Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2010/06

Coffre-fort électronique D3S
Version 4.4

Paris, le 17 novembre 2010

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

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

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

Toute correspondance relative à ce rapport doit être adressée au :

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

certification. anssi@ssi. gouv. fr

Référence du rapport de certification **ANSSI-CSPN-2010/06**
Nom du produit **Coffre-fort électronique D3S**
Référence/version du produit **Version 4.4**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN, Phase expérimentale)**
Développeur(s) **Dictao** **152, avenue de Malakoff** **75116 PARIS**
Commanditaire **Dictao** **152, avenue de Malakoff** **75116 PARIS**
Centre d'évaluation **Oppida** **6, avenue du Vieil Etang 78180 Montigny Le Bretonneux** **Tél : +33 (0)1 30 14 19 00, mél : christophe.blad@oppida. fr**

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 « Coffre-fort électronique D3S**,** Version 4.4 **»** développé par Dictao. D3S est un coffre-fort électronique organisé suivant le principe d'une salle des coffres physique : on y trouve des armoires contenant un ou plusieurs coffres. Ce coffre-fort électronique est évalué dans un contexte particulier : la surveillance des activités transactionnelles d'un « opérateur » par une « autorité » (ARJEL[1]). L'« autorité » souhaite contrôler certaines opérations au sein du système d'information de l'opérateur et installe chez ce dernier un dispositif technique chargé de recueillir et d'archiver les traces de ces opérations.

D3S est un composant de ce dispositif technique chargé de garantir la traçabilité des opérations effectuées sur le système d'information de l'opérateur. Ce dispositif est constitué d'un capteur et du D3S. Le capteur, hors du périmètre du présent document, est chargé de récolter les données tracées.

Ces données sont ensuite archivées dans le coffre-fort electronique afin d'en garantir l'intégrité et l'exhaustivité dans le temps. Avant que les données ne soient transmises à l'« autorité », le D3S enregistre les données et les scelle de manière à ce qu'elles ne puissent être altérées, en rendant détectable tout ajout, suppression ou modification d'une opération.

Une partie de la sécurité proposée par le D3S s'appuie sur des mécanismes cryptographiques. Les clés utilisées par ces mécanismes sont gérées et protégées par un dispositif de sécurité matériel (ou HSM pour *Hardware Security Module*).

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.

1.2.1 Catégorie du produit

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

[1] Autorité de Régulation des Jeux En Ligne

1.2.2 Identification du produit

La version installée est numérotée 4.4. Aucune information, commande ou procédure n'est précisée dans les guides afin d'identifier sans ambiguïté la version logicielle installée. Cependant, on peut identifier la version de D3S dans le fichier de propriétés Maven, outil logiciel ayant permis de construire les deux fichiers War correspondant aux deux modules du produit (d3s-authority et d3s-storage) :

- D3S_4.4/container/webapps/dictao-d3s-authority-web/META-INF/maven/com.dictao.d3s/dictao-d3s-authority-web/pom.properties ;

- D3S_4.4/container/webapps /dictao-d3s-storage/META-INF/maven/com.dictao.d3s/dictao-d3s-storage/pom.properties.

1.2.3 Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- le contrôle de l'accès au coffre-fort ;
- le chiffrement des dépôts (création de l'enveloppe) ;
- le scellement des dépôts (création de la trace) ;
- le chaînage des traces ;
- la signature de la configuration du coffre-fort.

1.2.4 Configuration évaluée

Sans objet.

2 L'évaluation

2.1 Référentiels d'évaluation

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

2.2 Charge de travail prévue et durée de l'évaluation

La charge de travail prévue lors de la demande de certification était conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 35 hommes x jours. L'évaluation s'est déroulée au cours du mois de juin 2010.

2.3 Travaux d'évaluation

Ce paragraphe apporte des précisions sur le déroulement de l'évaluation et d'éventuels compléments sur la cible de sécurité [ST], issus du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1 Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1 Spécification de besoin du produit

Conforme à la cible de sécurité [ST] (chapitre « Argumentaire »).

2.3.1.2 Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [ST] (chapitre « Description des biens sensibles que le produit doit protéger »).

2.3.1.3 Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [ST] (chapitre « Menaces considérées »).

