Dictao

152, avenue de Malakoff
75116 Paris

Cible de sécurité C.S.P.N.
Coffre-fort électronique D3S

CSPN D3S

Réf. : dictao_d3s_cible_cspn
Version 1.24 du 19 nov. 2010

Référence :	dictao_d3s_cible_cspn
Version :	1.24
Date de dernière mise à jour :	19 nov. 2010
Niveau de confidentialité :	Communication, reproduction ou utilisation interdites sauf autorisation préalable de Dictao

Diffusion

Destinataires	Objet de la diffusion
ANSSI ARJEL 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	T	1 fév. 2010	SLA	Version validée
1.1	T	22 fév. 2010	SLA	Mise à jour des menaces
1.2	T	29 mars 2010	Dictao	Signature configuration
1.21	T	6 avr. 2010	Dictao	Ajouts mineurs
1.22	T	4 nov. 2010	Dictao	Précisions sur les droits utilisateurs
1.23	T	16 nov. 2010	Dictao	Précisions sur les menaces
1.24	T	19 nov. 2010	Dictao	Ajustement confidentialité

[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 coffre-fort numérique ***Dictao Secure Storage Server*** (**D3S**) pour son homologation par l'Agence nationale de la sécurité des systèmes d'information. Les fonctions de sécurité décrites ici, proches des exigences de l'Autorité de régulation des jeux en ligne (ARJEL), sont toutefois susceptibles de répondre à de nombreux autres cas d'usages et ne se limitent pas aux seules exigences afférentes aux jeux en ligne.

1.1 Vocabulaire

- **Armoire**

Une armoire est un ensemble de coffres dédiés à un groupe d'utilisateurs identifiés.

- **Autorité**

Terme abstrait pour désigner l'organisme chargé d'auditer les traces.

- **Coffre**

Un coffre est l'espace de stockage élémentaire de D3S : c'est au sein d'un coffre que sont stockées les pièces numériques et qu'est assurée la traçabilité des opérations relatives à celui-ci.

- **Dépôt**

Acte d'ajouter une ou plusieurs pièces numériques dans **D3S**. Tout dépôt donne lieu à la génération d'une preuve de dépôt permettant d'assurer l'auditabilité des opérations effectuées et la restitution des dépôts aux rôles habilités.

- **Enveloppe**

On parle d'enveloppe pour désigner une pièce numérique sous forme chiffrée.

- **Export**

L'export consiste à sortir du **D3S** les enveloppes (pas de déchiffrement des données, contrairement à la restitution (voir ci-dessous)).

- **Opérateur**

Organisation auditée par l'autorité.

- **Pièce numérique**

Une pièce numérique est constituée des données déposées dans le coffre au cours d'une opération de dépôt. Le fonctionnement du coffre-fort est indépendant de la nature et du format de ces données, et son rôle est d'en assurer l'intégrité et la confidentialité.

Toute pièce numérique est identifiée de manière unique dans **D3S**.

Aussi appelé « paquet d'information archivé » selon le cahier des charges de l'A.N.S.S.I. (réf. SGDN/DCSSI/SDO/BCS).

➢ Preuve de dépôt

Afin d'assurer la traçabilité des opérations effectuées (au minimum, dépôts et retraits), le coffre-fort conserve, pour chaque dépôt, un certain nombre d'informations permettant, par exemple, d'imputer le dépôt à un utilisateur donné, vérifier l'ordre de ces opérations, etc.

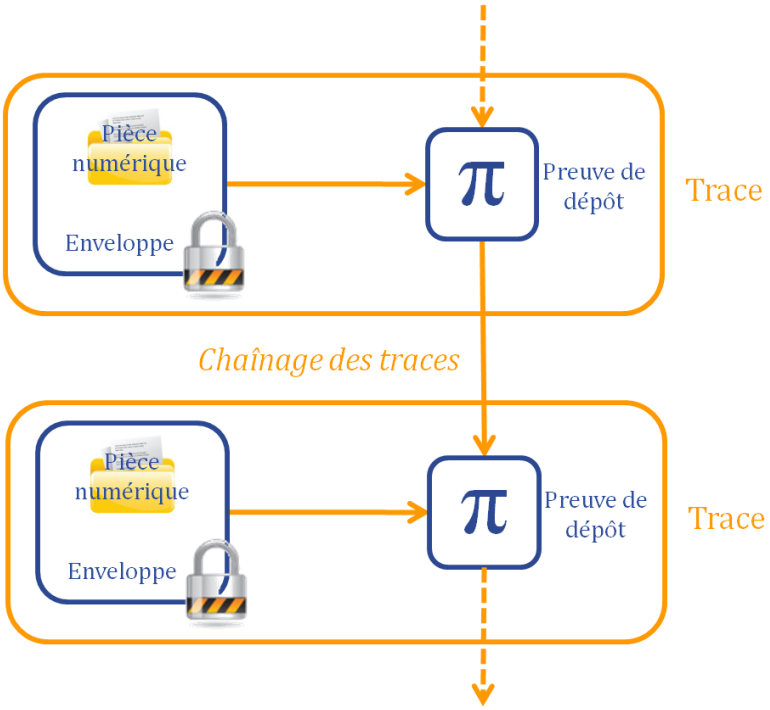
Ces informations sont appelées « preuves » tout court lorsqu'aucune confusion n'est à craindre.

