Dictao

152, avenue de Malakoff
75116 Paris

Cible de sécurité C.S.P.N.

Service DTP

Réf. : dictao_DTP_cible_cspn
Version 1.7 du 13/03/2013

Référence : **Version :** **Date de dernière mise à jour :**	dictao_DTP_cible_cspn 1.7 13/03/2013
Niveau de confidentialité :	CONFIDENTIEL

Diffusion

Destinataires	Objet de la diffusion
ANSSI	Certification C.S.P.N.
OPPIDA	Certification C.S.P.N

Table des mises à jour du document

N° de version	Etat[1]	Date	Auteur	Objet de la mise à jour
1.0	V	28 mars 2012	Dictao	Version validée
1.1	V	05 avril 2012	Dictao	Prise en compte des remarques avant enregistrement
1.2	V	14 mai 2012	Dictao	Mise à jour de l'algorithme de hachage de la signature de l'audit et de l'algorithme de signature de génération de certifcats à usage unique par souci d'interropérabilité
1.3	V	02 juillet 2012	Dictao	Précision sur les hypothèses de sécurité des documents PDF soumis à la plateforme DTP
1.4	V	08 janvier 2013	Dictao	Clarification du vocabulaire entre application métier et application tierce. Précision sur la consommation du jeton d'accès à usage unique. Précision sur les interactions entre les différents acteurs et composants de l'architecture.Précision sur les hypothèses de sécurité de la politique de mise à jour d'Apache. Précision sur le status de l'application métier (élément de confiance dans les hypothèses de sécurité). Description de la politique d'OTP SMS utilisée.
1.5	V	21 janvier 2013	Dictao	Clarification de l'identification du produit à évaluer. Mise à jour de l'environnement technique du produit. Suppression du VPN des fonctions sécurité et prise en compte du VPN comme hypothèse sur l'environnement. Précision sur le type signature personnelle réalisée par DTP
1.6	V	04 février 2013	Dictao	Clarification sur le mode de communication entre l'application métier et le Service DTP Précision sur le type d'authentification TLS de l'application métier
1.7	V	13 mars 2013	Dictao	Précision sur les menaces considèrées

[1] **T** : En cours de modification ; **V** : Validé

SOMMAIRE

1. INTRODUCTION

Le présent document est la cible de sécurité pour la certification de sécurité de premier niveau (C.S.P.N.) du ***Service DTP (Dictao Trust Platform)*** par l'Agence nationale de la sécurité des systèmes d'information. Les fonctions de sécurité décrites ici permettent de mettre en œuvre des fonctions de création et de validation de signatures numériques.

1.1 Vocabulaire

- Application métier : client applicatif légitime et préalablement enregistré du service DTP. Cette application métier initialise la transaction, ajoute le document à signer, demande les droits d'accès pour ses utilisateurs et finalement récupère le document signé par toutes les parties ainsi que la preuve de transaction générée par DTP. Cette application métier peut personnaliser l'affichage à travers le mécanisme dit « compagnie ».
- Application tierce : tout applicatif externe à la plateforme DTP autre que l'application métier.
- Compagnie : il s'agit d'une spécialisation de l'application métier permettant de personnaliser l'affichage offert à l'utilisateur final. La mise en page est identique. Toutefois la feuille de style peut être personnalisée, ainsi que les logos et les images. Ainsi une application peut avoir plusieurs compagnies et offrir le même type de contrat sous des marques différentes et des identités graphiques différentes.
- Utilisateur final : personne physique, identifiée dans le système d'information de l'application métier, représentant la seconde partie dans l'établissement du contrat avec l'application métier.
- Preuve de transaction : archive électronique contenant l'ensemble des données utilisées pour établir les signatures électroniques du document proposé par l'application métier à l'utilisateur. Les preuves de transaction sont stockées en base de données. Elle contient notamment :
    - La trace d'audit de la transaction qui contient la description de l'ensemble des actions (création, cachet serveur, consultation, signature utilisateur final, archivage…) liées à la constitution de la transaction ;
    - La preuve d'authentification de l'utilisateur final lors de sa demande de signature du contrat ;
    - Le contrat signé par les deux parties.

