IDEMIA Identity & Security France
2, Place Samuel de Champlain
92400 Courbevoie
France

Politique de signature et de validation de signature de Dictao

Signature Cachet

Réf. : dictao_IGC_PSV
Version 1.1 du 10/04/2019

Référence : **Version :** **Date de dernière mise à jour :**	dictao_IGC_PSV 1.1 10/04/2019
Niveau de confidentialité :	DIFFUSION RESTREINTE

Diffusion

Table des mises à jour du document

N° de version	Etat[1]	Date	Auteur	Objet de la mise à jour
0.1	T	11/02/14	DICTAO	Création
1	V	05/03/14	DICTAO	Publication
1.1	V	10/04/19	IDEMIA	Mise à jour de la raison sociale

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

SOMMAIRE

1. OBJET DU DOCUMENT

La signature électronique apposée sur un ensemble de données permet de garantir l'intégrité de ces données et l'authenticité de leur émetteur.

Une politique de signature et de validation est un document décrivant les règles à suivre pour créer et valider des signatures électroniques dans le cadre de transactions électroniques.

Ces politiques ont été élaborés en s'appuyant sur les recommandations du document ETSI TR 102 041 – V1.1.1: Signature Policies Report.

Ce document s'organise de la façon suivante :

- Chapitre 1 : Objet du document, le présent chapitre
- Chapitre 2 : Champ d'application
- Chapitre 3 : Obligations et recommandations générales
- Chapitre 4 : Politique de signature 'Cachet'
- Chapitre 5 : Politique de validation de signature 'Cachet'

2. CHAMP D'APPLICATION

2.1 Préambule

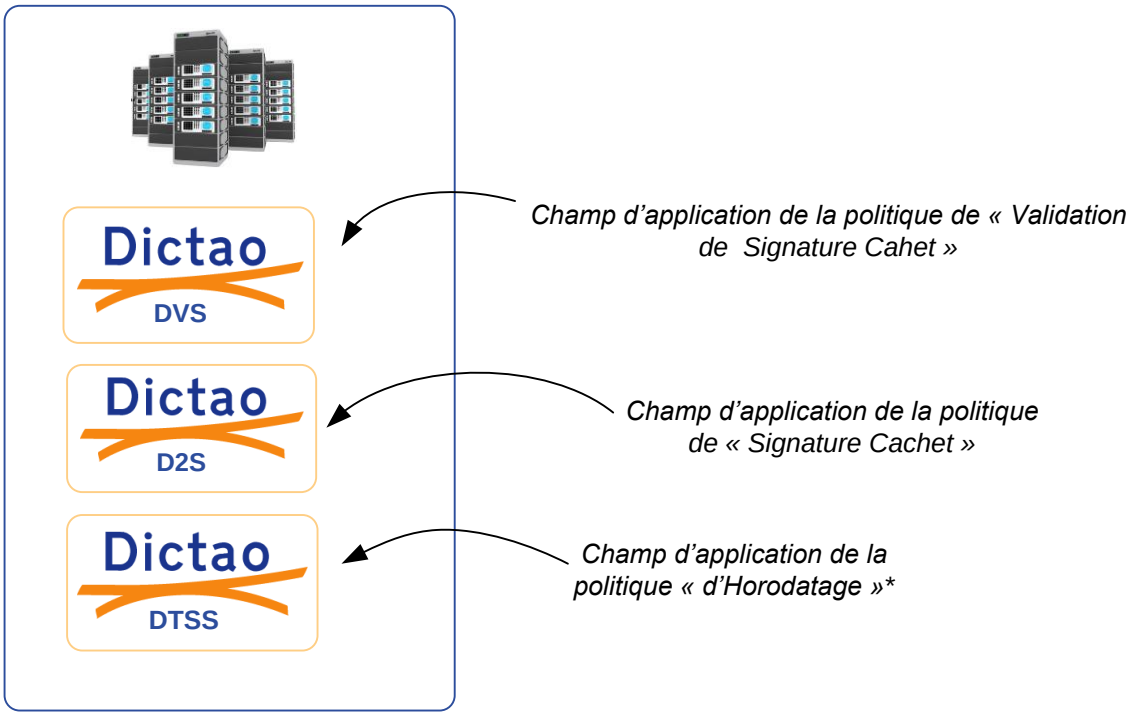
Nous vous informons que la dissolution et de la transmission universelle de patrimoine de la société Dictao à la société Idemia Identity & Security France, société par actions simplifiées, dont le siège social est domicilié au 2 Place Samuel de Champlain, 92400 Courbevoie, immatriculé au RCS de Nanterre, sous le numéro 440 305 282, est effective depuis le 2 Janvier 2015.

Suite à cette dissolution avec transmission universelle de patrimoine, l'ensemble des contrats conclus par Dictao avec ses clients et prestataires ont été transmis à Idemia Identity & Security France (société appartenant au groupe IDEMIA et dénommé comme tel par la suite), qui lui a succédé tant aux titres de ses droits que ses obligations, dans le strict respect des conditions contractuelles.

La présente politique de signature & de validation de signature s'applique aux :

- Processus de création de Signature Cachet pouvant être au nom
  - De IDEMIA
  - D'un client de IDEMIA
- Processus de validation de signature de « Signature Cachet » et de création des « Preuves de Validation » au nom de IDEMIA.

Les schémas ci-dessous mettent en évidence le lien entre les différentes briques composant le socle de signature et de validation de signature décrites dans le présent document.



Note : Les politiques décrites dans le présent document font référence à l'utilisation de données horodatées. Les contremarques de temps sont générées conformément à la politique d'horodatage de IDEMIA publiée sous la référence 1.2.250.1.195.7.4.1.1 ci-après intitulée « PH-Dictao ».

