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-2013/04

Dictao Trust Platform
Version 4

Paris, le 18 avril 2013

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

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

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

Toute correspondance relative à ce rapport doit être adressée au :

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

certification.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2013/04**
Nom du produit **Dictao Trust Platform**
Référence/version du produit **Version 4**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **Dictao SA** **152 avenue Malakoff** **75116 Paris** **France**
Commanditaire **Dictao SA** **152 avenue Malakoff** **75116 Paris** **France**
Centre d'évaluation **Oppida** **4-6 avenue du vieil étang,** **78180 Montigny le Bretonneux** **France**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

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

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

Table des matières

1. Le produit

1.1. Présentation du produit

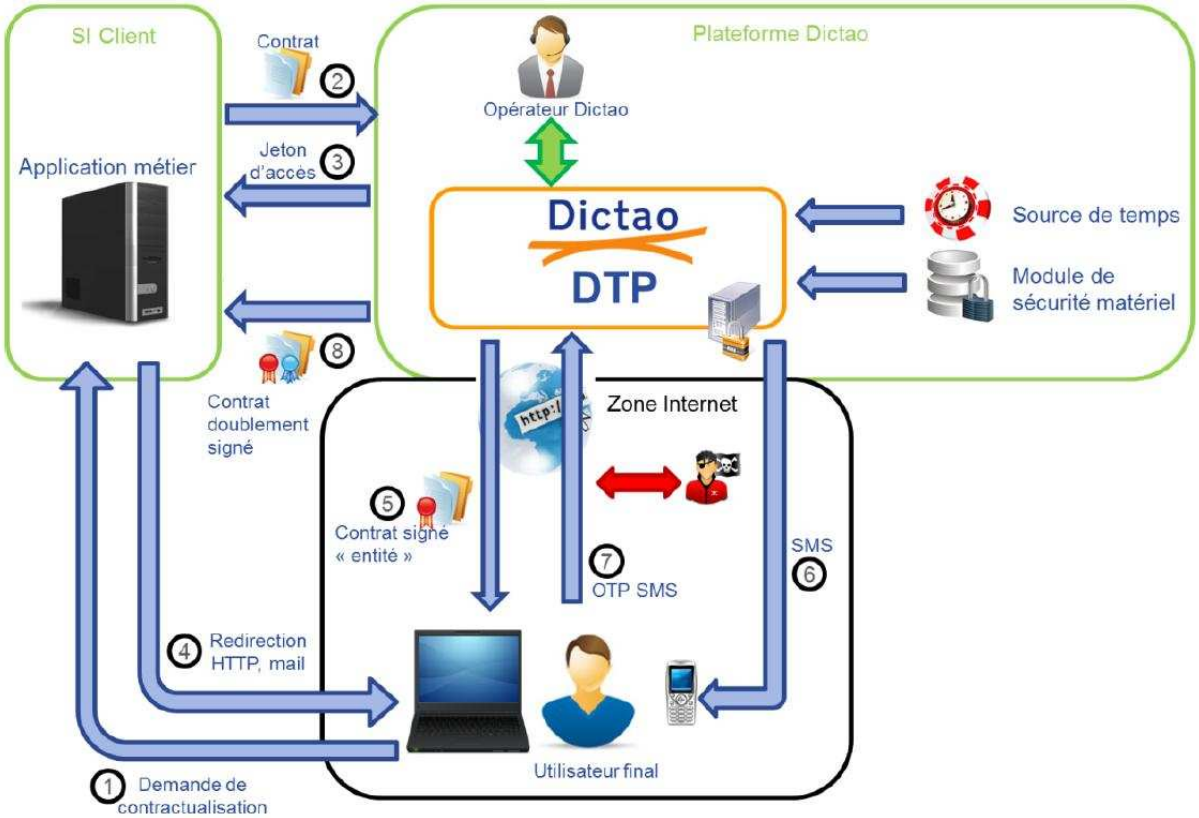
Le produit évalué est « Dictao Trust Platform (DTP), version 4 » développé par la société Dictao. DTP est une application ordonnançant les étapes d'une contractualisation en ligne par laquelle des opérations de confiance sont nécessaires.

Le produit permet à une application métier de :

- créer, archiver ou annuler une contractualisation ;
- ajouter un document à signer à une contractualisation ;
- demander un jeton d'accès de signature pour un utilisateur final ;
- récupérer le contrat signé par les deux parties et la preuve de transaction associée.

DTP fournit également à l'utilisateur final une interface lui permettant de visualiser le contrat et de donner son consentement à la signature électronique du contrat.

