration des Pratiques de Certification : Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Domaine de confiance : Un domaine de confiance regroupe une ou plusieurs AC, organismes reconnus compétents et de confiance pour délivrer des certificats et en assurer la validité. Les domaines de confiances sont créés et gérés au niveau du Centre de Certification. Il existe par défaut dans le Trust.Center® deux domaines dédiés à la gestion des rôles de confiance de Trust.Center®, un domaine complémentaire est généré pour la certification des porteurs de certificats. L'ajout d'autres domaines correspond à un cloisonnement souhaité pour l'administration et la mise en œuvre d'AC. Les fonctionnalités d'un domaine de confiance permettent de garantir l'unicité du champ « subject » des certificats signés par une AC donnée. De même, un domaine de confiance permet de garantir le contenu et le format des certificats des porteurs de certificats, des rôles de confiance et d'AC ainsi que des LCR générés par une ou des AC identifiées.

Infrastructure de Gestion de Clés : Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des applications. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Liste de Certificat Révoqués (LCR ou CRL) : Liste contenant les identifiants des certificats révoqués ou invalides. Lors d'une révocation, l'AC ajoute l'identifiant du certificat à révoquer dans la CRL, la signe et la transmet au service de publication. Il appartient au système d'inspection des titres qui souhaite connaître l'état d'un certificat de vérifier la présence de l'identifiant correspondant dans la liste. Quand il s'agit de liste de révocation pour des AC, le terme Liste des Autorités Révoquées (LAR) est utilisé.

Module cryptographique : Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions cryptographiques et l'utilisation de bi-clés cryptographiques. Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité utilisés par les composantes de l'IGC. Dans le cadre du présent document, lorsqu'un module cryptographique est matériel alors il est appelé ressource cryptographique.

Offre de certification : L'offre de certification recouvre dans K.Registration® l'ensemble du processus de remise d'un certificat à un utilisateur. L'offre inclut à la fois le profil du certificat qui sera délivré à l'utilisateur final, mais aussi le paramétrage des différentes étapes nécessaires à la gestion de la demande en elle même (rôles de confiance, droits nécessaire pour les actions de gestion au sein de l'offre, actions au sein d'une offre, états des actions, enchaînements, notification des actions, ...). L'offre est le point d'articulation de l'ensemble des fonctions de K.Registration®, sur lequel viennent s'authentifier des opérateurs possédant des rôles de confiance avec des droits spécifiques sur ces fonctions.

Politique de certification : Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Politique de sécurité: ensemble de règles édictées par une autorité de sécurité et relatives à l'utilisation, la fourniture de services et d'installations de sécurité [ISO/IEC 9594-8; ITU-T X.509].

Porteur de certificat : Toute personne physique ou morale, organisme administratif ou système informatique matériel et logiciel qui détient un certificat et un bi-clé associé délivré par une AC afin d'accéder à une application conformément à la politique de sécurité de cette application et à la politique de sécurité édictée par l'AA.

Porteurs de secret (ou porteur de données d'activation) : Porteurs de données d'activation (parfois appelées parts de secret) auxquels les éléments d'activation des ressources cryptographiques et des clés qu'elles supportent sont confiés. Ils en assurent la protection ainsi que la disponibilité.

Prestataire de services de confiance (PSCO) : Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCO peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCO comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCO peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCO peut être identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat. Le PSCO met en œuvre plusieurs PC à l'aide de Trust.Center® (gestion des domaines de confiance) et de K.Registration® (gestion des offres de certification) au profit de promoteur d'application.

Promoteur d'application - Ce terme générique désigne un organisme qui est met en œuvre une application (Banques, Entreprise, Administrations de l'Etat, Collectivités territoriales, Organismes gérant des régimes de protection sociale, …). Le promoteur d'application définit les politiques de certification et la politique de sécurité de l'application avec laquelle un porteur de certificat interagit à l'aide de certificat électronique.