2. IDENTIFICATION DU PRODUIT

Organisation éditrice	Dictao
Lien vers l'organisation	www.dictao.com
Nom commercial du produit	*Service DTP ("Dictao Trust Platform")*
Numéro de la version évaluée	4
Catégorie de produit	Identification, authentification et contrôle

Note : Le produit identifié par cette cible est un service de contractualisation dématérialisé. Le terme *Platform* n'apparait dans la dénomination commerciale du produit que pour des raisons de lisibilité marketing.

3. ARGUMENTAIRE

Le contexte d'utilisation correspond à la signature de contrat en ligne proposé par une application métier à destination d'un contractant.

3.1 Description fonctionnelle

DTP est une application ordonnant les étapes de la contractualisation en ligne nécessitant des opérations de confiance.

La contractualisation est appelée transaction. Une transaction est initiée par une application métier.

Chaque transaction est identifiée de manière univoque par un identifiant unique généré par le service DTP. Seule l'application initiatrice de la transaction a les droits de modifier cette transaction.

Les paramètres des appels manipulant une transaction sont sauvegardés par DTP afin de constituer la trace d'audit de la transaction.

L'application métier peut, à travers l'interface applicative de DTP :

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

L'utilisateur final dispose d'une interface lui permettant de visualiser le contrat et de donner son consentement à la signature électronique du contrat. Cette interface graphique est accessible sur présentation du jeton d'accès demandé par l'application métier.

Trois signatures électroniques sont réalisées par DTP :

1. La première a lieu lorsque l'application métier ajoute le contrat à signer dans la transaction. Cette signature est le cachet serveur de l'entité au nom de l'émetteur du document.
2. La deuxième a lieu lorsque l'utilisateur final consent au contrat. La génération des clefs et la création de la requête de certification pour l'utilisateur final sont réalisées par DTP. La signature électronique est réalisée au nom de l'utilisateur final. Le bi-clef généré par un module de sécurité matériel (HSM, *Hardware Security Module*) et le certificat de signature ne sont pas réutilisables d'une transaction à l'autre.

   Cette signature personnelle respecte les exigences d'une signature électronique sécurisée au sens du décret 2001-272, en application de l'article 1316-4 du code civil, c'est-à-dire :

