PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2007/21

DICTAO VALIDATION SERVER (DVS) version 4.0.6

Paris, le 24 octobre 2007

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

Avertissement

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

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

Toute correspondance relative à ce rapport doit être adressée au :

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

certification.dcssi@sgdn.pm.gouv.fr

Référence du rapport de certification

DCSSI-2007/21

Nom du produit

DICTAO VALIDATION SERVER (DVS)

Référence/version du produit

Version 4.0.6

Conformité à un profil de protection

PP/nc0503 (« PP-MVSE »)

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 3 augmenté

ADV_LLD.1*, ADV_IMP.1*, ALC_FLR.3, ALC_TAT.1*, AVA_VLA.2

***appliqués aux exigences FCS**

Développeur(s)

Dictao

152, avenue de Malakoff

75116 Paris

Commanditaire

Dictao

152, avenue de Malakoff

75116 Paris

Centre d'évaluation

Oppida

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

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

Accords de reconnaissance applicables

CCRA **SOG-IS**

Préface

La certification

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

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

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

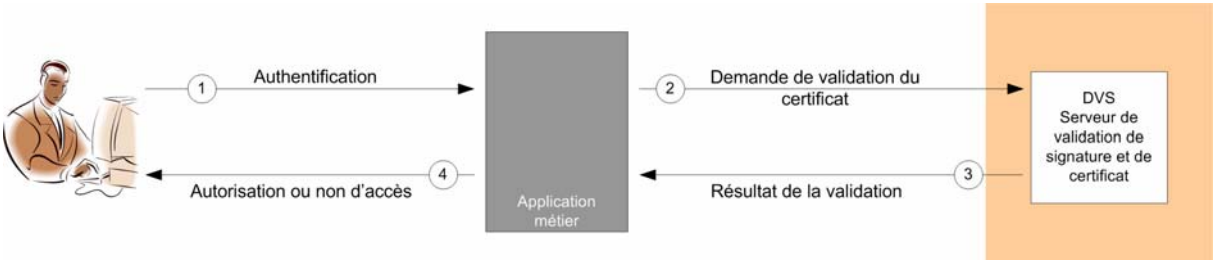
1.1. Présentation du produit

Le produit évalué est le serveur de vérification de signature électronique « **DICTAO VALIDATION SERVER (DVS), version 4.0.6 »** développé par Dictao.

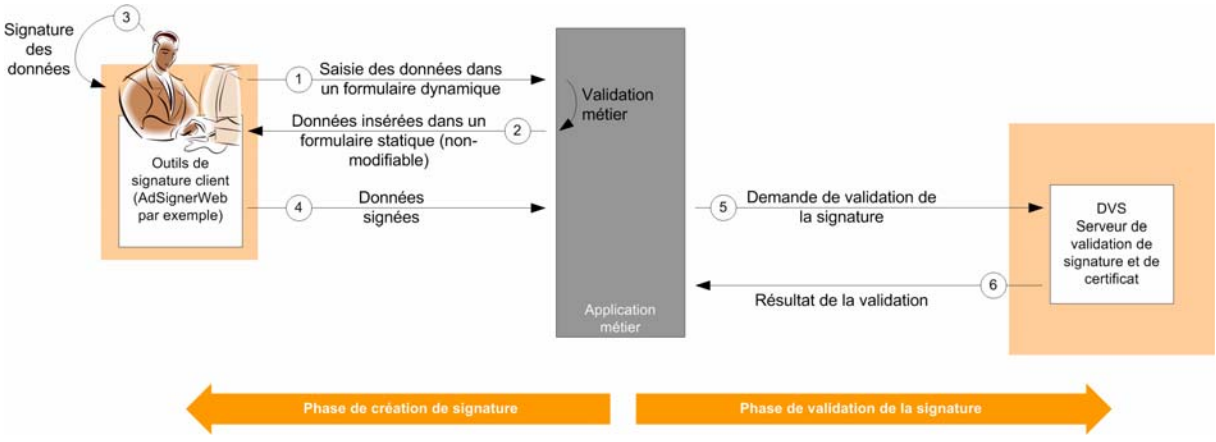
Ce serveur permet aux applications souhaitant intégrer des fonctionnalités de confiance telles que l'authentification par certificat ou la signature de documents électroniques, de déléguer toute la complexité du système de confiance à un service unique facilement configurable et qui saura répondre à la quasi-totalité des « cinématiques de confiance » des organisations.

DVS est un serveur de validation de certificats et de signatures électroniques multi-application supportant les standards de signature courants : PKCS #7, CMS, PDF, XML-DSig et XAdES.