➢ Restitution

Acte de lecture (accès aux données) d'une ou plusieurs pièces numériques précédemment déposées. La restitution implique le déchiffrement de l'enveloppe contenant la pièce (lecture et accès aux données).

➢ Trace

Une trace est constituée d'une enveloppe et de sa preuve de dépôt associée.



2. IDENTIFICATION DU PRODUIT

Organisation éditrice	Dictao
Lien vers l'organisation	www.dictao.com
Nom commercial du produit	*Dictao Secure Storage Server (D3S)*
Numéro de la version évaluée	4.4
Catégorie de produit	9 – Stockage sécurisé

3. ARGUMENTAIRE

Le contexte d'utilisation correspond à la surveillance des activités transactionnelles d'une entité ci-nommée « opérateur » par une « autorité ». L'autorité souhaite contrôler certaines opérations au sein du système d'information de l'opérateur et installe à cette fin chez ce dernier un dispositif technique chargé de recueillir et d'archiver des traces de ces opérations.

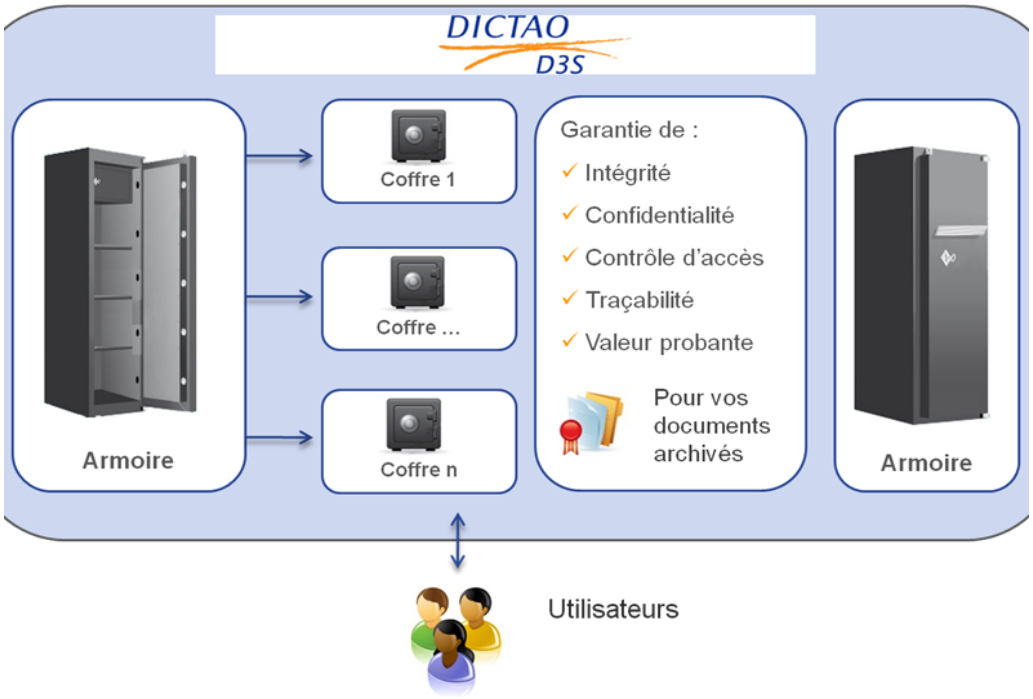
D3S est un composant de ce dispositif technique chargé de garantir la traçabilité des opérations effectuées sur le système d'information. Ce dispositif est constitué d'un capteur et du **D3S**. Le capteur, hors du périmètre du présent document, est chargé de récolter les données tracées. Ces données sont ensuite archivées dans le coffre-fort numérique 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 tout ajout, suppression ou modification de transaction détectable.