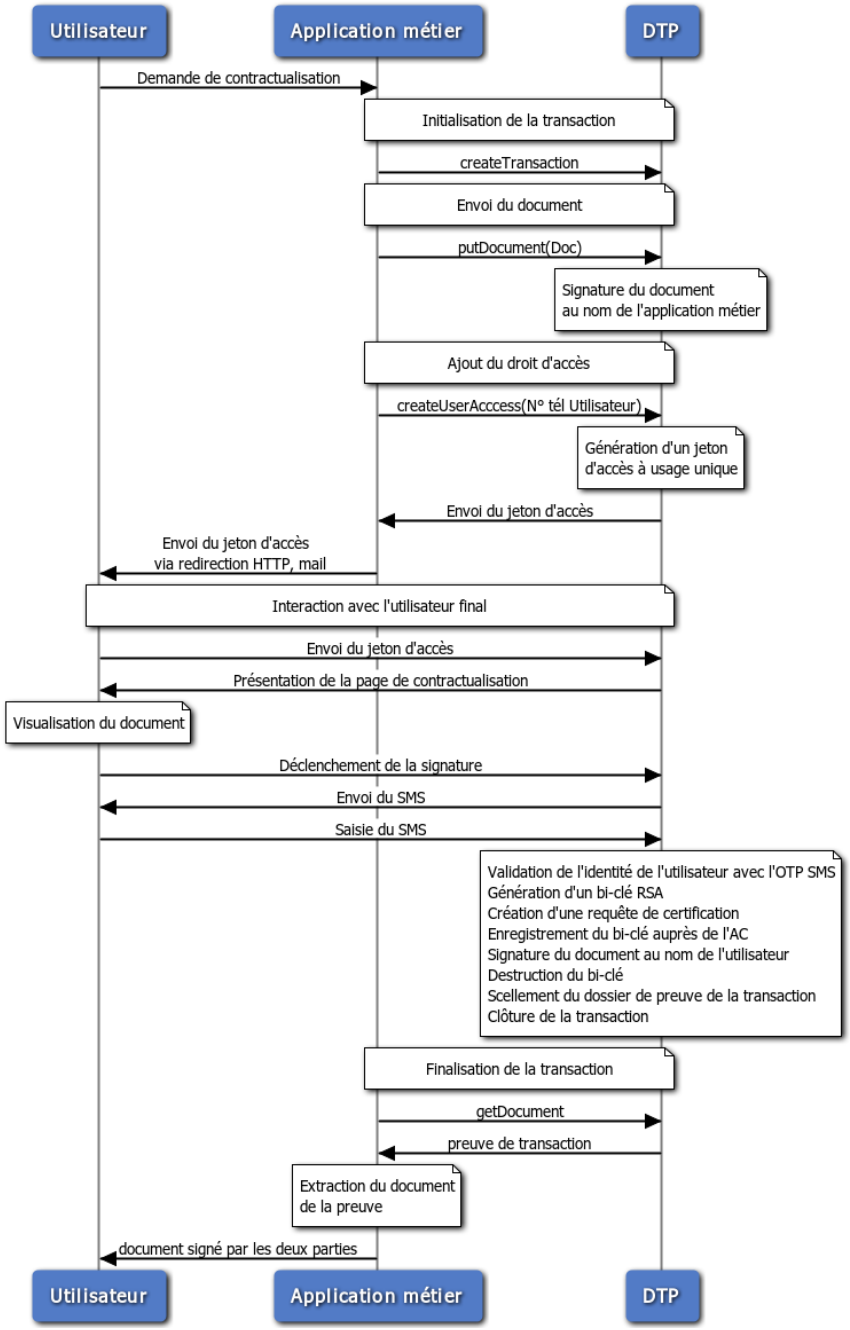
   - est un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ;
   - est propre au signataire ;
   - est créée par des moyens que le signataire peut garder sous son contrôle exclusif ;
   - garantit avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.

   Elles ne sont cependant pas « présumées fiables ». La fiabilité est présumée, jusqu'à preuve contraire, lorsque le procédé met en œuvre :

   - une signature électronique sécurisée,
   - établie grâce à un dispositif sécurisé de création de signature électronique (typiquement une carte à puce),
   - et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié (nécessite notamment un face à face).

   Par opposition, les signatures personnelles apposées par DTP sont donc dites « signature simple ».
3. La troisième a lieu lors du scellement de la transaction. Elle porte sur la preuve de transaction et est un cachet serveur également réalisé par le service DTP.

3.1.1 Cycle de vie typique d'une transaction



L'utilisateur final se connecte à l'application métier pour y faire une demande de contractualisation.

La transaction est initialisée par l'application métier à l'aide d'un appel createTransaction.

L'application métier est ensuite en mesure d'envoyer le document à signer à DTP par un appel à putDocument. Ce document est signé au nom de l'application métier appelante.

Un accès utilisateur est demandé par l'application métier, au nom de l'utilisateur final. L'application métier fournit un numéro de téléphone associé à l'utilisateur final. Un jeton d'accès à usage unique est alors crée par DTP suite à l'appel de la méthode createUserAccess.

Ce jeton d'accès a une durée de vie limitée déterminée par l'application métier. Ce jeton d'accès n'est plus utilisable dés que la contractualisation s'est achevée avec succès ou que la durée de validité est dépassée.

L'utilisateur final est invité à se rendre sur l'interface utilisateur de DTP où il devra présenter son jeton d'accès. Il peut alors visualiser le contrat et faire part de son engagement pour déclencher la signature du contrat à l'aide d'un OTP transmis par SMS.