2.3.1.4 Fonctions de sécurité

La fonction d'authentification forte décrite dans la cible de sécurité [ST] est associée à un mécanisme de gestion des rôles « Déposant » et « Lecteur ». Pour les administrateurs, l'accès est réalisé en SSH.

2.3.1.5 Hypothèses sur l'utilisation du produit

Les accès aux fonctionnalités du coffre-fort doivent être effectués au travers de canaux sécurisés (HTTPS). Ceux-ci doivent être configurés conformément à l'état de l'art notamment en termes de suites de chiffrement autorisées et de versions protocolaires.

2.3.1.6 Utilisateurs typiques

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

2.3.2 Installation du produit

Lors de l'installation du produit Coffre-fort D3S, Dictao fournit le système d'exploitation et l'application Coffre-fort D3S. Le produit est livré clé en main. En effet, Dictao installe le socle système et l'application Coffre fort D3S, et configure le HSM ainsi que le coffre-fort. Le produit est ensuite livré au client prêt à fonctionner, sans nécessité de configuration supplémentaire.
Dictao fournit alors :

- à l'opérateur de jeu, le certificat avec le profil « Déposant » permettant le dépôt des traces, ainsi que les clés permettant l'administration basique du système (arrêter et redémarrer l'application et les interfaces réseaux) via SSH ;
- à l'« autorité » le certificat permettant d'administrer le produit (hors cible), le certificat avec le profil « Lecteur » permettant d'exporter les traces et de vérifier leur chaînage, les cartes à puces personnalisées lors de la cérémonie des clés permettant de réinitialiser le HSM et enfin les clés liées aux opérations de vérification de vérification de signatures et de déchiffrement des traces.

La procédure d'initialisation du boîtier HSM et la procédure de configuration du coffre-fort sont décrites dans [Guide_Op_Initialisation].

2.3.2.1 Plate-forme de test

Le matériel utilisé pour les tests est le suivant :

- processeur Intel Core2 Duo T6600 cadencé à 2.40GHz ;
- 1 Go de mémoire vive ;
- disque dur SATA d'une capacité de 80 GB ;
- 2 interfaces réseau 10/100/1000 :
- boîtier HSM Ncipher ;
- 3 cartes à puce SoftCard ;
- lecteur de carte.

L'architecture logicielle fournie est la suivante, le socle système étant un système d'exploitation de type Linux :

- un noyau Linux 2.6.18-194.el5 (Red Hat Enterprise Linux Server release 5.5 - Tikanga) ;
- les composants suivants installés sur le serveur afin de faire fonctionner l'application :
    - coffre Fort D3S ;
    - java runtime environnement build 1.6.0_19-b04 ;
    - java runtime environnement build 1.5.0_22 (partie initialisation/administration de la solution) ;
    - Oracle version 10.2.0.1 (installée dans /u01/app/) ;
    - openSSL version 0.9.8e-fips-rhel5 01 Jul 2008;
    - apache tomcat version 6.0.20 ;
    - apache tomcat version 5.5.23 (partie initialisation/administration de la solution) ;
    - openSSH 4.3p2-41.el5.

2.3.2.2 Particularités de paramétrage de l'environnement

Sans objet.

2.3.2.3 Options d'installation retenues pour le produit

Sans objet.

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

Sans objet.

2.3.2.5 Durée de l'installation

Sans objet.

2.3.2.6 Notes et remarques diverses

Sans objet.

2.3.3 Analyse de la conformité

2.3.3.1 Analyse de la documentation

Les guides [GUIDES] sont clairs, didactiques et étayés par de nombreux exemples.

2.3.3.2 Revue du code source

Le code source n'a pas été examiné.

2.3.3.3 Fonctions testées

Le tableau ci-dessous reprend les tests menés lors de l'évaluation ainsi que les verdicts associés (***Réussite***, ***Échec*** ou ***Non Conclusif***).

Description de la fonction	**Résultat**
Contrôle de l'accès au coffre et aux traces qu'il contient : authentification par certificats SSL et autorisation des opérations selon les profils « déposant », « lecteur » et « administrateur »	***Réussite***
Protection en intégrité et en confidentialité des échanges avec le coffre	***Réussite***
Chiffrement et scellement des dépôts et des traces	***Réussite***
Chainage et protection en intégrité d'une suite de traces	***Réussite,*** toutefois, voir chapitre 2.3.4
Protection en intégrité du fichier de configuration du coffre	***Réussite***

2.3.3.4 Synthèse des fonctions testées et non testées

Les tests de conformité ont permis de tester toutes les fonctionnalités offertes par l'IHM Web et les Web Services destinés aux différents profils d'utilisateurs.