Le support de stockage ne fait pas partie du **D3S** en ce sens que les propriétés de sécurité (confidentialité, intégrité, chaînage) des données contrôlées par le coffre-fort sont indépendantes du système de stockage (système de fichiers, base de données…).

3.1 Description fonctionnelle

D3S est organisé suivant le principe d'une **salle des coffres physique** : on y trouve des **armoires**, ces armoires contenant elles-mêmes un ou plusieurs **coffres**.

Chacun des coffres peut être soit vide, soit contenir une ou plusieurs **pièces numériques**.



3.2 Utilisation du produit

D3S est supposé être installé et configuré dans le cadre d'un processus contrôlé (voir ci-après pour les détails de la mise en production du **D3S**).

D3S s'appuie sur un support de stockage et, raisonnablement, sur un confinement matériel des secrets cryptographiques qu'il utilise (scellement). Ces secrets sont identifiés en section 3.4.

3.2.1 Utilisateurs et profils

Une fois installé, **D3S** interagit avec différents utilisateurs, auxquels sont associés différents profils :

- Le déposant : il s'agit du client applicatif (logiciel) chargé de récupérer les données à tracer. Cet utilisateur s'authentifie auprès du **D3S** avec un profil « ***déposant*** ».
- Les agents dotés des pouvoirs de contrôle et d'audit. Ceux-ci s'authentifient auprès du **D3S** avec un profil « ***lecteur*** ». Il peut s'agir de personnes physiques ou de logiciels.
- Les agents (personnes physiques) chargés de la gestion des profils. Ceux-ci s'authentifient auprès du **D3S** avec un profil « ***administrateur*** ».

Profil	Utilisateur	Opérations et droits
Déposant	Capteur	❑ Dépôt de pièces numériques ❑ Vérification de l'intégrité et de la complétude des preuves de dépôt
Lecteur	Agent d'audit et de contrôle	❑ Récupération des pièces numériques chiffrées (export) ❑ Vérification de l'intégrité et de la complétude des preuves de dépôt
Administrateur	Autorité	❑ Paramétrage initial du coffre

Le **D3S** permet de configurer plusieurs « coffres » distincts (espaces de stockage), chaque coffre ayant un ensemble d'utilisateurs et de profils potentiellement cloisonnés : droits, profils et utilisateurs s'entendent par coffre.

Par ailleurs, les personnels techniques (personnes physiques) chargées de l'exploitation du **D3S** au quotidien, qu'il s'agisse de personnes dépendant de l'opérateur ou d'un prestataire, interagissent de façon indirecte sur le **D3S** et son environnement (réseau, matériel, démarrage et redémarrage de la plate-forme, etc.). Ces personnels n'ont pas de profil associé ni de rôle fonctionnel vis-à-vis du **D3S**.

Les actions autorisées pour chaque profil sont distinctes (cloisonnement des rôles). Ainsi, par exemple, un lecteur ne peut pas déposer de pièces et, réciproquement, un déposant n'est pas en mesure de lire une quelconque pièce numérique.

3.2.2 Configuration du D3S (administration)

La gestion des profils, des clés et des différents paramètres du **D3S** est effectuée par les administrateurs.

Un administrateur n'a aucun droit sur le contenu des coffres.

3.2.3 Dépôt (utilisation)

En fonctionnement courant, les « déposants » s'authentifient après du **D3S** et y déposent des pièces numériques. Le dépôt d'une pièce numérique dans le **D3S** se déroule comme suit :

1. Chiffrement de la pièce (création de l'enveloppe)
2. Génération et scellement de la preuve de dépôt associée (création de la trace)

Un déposant ne peut ni lire les pièces déposées (y compris siennes) ni accéder à la configuration du **D3S**. Il peut accéder aux preuves des pièces qu'il a déposées.

3.2.4 Audit (utilisation)

En fonctionnement courant, les utilisateurs « lecteurs » s'authentifient après du **D3S** et accèdent au enveloppes (export des données non déchiffrées) des pièces numériques déposées et aux preuves associées. Un lecteur ne peut ni modifier les pièces déposées ni accéder à la configuration du **D3S**.