Lors de la signature, DTP valide l'identité du signataire à l'aide du moyen OTP SMS. Si l'authentification est valide, il procède à la génération d'un bi-clef RSA, à la création d'une requête de certification et à l'enregistrement de ce bi-clef par une Autorité de Certification interne à DTP. Le contrat est ensuite signé par DTP au nom de l'utilisateur. Puis finalement, DTP supprime le bi-clef de sa mémoire.

En fin de transaction, DTP procède automatiquement au scellement de la transaction et sa fermeture.

L'application métier récupère alors les différents documents constituant la transaction, que ce soit le contrat signé par toutes les parties ou la preuve de transaction.

3.2 Utilisation du produit

3.2.1 Description des hypothèses sur l'utilisation du produit

DTP fait l'hypothèse que l'application métier est de confiance et par conséquent que les documents à signer le sont également et que leur contenu est légal. Par exemple, les documents doivent être stables sémantiquement (ils ne contiennent pas de script générant un contenu dynamique), ne masquent pas d'information (ils ne contiennent pas de texte blanc sur fond blanc) et les engagements contractuels sont conformes à la législation en vigueur.

3.2.2 Utilisateurs

Une fois installé, DTP interagit avec différents utilisateurs.

L'application métier est le client applicatif (logiciel) chargé de la création de la transaction, de l'ajout de document à signer, de la fermeture de la transaction, entre autres.

Les contractants sont les utilisateurs physiques. Après authentification, ils ont la possibilité de déclencher le processus de signature du document soumis par l'application métier.

Les agents sont les personnes physiques chargées de la gestion de la configuration du service DTP. Ils peuvent ajouter ou retirer une nouvelle application métier ou une compagnie d'une application métier. L'administration du service est effectuée par des opérateurs de Dictao. Le service n'offre aucune interface d'administration aux applications métiers et aux utilisateurs.

3.2.3 Interface de service

L'application métier utilise une interface de type Web Service qui permet de :

- Créer la transaction dans le système service DTP ;
- Ajouter un document à la transaction ;
- Ajouter des droits d'accès à la transaction ;
- Retrouver un document ;
- Annuler une transaction ;
- Archiver une transaction.

Cette interface applicative requiert une authentification par certificat pour son utilisation par l'application métier.

L'interface applicative n'est accessible qu'à travers un canal de communication sécurisé TLS avec authentification mutuelle par certificat.

L'ajout du contrat à la transaction provoque systématiquement l'application d'un cachet serveur garantissant l'intégrité du contrat dans les étapes suivantes de la contractualisation.

3.2.4 Interface utilisateur final

DTP propose une interface graphique à l'utilisateur final sous la forme de pages Web. Cette interface n'est accessible qu'à l'aide d'un jeton d'accès à usage unique demandé par l'application métier. Cette interface utilisateur expose les contrôles nécessaires aux utilisateurs finaux pour compléter la transaction avec leur signature électronique.

L'interface de signature de contrat permettent à l'utilisateur de visualiser les données de l'application métier, d'accéder à la politique de signature à travers un lien hypertexte, de lui donner son consentement par une case à cocher ainsi que l'acceptation explicite des clauses particulières.

La demande de signature est validée par la saisie d'un OTP transmis préalablement par SMS à l'utilisateur final par DTP.

Les pages Web à destination des utilisateurs finaux sont servies sur Internet à travers un canal de communication sécurisé suivant le protocole TLS qui garantit l'intégrité et la confidentialité des informations échangées.

Ainsi le contrat présenté à l'utilisateur pour la signature est celui qui sera signé par la plateforme DTP au nom de DTP.

3.2.5 Configuration du DTP (administration)

La gestion des applications métier, des clés et des paramètres est effectuée par les administrateurs. L'administration de la plateforme se fait à l'aide de fichiers sur le système d'exploitation. L'accès aux machines se fait par session à distance ssh lancée depuis un bastion sur la plateforme. L'accès au bastion se fait par bureau distant depuis le réseau de Dictao uniquement.