Validation de certificat :



Vérification de signature électronique :



1.2. Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.
Cette cible de sécurité est conforme au profil de protection « Module de vérification de signature électronique » [PP]. Elle met en œuvre les modules de contrôle sémantique pour les formats « texte brut » et « html restreint » définis par Dictao.

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version 4.0.6 certifiée du produit DVS est identifiable sur le CD-ROM d'installation et via l'interface d'administration.
La configuration évaluée est le produit sans aucun « plugin » installé.

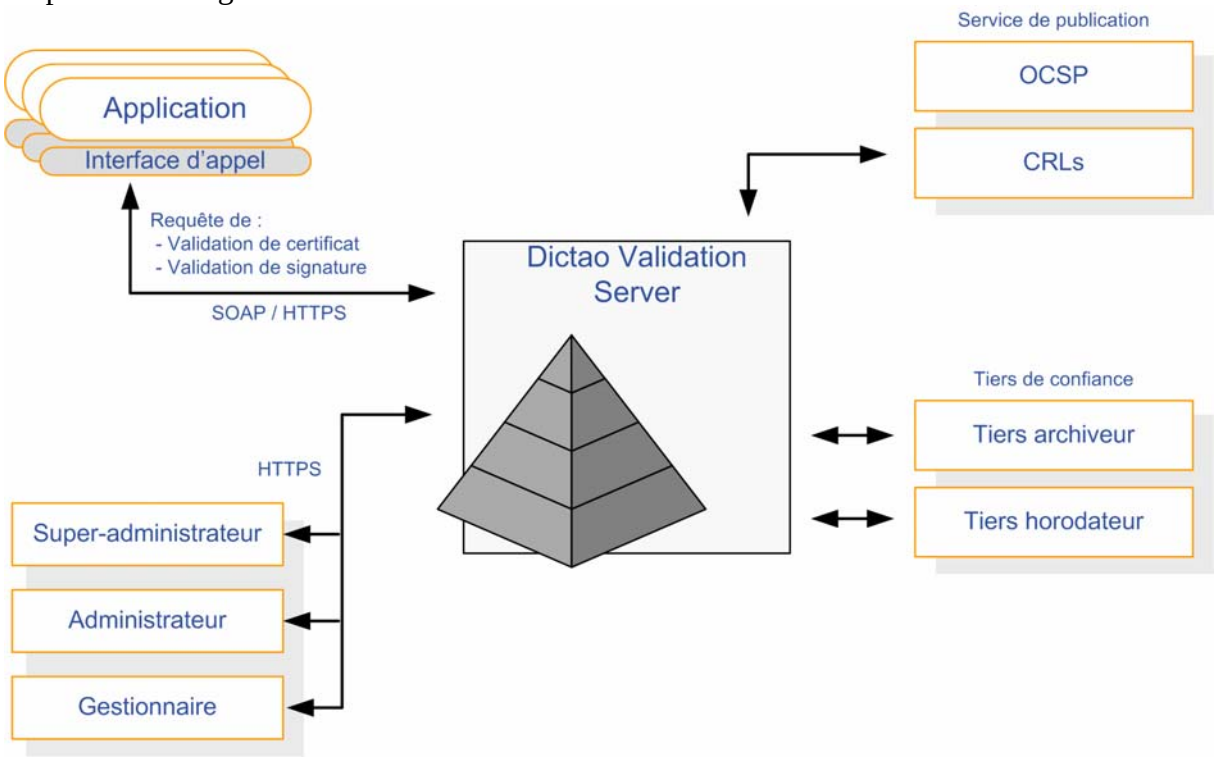
1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit DVS sont :