Rôle de confiance : Ceux sont des opérateurs qui sont authentifiés sur une composante d'IGC à l'aide de certificats délivrés par une AC technique. Ils sont utilisés pour administrer, opérer ou auditer la composante d'IGC.

Utilisateur de certificat (UC) : Application, personne physique ou morale, organisme administratif ou système informatique matériel et/ou logiciel qui utilise un certificat électronique d'un porteur de certificat afin de valider les fonctions de sécurité mises en œuvre à l'aide des certificats (signature, chiffrement et authentification). Pour valider un certificat, un UC utilise une ou des LCR ou un service d'information sur l'état des certificats (OCSP).

9 ANNEXE C : REFERENCES

Ref.	Document
[AUTH]	Référentiel Général de Sécurité, Annexe B3. Authentification : Règles et recommandations concernant les mécanismes d'authentification, version 1.0 du 13 janvier 2010.
[CC]	Common Criteria for Information Technology Security Evaluation version 3.1.: Part 1:, Introduction and general model, ref. CCMB-2006-09-001 rev. 1, September 2006, Part 2: Security functional requirements, ref. CCMB-2007-09-002 rev. 2, September 2007, Part 3: Security assurance requirements, ref. CCMB-2007-09-003 rev. 2, September 2007
[CRYPT_STD]	Référentiel Général de Sécurité, Annexe B1. Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. Version 1.2 du 26 janvier 2010.
[CRYPT_GC]	Référentiel Général de Sécurité, Annexe B2. Gestion des clés cryptographiques, Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard – Version 1.10 du 24 octobre 2008
[QS]	Processus de qualification d'un produit de sécurité - niveau standard - version 1.1, ref. N° 549/SGDN/DCSSI/SDR, SGDN/DCSSI, 18/03/2008.
[OTAN]	NATO Public Key Infrastructure (NPKI) Certificate Policy (AC/322-(D2004)0024 du 05 avril 2004, § 6.2 Private Key protection.
[RSA]	RSA Laboratories. PKCS #1 v2.1: RSA Encryption Standard. June 2000.
[RFC3279]	IETF - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile
[3DES]	American National Standards Institute. ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of Operation. 1998
[SHA1]	FIPS 180-2: "Secure Hash Standard", United States of American, National Institute of Science and Technology, Federal Information Processing Standard (FIPS) 180-2, 1 August 2002
[SHA224]	FIPS 180-2: "Secure Hash Standard", United States of American, National Institute of Science and Technology, Federal Information Processing Standard (FIPS) 180-2, 1 August 2002
[SHA256]	FIPS 180-2: "Secure Hash Standard", United States of American, National Institute of Science and Technology, Federal Information Processing Standard (FIPS) 180-2, 1 August 2002
[SHA384]	FIPS 180-2: "Secure Hash Standard", United States of American, National Institute of Science and Technology, Federal Information Processing Standard (FIPS) 180-2, 1 August 2002
[SHA512]	FIPS 180-2: "Secure Hash Standard", United States of American, National Institute of Science and Technology, Federal Information Processing Standard (FIPS) 180-2, 1 August 2002
[EBIOS v2]	Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) – SGDN/DSCSSI (2004).
[PP_AC]	Profil de protection, Autorité de Certification, PP_AC, 01/03/2000, version, 2.6
[PP_AE]	Profil de protection, Autorité d'Enregistrement, PP_AE, 01/03/2000, version, 2.6
[PP_IGC]	Profil de protection, Infrastructure de Gestion de Clés, PP_IGC, 01/03/2000, version, 2.6
[PP_CIMC]	Certificate Issuing and Management Components Family of Protection Profiles, Version 1.0, October 31, 2001
[RGS]	Référentiel Général de Sécurité, Version 1.0 du 6 mai 2010
[XRMP]	Xml Request Management Protocol, version 2.0, KEYNECTIS (2005)