Dans les fichiers de configuration de la plateforme, l'enregistrement d'une nouvelle application consiste à :

- Ajouter un identifiant d'application ;
- Associer un certificat d'authentification ;
- Associer un bi-clef et un certificat de signature « cachet serveur » ;
- Associer une feuille de style en cascade pour l'affichage des pages hypertextes à destination des utilisateurs finaux ;
- Associer un ensemble de clauses particulières à présenter pour acception explicite de l'utilisateur final.

3.2.6 Preuve de transaction (utilisation)

DTP génère une preuve de transaction permettant de rejouer les étapes conduisant, d'un point de vue métier, à l'établissement du contrat entre l'application métier et l'utilisateur final.

La preuve de transaction se veut opposable en cas de contestation de la part d'une ou des parties du contrat établi.

En fin de transaction, la preuve est scellée afin de garantir son intégrité dans le temps.

Elle contient notamment :

- La preuve d'authentification de l'utilisateur final lors de sa demande de signature ;
- Le contrat signé par « cachet serveur » de l'application métier et par l'utilisateur ;
- La trace d'audit du système DTP.

La trace d'audit est construite par DTP à la suite de chacune des actions de l'application métier ou de l'utilisateur final.

Elle contient notamment:

- Les éléments d'identification de l'application métier, la date de création et, le cas échéant, la date de fermeture de la transaction ;

- Pour chaque action, le type (Création, Ajout de document, signature, fermeture, …) et la date d'action ;

- Dans le cas d'une signature, la référence dans le système de stockage vers le document signé.

Les preuves de transaction sont accessibles par l'application métier à travers un appel GetDocument.

3.3 Environnement technique

3.3.1 Description des hypothèses sur l'environnement

L'application métier est l'infrastructure logicielle chargée d'initier la transaction, d'ajouter les droits d'accès à la transaction et d'ajouter un ou plusieurs documents à la transaction. L'application métier est un élément de l'infrastructure de contractualisation que vient renforcer DTP.

La plateforme DTP est correctement dimensionnée pour supporter les contraintes opérationnelles issues de l'application métier (pas de risque de déni de service dû à une saturation des espaces de stockages, de bande passante ou de capacité de traitement).

DTP est livré par Dictao (ou un prestataire habilité) préinstallé et préconfiguré :

- la clef de scellement des preuves de transactions est générée et stockée dans un HSM livré avec le système.
- les applications métiers sont configurées dans DTP.
- l'OS est durci notamment par l'utilisation de deux comptes utilisateurs administrateurs machine (root) et exploitant DTP (oper). Le durcissement de l'OS consiste aussi en la modification de la configuration par défaut du système avec entre autres, la protection du redémarrage, la mise en place des protections CPU contre les attaques par débordement mémoire et la désactivation des démons non utilisés, entre autres.
- la version d'Apache installée est la version 2.2.15 et elle est à jour au niveau des patchs de sécurité[1].

L'exploitant DTP ne dispose que des accès aux fonctions d'exploitation (arrêt, redémarrage, téléchargement de logs techniques). L'utilisation de mots de passe forts (conformément à la note d'information CERTA-2005-INF-001) est recommandée.

Cette installation n'entre pas dans le périmètre d'évaluation dans la mesure où elle concerne l'ensemble de la plateforme et non seulement DTP.

[1] Cf. https://access.redhat.com/security/updates/backporting/

L'accès physique à la machine sur laquelle DTP est hébergé est supposé être contrôlé de manière à prévenir toute altération par ce biais.