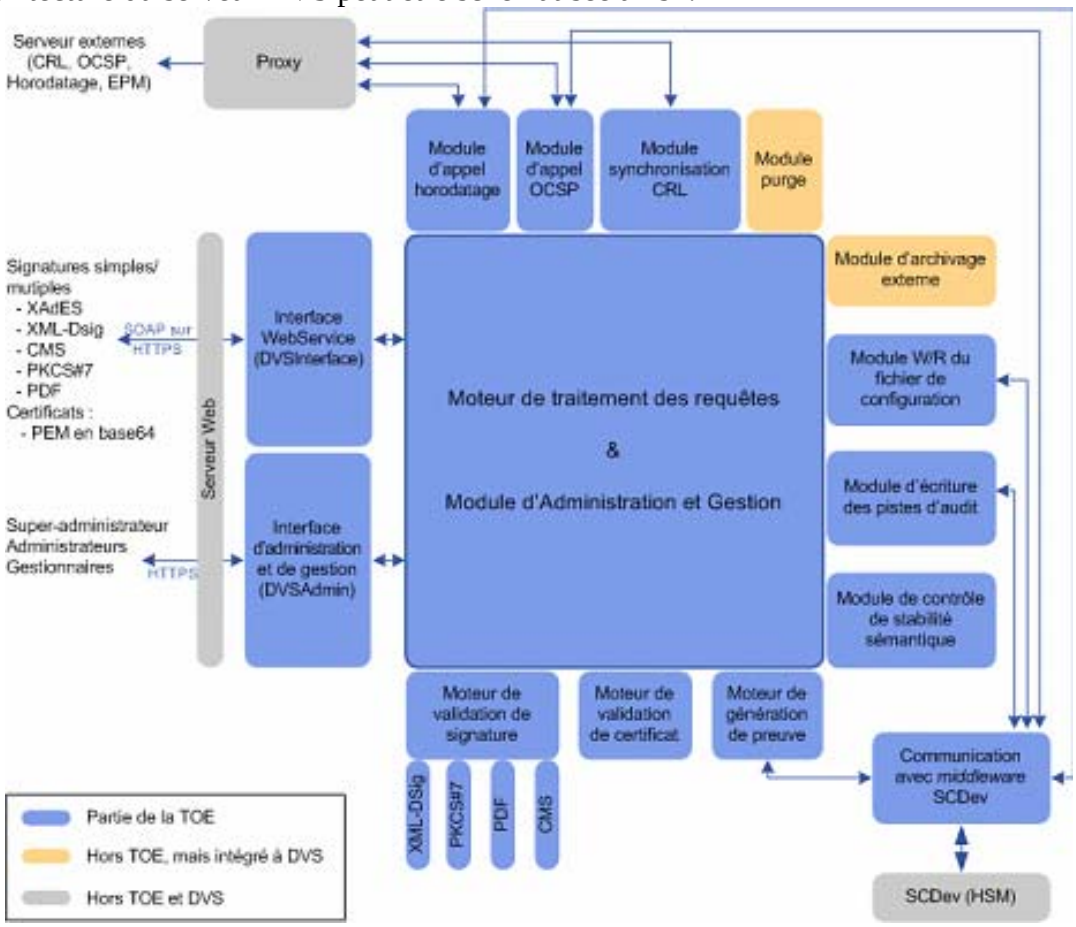
- la demande de validation de signature au serveur DVS au travers d'une interface d'appel de type Web Services (F.Validation_Signature) ;
- la demande de validation de certificat au serveur DVS au travers d'une interface d'appel de type Web Services (F.Validation_Certificat) ;
- la génération de traces d'audit pour des opérations sur le DVS (F.Generation_Audit)
- la récupération de preuves et la visualisation des données signées qu'elles contiennent, la consultation de transactions, la consultation de rapports d'activité (F.Gestionnaires et F.SuperGestionnaires) ;
- la gestion des groupes d'administration, la consultation des traces d'audit, la définition des ressources pour les administrateurs d'applications (F.SuperAdminstration) ;
- la gestion des utilisateurs au sein de leur groupe, le paramétrage des politiques de confiance mutualisées, l'ouverture du service à de nouvelles applications métier, la consultation des traces d'audit relatives à leurs groupes respectifs, la création de transactions pour une application donnée et l'association à chacune de ces transactions d'une politique de confiance (F.Administration).

1.2.3. Architecture

Le produit s'intègre dans l'environnement suivant :



L'architecture du serveur DVS peut être schématisée ainsi :



Le produit a été développé sur le site suivant :

Dictao

152, avenue de Malakoff
75116 Paris
France

Pour l'évaluation, l'évaluateur a considéré comme « administrateur du produit », les rôles administrateurs, super-administrateurs, gestionnaires et super-gestionnaires présentés dans la cible de sécurité [ST] et comme « utilisateur du produit », les applications appelantes s'interfaçant au serveur DVS. Les « guides d'utilisation » sont donc les guides de recommandations pour les développeurs, fournis par Dictao.

1.2.4. Configuration évaluée

Le produit a été évalué sur la configuration suivante :

- Station de travail de type SPARC,
- Système d'exploitation : Sun Solaris 10,
- Base de données : Oracle 10g,
- Serveur web : Apache 2.2,
- Serveur d'applications : Tomcat 5.0.28,
- Boîtier HSM : nCipher netShield (FIPS 140-2 Level-2).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].
Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par la DCSSI, ont été utilisées.