La séquence de signature se déroule en 8 étapes, comme indiqué dans la figure ci-dessous :



1. l'utilisateur se connecte à l'application métier pour une demande de contractualisation via Internet ;
2. l'application métier envoie à DTP le document à signer ;

3. l'application métier demande un accès à DTP pour l'utilisateur et reçoit un jeton d'accès ;
4. l'application métier transfère le jeton d'accès vers l'utilisateur ;
5. l'utilisateur se connecte sur l'interface de DTP grâce à son jeton d'accès et visualise le contrat signé par l'entité émettrice ;
6. l'utilisateur reçoit un code d'accès à usage unique (*one time password* ou OTP) par SMS (*short message service*);
7. l'utilisateur donne son consentement via une case à cocher puis effectue la demande de signature après saisie de l'OTP ;
8. l'application métier peut alors récupérer le document doublement signé sur DTP via le protocole TLS avec authentification mutuelle par certificat.

1.2. Description du produit évalué

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

1.2.1. Catégorie du produit

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

1.2.2. Identification du produit

Une procédure exécutée lors de la compilation et de l'installation du produit est responsable du calcul d'une somme de contrôle qui est automatiquement insérée dans la configuration générée. La somme de contrôle *dtpVersionId* contenue dans les preuves de scellement générées permet d'identifier la version de la plateforme évaluée.

La version certifiée du produit est identifiable par la somme de contrôle suivante :

bc067bf9360d0c821322a7712ed727bd24fbfd9f110f035faef005d1ff4f4bb0

Les briques principales du produit sont les suivantes :

Fonction	Application et branche	Version évaluée
Distribution GNU/Linux	CentOS 6.x	6.2
Serveur Web	Apache 2.2.x	2.2.15
Serveur d'application	Tomcat 6.0.x	6.0.35
Machine virtuelle Java	Oracle JRE 1.6.0.x	1.6.0_31-b04

1.2.3. Services de sécurité

Les services de sécurité fournis par le produit faisant l'objet de l'évaluation sont :
- l'authentification forte des applications métiers par certificat ;
- la protection des informations envoyées entre DTP et les applications métier et entre DTP et le client ;
- la signature « cachet serveur » des contrats garantissant leur intégrité tout au long du processus ;
- l'authentification des utilisateurs par OTP ;
- la génération de clés et de certificats à usage unique pour les utilisateurs finaux ;
- la signature des preuves de transaction, permettant d'assurer que la contractualisation a eu lieu.

Le module de sécurité matériel effectuant la signature du contrat pour le compte de l'utilisateur n'a pas été évalué.

1.2.4. Configuration évaluée

Dans sa version évaluée, le produit n'offre pas les fonctionnalités suivantes :
- la signature multi-tenant (plateforme partagée entre plusieurs applications métiers) ;
- la signature multi-documents ;
- la signature du contrat sur le poste de l'utilisateur final.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. Les références des documents se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 35 hommes x jours.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues 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 [CDS] (chapitre 3 « Argumentaire »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 3.4 « Biens à protéger »).

2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 3.5 « Menaces considérées »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 4 « Fonctions de sécurité »).

2.3.1.5. Utilisateurs typiques

Deux types d'acteurs sont évoqués dans la cible de sécurité [CDS] (chapitre 3.2.2 « Utilisateurs ») :

- l'application métier : cette application exploite les services Web proposés par le service DTP pour mettre à disposition de ses propres clients un outil de signature de contrats ;
- l'utilisateur final : après visualisation du contrat (en accédant à une adresse particulière contenant son jeton d'accès), l'utilisateur décide ou non de signer électroniquement ce contrat en cochant une case d'acceptation et en fournissant l'OTP qu'il a préalablement reçu par SMS.

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Dictao a fourni à l'évaluateur des outils permettant de réaliser les tests (client lourd réalisant les appels aux *webservices* et sources Java pour compiler un client personnalisé).
Un kit de connexion au DVS (*Dictao Validation Server*) a également été fourni à l'évaluateur pour lui permettre de vérifier la validité des signatures générées au travers du service DTP.

2.3.2.2. Particularités de paramétrage de l'environnement

L'installation du produit ne nécessite aucun paramétrage particulier.

2.3.2.3. Options d'installation retenues pour le produit

Aucune option d'installation n'est disponible.

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

L'utilisateur final doit disposer d'un navigateur web graphique et le plugin Adobe Acrobat Reader doit y être installé pour permettre la visualisation du document à signer.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est claire et aucune non-conformité n'a été relevée.

2.3.4. Revue du code source (facultative)

Les évaluateurs ont eu accès à une partie du code source sur leur demande.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Authentification forte des applications par certificat	**Réussite**
Signature « cachet serveur » des documents déposés	**Réussite**
Service des pages d'affichage et de signature protégées requérant une authentification serveur.	**Réussite**
Authentification des utilisateurs par OTP SMS	**Réussite**
Génération des clés et des certificats à usage unique pour les utilisateurs finaux	**Sans conclusion**

Signature des preuves de transaction	**Réussite**

2.3.6. Fonctionnalités non testées

Sans objet.