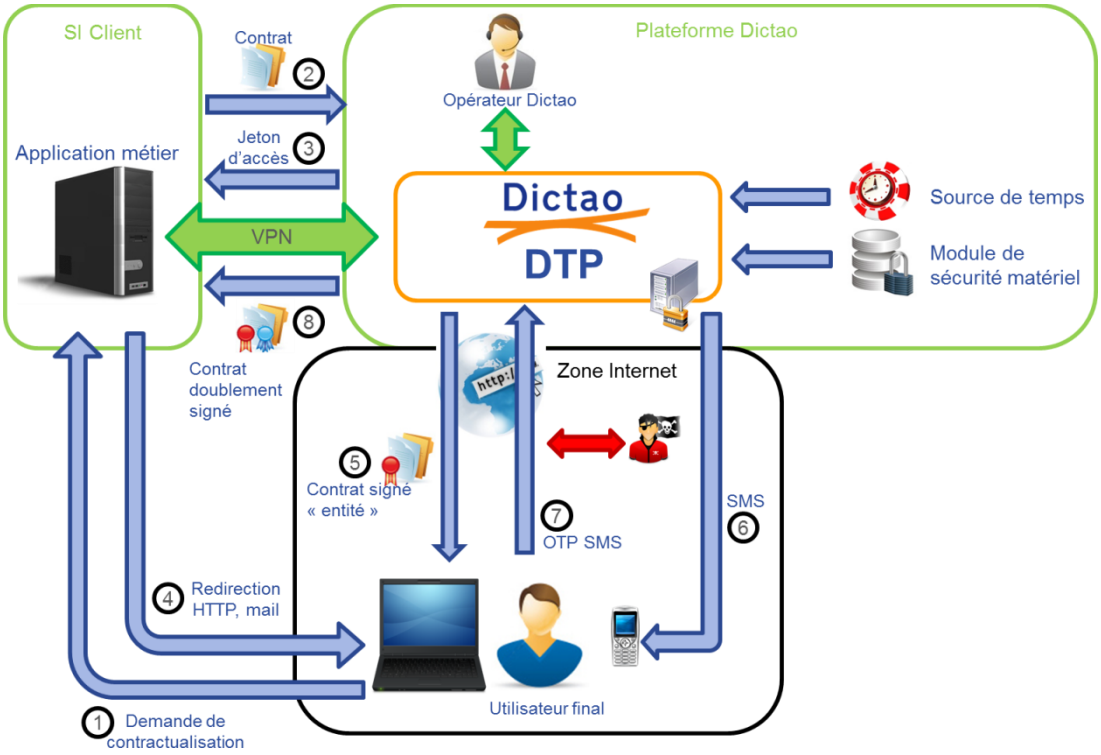
Dans le cas où DTP est mis à disposition sous la forme d'un service en ligne, cette hypothèse couvre les agents de Dictao que sont les administrateurs systèmes et les exploitants en charge des serveurs et du service DTP.

L'accès aux web services de la plateforme DTP se fait exclusivement via le protocole TLS à travers un réseau privé virtuel au standard IPSEC. Les accès sont ainsi autorisés uniquement pour un ensemble d'adresse IP en liste blanche pour des applications connues de Dictao.

3.3.2 Source de temps

La précision de l'horloge par rapport à laquelle DTP se synchronise pour dater les événements journalisés doit être inférieure à 1 seconde par rapport au temps UTC. Cette source de temps est supposée fiable.

3.3.3 Architecture



Cette figure présente les différents flux autour et au sein du service DTP. Les applications métiers accèdent à DTP via le protocole TLS avec authentification mutuelle par certificat. Les utilisateurs accèdent à l'application métier puis à DTP à travers Internet.

1. L'utilisateur final se connecte à l'application métier pour une demande de contractualisation via Internet ;
2. L'application métier envoie à DTP le document à signer par l'utilisateur final via le protocole TLS avec authentification mutuelle par certificat ;
3. L'application métier demande un accès utilisateur à DTP via le protocole TLS avec authentification mutuelle par certificat ;
4. L'application métier transfère le jeton d'accès à l'utilisateur final via une redirection HTTP ou via une URL fournie par mail ;
5. L'utilisateur se connecte sur l'interface utilisateur de DTP et visualise le contrat signé entité ;
6. L'utilisateur reçoit l'OTP via SMS ;
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.

3.4 Biens à protéger

3.4.1 Interface de l'utilisateur final

DTP doit permettre à l'utilisateur de vérifier que les données qui lui sont présentées à travers les pages hypertextes sont authentiques et n'ont pu être altérées.

3.4.2 Document à signer et preuve de transaction

DTP doit s'assurer des propriétés relatives à la sécurité du document à signer et à la preuve de transaction. Seuls l'application et l'utilisateur final ont accès aux informations et au contenu de ces documents.