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 23 octobre 2007, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et donnent lieu aux conclusions suivantes :

L'utilisation des fonctions de hachage SHA-256, SHA-384, SHA-512 et l'utilisation du RSA avec des modules d'au moins 1536 bits atteignent le niveau *standard* défini dans le référentiel cryptographique de la DCSSI (cf. [REF-CRY]).

Le système utilise parfois la seule fonction de hachage SHA-1 pour des raisons d'interopérabilité dans certains environnements, ainsi que des modules RSA de 1024 bits. Cette fonction de hachage et l'utilisation de ces modules ne sont pas reconnues de niveau de robustesse standard.

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

3. La certification

3.1. Conclusion

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

Ce certificat atteste que le produit « DICTAO VALIDATION SERVER (DVS), version 4.0.6 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté.

3.2. Restrictions d'usage

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

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], il devra notamment suivre les recommandations rappelées ci-après.

1. Les administrateurs du produit devront s'assurer de l'authenticité de l'origine des politiques de signature avant qu'elles ne soient utilisées par le produit (cf. [ST] OE1.Authenticité_Origine_Politique_Signature).

2. La machine hôte sur laquelle le produit s'exécute devra être soit directement sous la responsabilité du vérificateur soit sous la responsabilité d'une personne morale ou physique qui lui garantit que les mesures de sécurité précisées dans la cible de sécurité [ST] sont bien appliquées (cf. [ST] OE2.Machine_Hôte).

3. La machine à partir de laquelle les administrateurs et les super-administrateurs accèdent aux fonctions d'administration devra être sous la responsabilité d'une personne morale ou physique qui lui garantit que les mesures de sécurité précisées dans la cible de sécurité [ST] sont bien appliquées (cf. [ST] OE3.Poste_(Super-)Administrateur).

4. La machine à partir de laquelle les gestionnaires ou les super-gestionnaires accèdent aux fonctions de gestion devra être sous la responsabilité d'une personne morale ou physique qui lui garantit que les mesures de sécurité précisées dans la cible de sécurité [ST] sont bien appliquées (cf. [ST] OE4.Poste_Gestionnaire).

5. Le système de vérification de signature dans lequel s'insère le produit doit posséder des applications de visualisation qui, soit retranscrivent fidèlement le document à vérifier, soit préviennent l'utilisateur des éventuels problèmes d'incompatibilité du dispositif de présentation avec le format du document. Les politiques de validation du

produit doivent définir, en fonction des formats supportés par celle-ci, des applications de référence pour la visualisation du document signé (cf. [ST] OE5.Présentation_Document).

6. L'administrateur du produit devra s'assurer de la cohérence entre les modules de visualisation, les modules de contrôle sémantique et les formats utilisés par le produit. Il devra paramétrer la liste des modules de référence conformément aux guides. L'identification des modules de visualisation dans cette liste devra préciser les contextes de visualisation. Les développeurs des applications appelantes devront implémenter les modules de visualisation de référence pour chaque format supporté. Il est recommandé de visualiser un document vérifié en mode texte dans un module de visualisation pour le mode texte, afin d'éviter l'interprétation de balises HTML qui pourraient s'y trouver.

7. L'environnement du produit devra fournir un module de contrôle capable de déterminer si la sémantique du document signé est invariante, instable ou non vérifiable. Ce module doit communiquer le statut de son analyse au produit (cf. [ST] OE.Contrôle_Sémantique_Document_Signé).

8. Les administrateurs et les super-administrateurs de sécurité du produit sont de confiance, formés à l'utilisation du produit et disposent des moyens nécessaires à la réalisation de leur activité (cf. [ST] OE6.(Super-)Administrateur_De_Sécurité_Sûr).

9. Les gestionnaires et super-gestionnaires du produit sont de confiance, formés à l'utilisation du produit et disposent des moyens nécessaires à la réalisation de leur activité (cf. [ST] OE7.Gestionnaire_Sûr).

10. L'application appelante est de confiance et doit être développée conformément aux recommandations se trouvant dans le guide de développement d'applications appelantes (cf. [ST] OE8.Application_Cliente_Sûre).

11. L'environnement du produit devra lui fournir les données de validation nécessaires à la vérification de la signature (cf. [ST] OE9.Fourniture_Des_Données_De_Validation).

12. L'environnement du produit devra fournir aux administrateurs de sécurité les moyens de contrôler l'intégrité des services du produit (cf. [ST] OE10.Intégrité_Services).

13. Les super-administrateurs de sécurité doivent analyser périodiquement les traces d'audit afin de s'assurer du bon fonctionnement du produit (cf. [ST] OE11.Analyse_Périodique_Journaux).