3.3 Environnement technique

3.3.1 Matériel et logiciel

D3S s'appuie sur les éléments suivants :

- un support de stockage (disques, base de données, etc.) sur lequel sont enregistrées les enveloppes et les preuves de dépôt.
- un confinement matériel (*hardware security module*) des secrets cryptographiques (en particulier, la clé de signature utilisée pour le scellement des pièces et des traces)
- une source fiable de temps

3.3.2 Description des hypothèses sur l'environnement

➢ Capteur

Le capteur est l'infrastructure logicielle et matérielle chargée de capter et déposer les traces correspondant à l'activité du déposant (opérateur). Ce capteur est supposé être homologué indépendamment afin de démontrer son bon fonctionnement. Par conséquent, ce capteur est supposé être de confiance, ce qui comprend les hypothèses suivantes :

- Le capteur ne soumet que des pièces authentiques (correspondant à des transactions réelles et non, par exemple, des données aléatoires ou à des opérations factices)
- La plate-forme capteur-D3S est correctement dimensionnée pour supporter les contraintes opérationnelles de l'opérateur (pas de risque de déni de service dû à une saturation des espaces de stockage, de bande passante ou de capacité de traitement)
- Le capteur interprète les réponses (ou l'absence de réponse) du D3S de façon à resoumettre, le cas échéant, un dépôt dont il n'a pas reçu d'accusé de réception.

➢ Clé de déchiffrement

La clé (privée) de déchiffrement des dépôts d'un opérateur, c'est-à-dire de ses capteurs, ne peut en aucun cas être communiquée à l'opérateur. Cette clé est entièrement contrôlée par l'autorité émettrice et est stockée de manière sécurisée dans un HSM. Seuls les agents dotés des pouvoirs de contrôle et d'audit ont la possibilité d'utiliser cette clé.

Le déchiffrement des pièces numériques ne fait pas partie du périmètre d'évaluation.

➢ Installation et initialisation

Le **D3S** est livré par l'autorité (ou un prestataire habilité) préinstallé et préconfiguré pour un opérateur donné.

- La clef de scellement des preuves est générée et stockée dans un HSM (*hardware security module*) livré avec le système. L'opérateur ne dispose pas des secrets permettant de configurer ce module.
- La clef de chiffrement est configurée de manière applicative (clé publique).
- Les utilisateurs et leurs profils sont configurés. L'opérateur ne dispose que d'un profil déposant.
- L'OS est durci par l'utilisation de deux comptes utilisateurs administrateur machine (root) et exploitant D3S (oper). L'exploitant D3S ne dispose que des accès aux fonctions d'exploitation (arrêt, démarrage, téléchargement des logs techniques). L'utilisation de mots de passe forts (conformément à la note d'information CERTA « CERTA-2005-INF-001 ») est notamment recommandée.
- Les identifiants et mots de passe « root » ne sont pas communiqués aux opérateurs.

- Les identifiants et mots de passe « oper » sont communiqués aux opérateurs.

Cette installation n'entre pas dans le périmètre d'évaluation dans la mesure où elle concerne l'ensemble de la plate-forme et non seulement le coffre.

➢ Protection physique

L'accès physique à la machine sur laquelle **D3S** est hébergé est supposé être contrôlé de manière à prévenir toute altération par ce biais.

Dans le cas où le **D3S** est mis à disposition sous forme de service en ligne, cette hypothèse couvre les administrateurs systèmes en charge du maintien en condition opérationnelle des serveurs qui hébergent le service.