La solution ne contrôle pas le contenu du document, ni sur le fond (légalité) ni sur la forme (stabilité sémantique, blanc sur blanc, police), mais garantit que toute altération du contenu du document par des éléments externes est détectable (intégrité des documents tout au long du processus de contractualisation jusqu'à la preuve de transaction).

3.4.3 Clés de signature

Cinq types de clés de signature sont hébergés et manipulés par DTP.

1. Les clés de signature pour le cachet serveur des applications métiers,
2. La clé de scellement pour le cachet serveur de DTP sur les preuves de transactions
3. La clé de signature de l'autorité de certification utilisée pour générer les certificats des utilisateurs finaux,
4. La clé de signature de l'autorité d'horodatage,
5. Les clés de signatures des utilisateurs finaux.

DTP doit s'assurer du contrôle exclusif de chaque clé par l'acteur qui lui est propre.

3.5 Menaces considérées

3.5.1 Vol de données

Un attaquant essaye depuis Internet d'accéder aux données d'une transaction qui n'est pas la sienne. Toutes les données de la transaction sont considérées comme sensibles à cette menace.

Cette menace est notamment présente dans les configurations de DTP comprenant plusieurs applications.

L'attaquant peut être une application tierce malveillante et inconnue de la plateforme ou une application métier légitime (enregistrée sur DTP) tentant d'accéder aux ressources d'une autre application métier légitime ou autres ressources servies par DTP.

3.5.2 Altération de transaction

Un attaquant essaye depuis Internet de modifier, annuler ou invalider le contrat. Toutes les données de la transaction sont considérées comme sensibles à cette menace.

L'attaquant peut être une application tierce malveillante et inconnue de la plateforme ou une application métier légitime (enregistrée sur DTP) tentant d'accéder aux ressources d'une autre application métier légitime.

3.5.3 Usurpation d'identité

Un attaquant essaye de signer électroniquement un document sous une identité empruntée.

Cette menace peut être illustrée par les cas frauduleux où un agent initie des transactions pour l'ensemble de son portefeuille client et procède à la signature des contrats pour ses clients afin d'accroitre artificiellement son activité.

L'attaquant peut être une application tierce malveillante et inconnue de la plateforme ou une application métier légitime (enregistrée sur DTP) tentant d'accéder aux ressources d'une autre application métier légitime.

4. FONCTIONS DE SECURITE

4.1 Authentification forte des applications par certificat

DTP authentifie fortement toutes les applications métiers qui utilisent l'interface applicative de manière à garantir la traçabilité des appels ainsi que l'intégrité et la confidentialité des informations transmises. Cette authentification est mise en œuvre suivant le protocole standard TLS par DTP.

DTP réalise également un contrôle d'accès aux ressources par application métier basé sur la correlation de ces ressources avec le certificat présenté.

Cette fonction de sécurité contribue à protéger le contrat à signer (3.4.2) contre les menaces « vol de données » 3.5.1 et « altération de données » 3.5.2 avant son entrée dans le système DTP.

4.2 Signature « cachet serveur » des documents déposés

DTP applique une signature cryptographique de type « cachet serveur » sur les documents déposés par les applications métiers.

Cette opération est réalisée à l'entrée des documents dans le système DTP et garantit leur intégrité tout au long du processus, jusqu'à restitution.

Cette fonction de sécurité contribue à protéger le contrat à signer (3.4.2) contre la menace « altération de données » 3.5.2 durant tout le cycle de la transaction dans le système DTP.

4.3 Service des pages d'affichage et de signature protégées requérant une authentification serveur

Les pages à destination de l'utilisateur et notamment la page présentant le contrat à signer sont servies à travers un canal sécurisé suivant le protocole standard TLS avec authentification du serveur par certificat qui garantit l'intégrité et la confidentialité des informations échangées.

Cette fonction de sécurité contribue à protéger l'interface utilisateur (3.4.1) contre les menaces « vol de données » 3.5.1 et « altération de données » 3.5.2.