14. Les opérateurs d'hébergement doivent sauvegarder régulièrement les traces d'audit afin de prévenir toute saturation des disques de stockage (cf. [ST] OE12.Suppression_Périodique_journaux).

15. Les mots de passe ou autres moyens d'authentification des utilisateurs ((super-) administrateurs et gestionnaires) doivent être protégés par les utilisateurs de manière à répondre aux objectifs de sécurité du produit (cf. [ST] OE13.Protection_Moyens_Authentification).

16. L'activation et l'administration du boîtier cryptographique utilisé par le produit doivent être protégées à un niveau adéquat (cf. [ST] OE14.Protection_HSM).

17. Un module externe au produit doit permettre d'effectuer une authentification mutuelle entre le produit et les utilisateurs afin de se protéger contre l'usurpation d'identité (cf. [ST] OE15.Authentification_Mutuelle).

18. La clé privée utilisée pour la signature du fichier de configuration doit être protégée de manière adéquate (cf. [ST] OE16.Protection_Clé_Signature_Configuration).

19. Les communications entre le produit et les utilisateurs doivent être chiffrées par un module externe au produit, afin de protéger les communications en confidentialité. La protection doit être implémentée conformément aux recommandations de la DCSSI [CRYPT_STD] (cf. [ST] OE17.Protection_communications).

20. Les composants OCSP, IGC et serveurs d'horodatage auxquels le produit fait une requête doivent fournir des informations considérées fiables (cf. [ST] OE18.Services_Tiers_De_Confiance).

21. Le système d'exploitation et les composants principaux utilisés par le produit (ex : module d'archivage externe) doivent être soumis aux mêmes mesures de sécurité que la machine hôte du produit, précisées dans la cible de sécurité [ST].

22. Les serveurs Web qui utilisent le produit doivent être configurés de manière à ne pas utiliser d'algorithmes de chiffrement faible.

23. Il est recommandé de séparer les interfaces dédiées aux services de validation de celles dédiées aux services d'administration/gestion, afin de protéger le produit d'une tentative de saturation des services de validation.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

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

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

3.3.2. Reconnaissance internationale critères communs (CCRA)

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

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

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse.

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

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 3+	Intitulé du composant
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2		
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**3**	Authorisation controls
	ACM_SCP			**1**	**2**	**3**	3	3	**1**	TOE CM coverage
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**1**	Delivery procedures
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**1**	Informal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**1***	Subset of the implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1***	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3		
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**1**	Indentification of security measures
	ALC_FLR								**3**	Systematic Flow remediation
	ALC_LCD				**1**	**2**	2	**3**		
	ALC_TAT				**1**	**2**	**3**	3	**1***	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-level design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing – sample
AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**1**	Examination of guidance
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité DICTAO Validation Server (DVS) 7.0 » du 05/10/2007, réf. : dictao_adovi_cibledesecurite.doc Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Dictao Validation Server (DVS) – Cible de sécurité (version publique) version 1.0 du 16/10/2007, réf. : dictao_adovi_cibledesécurité_publique.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation, Projet ADOVI du 22/10/2007, réf. : OPPIDA/CESTI/ADOVI/RTE/1.
[ANA-CRY]	Cotation de mécanismes cryptographiques, Qualification « standard » ADOVI, réf.:1616/SGDN/DCSSI/SDS/LCR du 30/07/07
[CONF]	• Liste de configuration v31.0 du 16/10/07, réf. :dictao_ADOVI_anx08_listeconfiguration • Liste de configuration (logicielle) réf. : dictao_ADOVI_anx12svnList-406.txt version 4.0.6 du 16/10/07
[GUIDES]	Guide d'installation du produit : - Guide Installation et Exploitation v6.0 du 05/10/2007, réf. : dictao_adovi_gu01_Guide Installation et Exploitation. Guide d'administration du produit : - Guide d'opération, DVS 4.0 v5.0 du 05/10/2007, réf. : dictao_dvs_v4.0_gu04_guideopération. - Guide d'Administration, DVS 4.0 v6.0 du 16/10/2007, réf. : dictao_dvs_V4.0_ gu03_guideadministration. Guide d'utilisation du produit : - Guide d'implémentation, Dictao Validation Server 4.0 v3.0 du 05/10/2007, réf. : dictao_dvs_gu02_Guide Implementation.
[PP]	Profil de protection « Module de vérification de signature électronique » référence PP-MVSE (DCSSI - PP/nc0503) version 1.0, de février 2005.

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.