➢ Source de temps

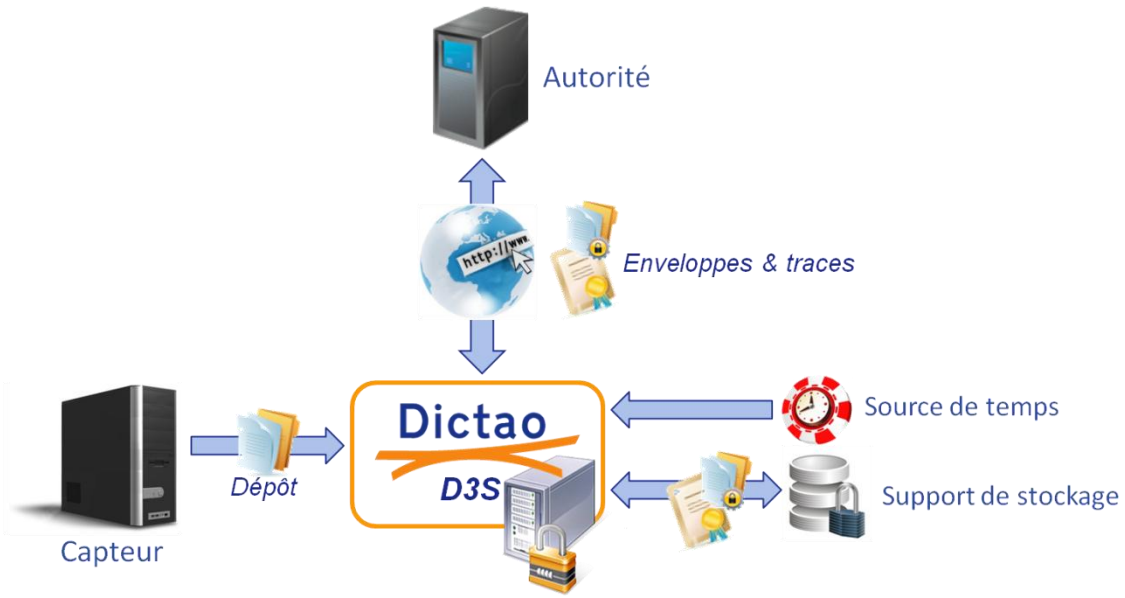
La précision de l'horloge par rapport à laquelle **D3S** se synchronise pour dater les événements journalisés ou archivés doit être inférieure à 1 seconde par rapport au temps UTC. Cette source de temps est supposée fiable.

➢ Opérations témoins

On suppose que l'autorité procède à des contrôles réguliers relatifs au bon fonctionnement des plates-formes homologuées. En particulier, cette autorité génère elle-même des opérations, dites « opérations témoins », en amont du capteur à seule fin de constater la présence des traces associées dans le coffre-fort.

Cette mesure a pour objectif de détecter toute tentative de contournement, par l'opérateur, de l'enregistrement des traces d'opérations par la plate-forme (détournement de flux, mise en place d'un site parallèle, etc.).

3.3.3 Architecture



3.4 Biens à protéger

➢ Données de configuration du D3S

Ces données couvrent notamment les profils des utilisateurs et la clé (publique) de chiffrement. Seuls les administrateurs du **D3S** peuvent modifier la configuration du **D3S**. Ce bien est à protéger en intégrité.

➢ Traces

D3S doit assurer deux principales propriétés relatives à la sécurité des traces qu'il conserve :

- D'une part, seuls les profils habilités ont accès aux éléments déposés (confidentialité du contenu des enveloppes)
- Toute altération d'une enveloppe est détectable (intégrité des dépôts)
- D'autre part, on doit pouvoir contrôler l'intégrité et l'exhaustivité des preuves de dépôt. L'intégrité concerne les preuves individuelles, tandis que l'exhaustivité désigne l'intégrité de la séquence de ces preuves (chaînage). Nul ne doit pouvoir effacer, modifier ou insérer une trace sans que ce ne soit détectable.

3.5 Menaces considérées

➢ Dépôt de traces factices

L'opérateur effectue des dépôts dans **D3S** autrement que par le biais du capteur. L'objectif peut être de saturer l'espace de stockage des traces pour masquer des opérations frauduleuses subséquentes (qui ne seraient ainsi pas tracées). Pareillement, ces dépôts peuvent eux-mêmes servir simuler une activité inexistante.

➢ Injections de traces factices

L'opérateur ajoute ou modifie directement le contenu de l'espace de stockage. Il s'agit de la même attaque que précédemment, mais effectuée sur l'espace de stockage plutôt que sur l'interface de dépôt.

➢ Vol de données

Un attaquant accède à l'espace de stockage et en extrait des données relatives à l'activité de l'opérateur.

➢ Effacement des traces

Un attaquant accède à l'espace de stockage et y supprime des enregistrements.

➢ Altération de la configuration

Une personne non autorisée (c.-à-d. autre qu'un administrateur **D3S**) modifie la configuration du **D3S**. Cette attaque est essentiellement un préalable à la réalisation des autres menaces.

Techniquement, l'altération de la configuration revient à une ***prise de contrôle*** du coffre-fort par l'attaquant : si l'attaquant peut modifier la configuration à son gré, il est susceptible de modifier les paramètres critiques du coffre-fort.