Le service du contrat, portant un cachet serveur garant de son intégrité, à travers une communication sécurisée par le protocole standard TLS permet de garantir que les données

présentées sur le poste de l'utilisateur final n'ont pas été altérées et sont fidèles à la copie sur la plateforme DTP.

De plus, la page rendant le contrat sur le poste de l'utilisateur final exécute un script vérifiant qu'un plugin Adobe Reader est correctement installé. Si tel n'est pas le cas, alors un lien invite l'utilisateur final à le télécharger et l'installer avant de poursuivre l'étape de signature. Le bouton permettant la demande de signature est alors inactif.

4.4 Authentification des utilisateurs par OTP SMS

DTP authentifie les utilisateurs qui se présentent sur l'interface graphique de signature par l'intermédiaire d'un OTP SMS non rejouable.

La valeur de l'OTP est envoyée lors de la demande de création de signature par l'utilisateur final. C'est l'application métier qui transmet le numéro de téléphone de l'utilisateur à DTP.

La page demandant la valeur de l'OTP, ainsi que toutes les pages de l'interface graphique permettant la demande de signature électronique, sont servies suivant le protocole standard TLS avec authentification du serveur par certificat. Le processus d'authentification mène à la création d'une preuve d'authentification dans la preuve de transaction.

Cette fonction de sécurité contribue à protéger la clé de signature de l'utilisateur final (3.4.3) contre la menace « usurpation d'identité » 3.5.3.

4.5 Génération des clés et des certificats à usage unique pour les utilisateurs finaux

Après vérification de l'authentification de l'utilisateur, DTP déclenche la génération du bi-clé et la signature de la requête de certification par le module de confinement matériel.

La signature est elle aussi réalisée par le module de confinement matériel.

Après signature, DTP demande l'effacement de la clé signature par le module de confinement matériel.

Le certificat associé à la clé de signature de l'utilisateur final a une durée de vie de 60 secondes.

Ces mécanismes permettent d'assurer le contrôle exclusif du moyen de signature par le signataire.

Cette fonction de sécurité contribue à protéger la clé de signature de l'utilisateur final (3.4.3) contre la menace « usurpation d'identité » 3.5.3.

4.6 Signature des preuves de transaction

La preuve associée à une transaction est scellée électroniquement à la fin de la transaction ou à son annulation. Cette signature permet de constituer une preuve de transaction garantie en intégrité.

Cette fonction de sécurité contribue à protéger la preuve de transaction (3.4.2) contre la menace « altération de données » 3.5.2.

5. COMPLEMENTS TECHNIQUES

DTP utilise des mécanismes de signature utilisant des algorithmes asymétriques respectant les normes et standards cryptographiques.

Les signatures électroniques du contrat répondent aux critères suivants :

- Format de l'enveloppe de signature : **PAdES Part 2**
- Algorithme de hachage : **SHA256**
- Algorithme de signature : **RSA avec SHA256**

Les modules de sécurité matériels sont de modèle NCipher 1500.

La signature de la trace d'audit répond aux critères suivants :

- Format de l'enveloppe signature : **XAdES-T**
- Algorithme de hachage : **SHA256**
- Algorithme de signature : **RSA avec SHA256**

La génération de jeton d'horodatage est conforme à la **RFC3161**.

La génération des certificats à usage unique répond aux critères suivants :

- Algorithme de signature : **RSA avec SHA1**
- Durée de validité : **60 secondes**

Les aléas sont générés par les modules de sécurité matériels NCipher 1500.

Le VPN est mis en place à l'aide d'un boitier spécialisé Cisco ASA 5520 VPN+.

L'authentification par OTP SMS est réalisée à l'aide du produit Dictao Validation Server, embarqué dans la solution DTP. L'OTP SMS présente les caractéristiques suivantes :

- il se compose de 6 caractères numériques ;
- il a une durée de vie de 1200 secondes ;
- le compte utilisateur associé est bloqué au bout de 3 tentatives erronées successives de saisie de l'OTP pendant 3600 secondes, soit une durée garantissant l'expiration de l'OTP.