Les applications d'administration du produit D3S et de vérification de l'intégrité des traces et leur déchiffrement sont hors périmètre de la cible de sécurité [ST] et n'ont donc pas été analysées.

2.3.3.5 Avis d'expert sur le produit

Le produit est conforme à sa cible de sécurité.

Son interface est simple d'emploi. L'applicatif fournit uniquement les fonctionnalités dont l'utilisateur a besoin, les boutons dont il n'a pas besoin sont grisés et les fonctionnalités correspondantes sont désactivées côté serveur.

2.3.4 Analyse de la résistance des mécanismes et des fonctions

2.3.4.1 Liste des fonctions testées et résistance

Les fonctions testées sont celles citées au paragraphe 2.3.3.3. Sous réserve de la bonne configuration du produit par l'administrateur, un utilisateur illégitime ne pourra pas réaliser d'opérations pour lesquelles il n'a pas de droit.

La protection en intégrité du chaînage des preuves de dépôts présente une vulnérabilité résiduelle de conception qui n'est pas exploitable dans l'environnement prévu d'utilisation mais qui mériterait d'être corrigée pour être conforme à l'état de l'art dans le domaine.

2.3.4.2 Avis d'expert sur la résistance des mécanismes

La résistance des mécanismes de sécurité est conforme à l'état de l'art. Il n'a pas été mis en évidence de vulnérabilités exploitables dans le cadre de l'évaluation du produit. Les mécanismes de sécurité qui s'appuient sur la cryptographie font l'objet d'une analyse théorique particulière dont les principales conclusions sont données au chapitre 2.4.

2.3.5 Analyse des vulnérabilités (conception, implémentation…)

2.3.5.1 Liste des vulnérabilités connues

Les vulnérabilités publiques connues sur les différentes briques logicielles utilisées par le produit ne sont pas exploitables et n'impactent pas la sécurité du produit. Il n'a pas été identifié de vulnérabilités connues sur ce produit.

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

La protection en intégrité du chaînage des preuves de dépôts pourrait être améliorée. Il est contournable localement (au niveau de l'équipement) si celui-ci est compromis. Des améliorations sont envisageables et permettraient de renforcer la résistance à la compromission locale de l'équipement, sans toutefois l'éliminer complètement. C'est pourquoi il est considéré que le mécanisme répond quand même aux exigences de la cible de sécurité [ST].

Pour le reste, l'analyse n'a pas fait apparaître de vulnérabilités pouvant compromettre l'intégrité et la confidentialité d'une ou de plusieurs traces stockées par le Coffre-fort D3S.

Cependant, l'accès aux comptes systèmes « root » et « admin » doivent donner lieu à des mesures physiques et organisationnelles strictes afin d'assurer la protection des fonctions de sécurité du produit Coffre-fort D3S.

2.3.6 Analyse de la facilité d'emploi et préconisations

2.3.6.1 Cas où la sécurité est remise en cause

Sans objet.

2.3.6.2 Recommandations pour une utilisation sûre du produit

Compte « root »

Il est fortement recommandé que seule l'« autorité » possède le login / mot de passe d'accès au compte *root* qui permet d'accéder à l'ensemble des fonctions du système. Ce mot de passe doit donc suivre une politique de création et une politique de gestion conforme à la note du CERTA (No CERTA-2005-INF-001).

La plate-forme doit pouvoir être mise à jour. Il est préconisé que les mises à jour se fassent sous la responsabilité de l'« autorité » (puisque le mot de passe pour le compte « root » ne devrait être fourni ni à l'hébergeur, ni au développeur). Par exemple, la mise à jour pourrait être réalisée directement par l'« autorité » (le développeur fournit à l'« autorité » l'ensemble de la procédure de mise à jour, ainsi que les logiciels si besoin), soit indirectement (l'« autorité » s'authentifie en tant que « root », et laisse le développeur effectuer la mise à jour sous sa surveillance).