4. FONCTIONS DE SECURITE

4.1 Authentification forte des utilisateurs par certificat

D3S authentifie fortement tous les utilisateurs de manière à assurer l'intégrité de sa configuration et l'authenticité des dépôts (seul un profil « déposant » peut ajouter une trace dans **D3S**, en l'occurrence, compte tenu des hypothèses sur l'initialisation de la plate-forme, seul le capteur est habilité à effectuer des dépôts). Toute personne (ou système) souhaitant accéder au coffre-fort numérique est identifiée et authentifiée fortement par certificat.

Enfin, **D3S** sécurise les flux entre le client et lui-même en mettant en œuvre le protocole standard TLS. La mise en œuvre de TLS/SSL par le serveur **D3S** assure :

- L'authentification mutuelle forte des parties (serveur **D3S** et appelant) par certificat
- Le contrôle de l'intégrité des flux
- La confidentialité des données échangées

4.2 Chaînage des traces

Nul ne doit pouvoir effacer, modifier ou insérer une trace sans que ce ne soit détectable. Cette fonction assure donc le chaînage des différentes traces déposées : chaque trace est cryptographiquement liée à la trace qui la précède chronologiquement via le chaînage des preuves de dépôt associées aux traces.

Ce chaînage assure les propriétés suivantes :

- D'une part, la preuve de dépôt est intègre ; toute modification d'une preuve est détectable.
- D'autre part, toute modification de la suite des preuves (effacement, insertion, déplacement ou ajout) est détectable.

Remarque : en supposant que l'attaquant dispose d'un accès et des droits suffisants sur l'espace de stockage, il peut néanmoins supprimer les enveloppes et les preuves associées à partir « de la fin de la chaîne », voire tout effacer (un espace de stockage vierge est intègre et correctement chaîné). Cette attaque fait partie des risques assumés dans la mesure où plusieurs éléments contribuent à en amoindrir les effets et la possibilité de réalisation.

- Tout d'abord, l'attaquant doit disposer des droits et des accès nécessaires.
- Ensuite, le contexte d'utilisation du produit implique un volume d'opérations important, et toute intervention de ce type sur l'espace de stockage sans que cela ne brise le chaînage (il faut effacer la dernière trace avant que la trace suivante ne soit enregistrée par la plate-forme) est complexe à mettre en œuvre. La solution consistant à arrêter la plate-forme ou interrompre le flux en amont du capteur est détectable au niveau des dates des traces.
- Enfin, une telle manipulation est susceptible d'effacer une « opération témoin », ce qui sera alors détecté (voir l'hypothèse sur les opérations témoins).

4.3 Chiffrement et scellement des dépôts

D3S chiffre toutes les données déposées dans un coffre donné avec une clé publique de chiffrement définie dans la configuration. Cette enveloppe chiffrée est restituée telle quelle lors de l'export par un utilisateur autorisé. Le déchiffrement de l'enveloppe ne peut se faire que sur le poste local de ce dernier, à condition qu'il possède la clé privée idoine.

De plus, l'intégrité des pièces numériques déposées est assurée par un mécanisme de signature électronique (scellement). Ainsi,

- Une preuve de dépôt est générée et signée lors de la mise au coffre de la pièce numérique (dépôt)
- La signature de cette preuve est validée lors de la restitution de la pièce numérique (audit/retrait)

Cette preuve peut être retournée à l'utilisateur ou au module externe effectuant le dépôt.

4.4 Signature de la configuration

La configuration du coffre est décrite dans un fichier signé. Ce fichier contient les droits d'accès pour chacun des utilisateurs du système. La signature de ce fichier est vérifiée à la première demande d'autorisation de dépôt.

4.5 Compléments techniques

4.5.1 Algorithmes utilisés

D3S propose des mécanismes de chiffrement et de déchiffrement sûrs utilisant des algorithmes symétriques et asymétriques respectant les normes et standards cryptographiques.

➢ Signature

D3S respectent les formats de signature sont les suivants :

- Format de l'enveloppe signature : **XAdES**
- Algorithme de hachage : **SHA512**
- Algorithme de signature : **RSA avec SHA256**

➢ Chiffrement

Les mécanismes de chiffrement sont les suivants :

- Format de l'enveloppe chiffrée : **XMLEnc**
- Algorithme de chiffrement symétrique : **AES**
- Algorithme de chiffrement asymétrique : **RSA**