2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités

La génération des clés et des certificats à usage unique pour les utilisateurs finaux n'a pas été analysée car elle repose sur un produit dont les fonctions cryptographiques n'ont pas été évaluées, voir la première recommandation au chapitre 2.3.12.2.

2.3.8. Avis d'expert sur le produit

Le produit est conforme à sa cible de sécurité [CDS]. Aucune non-conformité n'a été détectée sur les fonctions de sécurité du produit.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Fonction et mécanisme
Authentification forte des applications métier
Gestion des sessions
Gestion des autorisations
Validation des données d'entrée

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Ces mécanismes sont considérés comme robustes et suffisants dans le cadre d'une évaluation CSPN.

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur cette version du produit.

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

Aucune.

2.3.11. Accès aux développeurs

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Au cours des échanges techniques qui ont eu lieu, le développeur a fait preuve d'une très bonne maîtrise de son produit et a été en mesure de répondre rapidement aux questions posées.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Néant.

2.3.12.2. Recommandations pour une utilisation sûre du produit

L'utilisation du produit doit être faite sur un PC hébergeant un système d'exploitation à jour concernant les correctifs de sécurité et correctement administré. Le poste doit être durci afin d'être protégé contre des codes malveillants (voir le guide d'hygiène informatique [GUIDE-ANSSI], notamment ses règles 14 et 15).

2.3.12.3. Avis d'expert sur la facilité d'emploi

Le service DTP est un SaaS. Il nécessite l'implémentation des appels aux *webservices*. Cette implémentation peut nécessiter du temps mais l'évaluateur estime que la documentation est suffisamment claire pour qu'elle puisse être réalisée dans de bonnes conditions.

Moyennant le respect des recommandations évoquées précédemment, l'évaluateur n'a pas identifié de cas où le produit serait configuré ou utilisé de façon non sûre mais qu'un utilisateur pourrait raisonnablement croire sûre.

2.3.12.4. Notes et remarques diverses

L'évaluateur préconise l'utilisation et le maintien à jour d'un anti-virus sur le serveur hébergeant l'application métier.

2.4. Analyse de la résistance des mécanismes cryptographiques

La liste de référence des mécanismes cryptographiques est fournie par la cible de sécurité [CDS] et les spécifications cryptographiques [SPEC_CRY]. La résistance de ces mécanismes a été analysée par l'évaluateur.
Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et concluent que tous les mécanismes analysés ne sont pas conformes aux exigences du référentiel cryptographique de l'ANSSI. En particulier, DICTAO devra s'assurer de l'utilisation d'un module de sécurité matériel qualifié par l'ANSSI.
Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilité pour le niveau visé.

2.5. Analyse du générateur d'aléas

Le produit s'appuie sur un générateur d'aléas externe ne faisant pas l'objet de la présente certification. Aucune information n'étant disponible sur ce générateur d'aléas, permettant la génération de l'ensemble des clefs de signature, ainsi que sur son utilisation effective par le générateur logiciel qu'il met en œuvre : il est recommandé au développeur de s'assurer que ce générateur physique d'aléa respecte bien les règles et recommandations du référentiel de l'ANSSI [REF_CRY] en choisissant, comme indiqué au paragraphe 2.4, un module de sécurité matériel qualifié par l'ANSSI.

3. La certification

3.1. Conclusion

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

Ce certificat atteste que le produit Dictao Trust Platform, version 4, soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2. Restrictions d'usage

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

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Dictao-CSPN-DTP-CdS-V1.7;* Référence : *dictao_DTP_cible_cspn ;* Version : *1.7* ; Date : *13/03/2013*
[RTE]	*Rapport technique d'évaluation CSPN Dictao Trust Platform;* Référence : *OPPIDA/CESTI/DTP/RTE/1.6* ; Date : *18/03/2013.*
[SPEC-CRY]	*Description des mécanismes cryptographiques. Plateforme de confiance DTP C.S.P.N. ;* Version : *1.0;* Date : *27/07/2012.*
[ANA-CRY]	*Rapport d'évaluation des mécanismes cryptographiques DTP;* Référence : *OPPIDA/2012/DOC/893/CRYPTO/1.3 ;* Version : *1.3 ;* Date : *06/03/2013.*
[GUIDES]	Guide d'installation : • *Guide du kit d'intégration CSPN* *Version : 1.0 ;* *Date : 15/05/2012.* • *Integration guide* *Version : 3.4 ;* *Date : 15/05/2012.* Guide d'utilisation : *Guide de démarrage DTP ;* Version : *1.0* ; Date : *20/07/2012.*

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr
[GUIDE-ANSSI]	Guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI), version finalisée du 28 janvier 2013. Disponible sur www.ssi.gouv.fr/hygiene-informatique.