Lors de la fermeture ou la réinitialisation de certains services, il est recommandé de demander à l'hébergeur de déconnecter physiquement le câble réseau connecté sur l'interface côté « déposant » du D3S afin d'éviter une exposition du système.

Quel que soit le mode d'intervention, la présence de l'« autorité » est préconisée afin de s'assurer de la non altération des dépôts et des traces déjà stockés.

Enfin, aucun système de chiffrement du disque n'étant mis en place, l'équipement hébergeant l'application Coffre-fort D3S devrait être scellé afin de détecter toute ouverture physique illégitime du boîtier. Ce scellé devrait être vérifié lors de chaque audit de la plate-forme.

Compte « admin »

Le compte « admin » possède un accès logique au socle système avec les droits d'un utilisateur de base, plus certaines fonctions d'administration accessibles via les commandes « *sudo* ».

Une vigilance particulière doit être donnée à la gestion des vulnérabilités du socle système. En effet, une élévation de privilège pourrait donner des informations sensibles à un utilisateur du compte « admin » comme les identifiants de connexion à la base de données.

Architecture D3S

Il est préconisé d'appliquer une architecture de type N-tiers, c'est-à-dire de découpler la base de données du reste de l'application. La base de données devrait être gérée par l'« autorité ».

2.3.6.3 Avis d'expert sur la facilité d'emploi

L'utilisation du produit est simple et intuitive, l'accès aux fonctionnalités est immédiat.

L'utilisation des Web Services (dépôt et vérification des traces) par le « déposant » s'avère simple d'emploi. Elle se fait à partir de l'application fournie par le développeur (Dictao)

2.3.7 Accès aux développeurs

L'évaluateur a pu contacter facilement les développeurs qui ont été coopératifs et ont répondu clairement aux questions de l'évaluateur.

2.4 Analyse de la résistance des mécanismes cryptographiques

Authentification SSL/TLS
La suite cryptographique suivante utilisée par le protocole TLS pour l'authentification est conforme au référentiel [RGS_B_1] de l'ANSSI :

Authentification	Echange de clés	Chiffrement	Code d'authentification de message
RSA 2048	RSA 2048	AES 128	SHA1

Vérification et signature du jeton d'autorisation
Les mécanismes cryptographiques mis en œuvre par le produit sont conformes au référentiel [RGS_B_1] de l'ANSSI.

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

Chiffrement des dépôts
L'utilisation de l'algorithme AES en mode CBC est conforme au référentiel [RGS_B_1] de l'ANSSI.

Protection en intégrité de la suite de traces
Le chaînage des preuves de dépôts est protégé en intégrité au moyen d'un mécanisme de signature conforme au référentiel [RGS_B_1].

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

2.5 Analyse du générateur d'aléas

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

3 La certification

3.1 Conclusion

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

Ce rapport de certification de sécurité de premier niveau atteste que le produit « Coffre-fort électronique D3S, Version 4.4 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST].

3.2 Restrictions d'usage

Dans le respect des hypothèses d'utilisation formulées par le développeur, aucune restriction d'usage n'est identifiée pour le produit Coffre-fort électronique D3S.

Annexe 1. Références documentaires du produit évalué

[ST]	Cible de sécurité C.S.P.N.Coffre-fort électronique D3S *Référence* : dictao_d3s_cible_cspn Version 1.23 *Date :* 16 Novembre 2010
[GUIDES]	Guide D3S d'Intégration des WebServices ARJEL Guide D3S de l'auditeur Guide D3S de l'opérateur Guide D3S Opérateur d'initialisation
[RTE]	Rapport Technique d'Évaluation (RTE) Coffre-fort D3S - DICTAO *Référence* : OPPIDA/CESTI/D3S/RTE/1.1 *Date :* 19 juillet 2010
[CRYPTO]	Rapport d'évaluation des mécanismes cryptographiques - Coffre-fort électronique D3S *Référence* : OPPIDA/CESTI/D3S/CRYPTO/1.3 *Date :* 02 novembre 2010

Annexe 2. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CSPN-CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI, disponible sur www. ssi. gouv. fr
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 2. 4, phase expérimentale, n° 915/SGDN/DCSSI/SDR/CCN du 25 avril 2008. Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1. 4. Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1. 3. Documents disponibles sur www. ssi. gouv. fr
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, v1.11