2.2 Identification du document et Date d'émission

Le présent document a été publié le 10 avril 2019 sous l'OID 1.2.250.1.195.7.4.1.1.

2.3 Période de validité

Le présent document entre en vigueur 3 jours ouvrés après la date de distribution ou de mise en ligne. Il reste en vigueur (sauf mention du contraire) tant que les services de signature électronique et de validation sont disponibles.

2.4 Mise à jour du document

2.4.1 Organisme responsable

Le présent document est maintenu par l'entité Digital Lab de IDEMIA.

Elle peut être contactée à l'adresse :

Idemia Identity & Security France,

2 Place Samuel de Champlain 92400 Courbevoie,

Coordonnées: info@idemia.com - Tél. : +33 1 73 60 20 20

2.4.2 Personnes physiques responsables

Le comité sécurité de l'entité Digital Lab de IDEMIA est responsable du présent document.

2.4.3 Procédure

La mise à jour du présent document implique la présence de plusieurs acteurs et est déclenchée essentiellement pour :

- Procéder à des modifications importantes,
- Prendre en compte de nouveaux besoins ou de nouveaux acteurs,
- Améliorer un cadre juridique,
- Améliorer la qualité du document.

Les versions publiées du présent document peuvent être signées par (au moins) l'une des personnes physiques responsables du document ; cette signature est effectuée à l'aide du certificat personnel de la personne physique responsable et est au format PDF.

Toute publication d'une nouvelle version du document consiste à archiver l'ancienne version et distribuer et mettre en ligne les éléments suivants :

- Document au format PDF

- OID du document
- Empreinte du document
- Date et heure exacte d'entrée en vigueur

2.4.4 Cohérence documentaire

Le document décrit le contexte de production des signatures de IDEMIA, et de leur validation.
Il revient au comité d'approbation de faire en sorte que ce document reste cohérent vis-à-vis de la politique de certification de l'autorité de certification de type « cachet » et les certificats identifiés par les OID 1.2.250.1.195.3.1.1.1 et 1.2.250.1.195.3.1.2.1, notamment en ce qui concerne la signature des preuves horodatée.

Les politiques définies par le présent document s'appuient sur la PH-Dictao qui décrit le contexte de production des contremarques de temps.
Il revient au comité d'approbation de s'assurer que le présent document reste cohérent vis-à-vis de la PH-Dictao en particulier en ce qui concerne la précision de l'horodatage.

2.4.1 Publication et consultation

IDEMIA se doit de tenir ces politiques à l'usage des utilisateurs de fonctions de signature ou de son service de validation de signature.
Ce document peut être distribué à ses utilisateurs finaux, soit par courrier électronique soit en le mettant en ligne.

Cette politique est publiée à l'adresse : http://trust.dictao.com/psv.html

Les informations relatives à la version courante du document et aux versions antérieures sont disponibles, pour les personnes autorisées, à l'adresse disponible au paragraphe 2.4.1, où une rubrique documentaire référence toutes les versions précédentes de ce document.

2.5 Données nominatives

Aucune donnée à caractère personnelle n'est enregistrée par les services de signature et de validation de IDEMIA.

2.6 Politique de confidentialité

Les informations suivantes auxquelles il peut être fait référence dans le présent document sont considérées confidentielles :

- Les données secrètes associées au certificat (clé privée, mot de passe, …)
- Les journaux des composants serveur (traces d'activité)
- Les rapports d'audit

3. OBLIGATIONS ET RECOMMANDATIONS GENERALES

3.1 Obligations appliquées aux signataires

3.1.1 Sécurité du poste client ou serveur

Le serveur à partir duquel une signature est produite ou demandée doit être protégé contre les virus, chevaux de Troie et autres logiciels malicieux susceptibles d'altérer le processus de signature (modification des données signées à l'insu du signataire, etc.). La responsabilité de cette protection en incombe au Directeur des Systèmes d'Information de IDEMIA.

3.1.2 Sécurité des clés de signature cahet

Les clés de signature sont stockées soit sur des Boitiers cryptographiques opérés par IDEMIA. Les clés de signature et leurs données d'activation sont gérées en conformité avec la politique de certification de l'AC Service pour les certificats référencés par l'OID 1.2.250.1.195.3.1.1.2.

En cas de compromission, le signataire doit immédiatement en avertir les responsables du service de signature afin que son accès à celui-ci soit fermé et/ou le certificat révoqué.

3.1.3 Données d'authentification

Le signataire (application interne de IDEMIA) doit s'assurer que les données qu'il utilise pour s'authentifier auprès du service de signature restent sous son contrôle exclusif (confidentialité).

En cas de compromission, il doit immédiatement en avertir les responsables du service de signature afin que son accès à celui-ci soit fermé et/ou le certificat révoqué.

3.1.4 Publication des CRL

Certaines données, notamment les listes de révocations, ne peuvent être mises à jour en temps réel et il s'écoule plusieurs heures (24 au maximum) avant la publication de ces données par l'entité responsable (l'autorité de certification, dans le cas d'une liste de révocation).

Dans ces conditions, il se peut qu'une signature soit déclarée valide si les données ont été signées entre le moment où le certificat a été révoqué et le moment où sa révocation a été publiée par l'autorité de certification et prise en compte par le service.

La publication des CRL est décrite dans la DPC de l'AC Service.

3.1.5 Limites de responsabilité

Le service de signature de IDEMIA n'est pas responsable du contenu des données signées.

3.2 Obligations appliquées à l'infrastructure de confiance

3.2.1 Sécurité

Les serveurs de signature et de validation de IDEMIA sont les éléments les plus sensibles de la cinématique de signature. Il est donc nécessaire de limiter l'accès physique et technique à ces serveurs et aux informations qu'ils contiennent aux seules personnes ayant des droits adéquats.

Les mesures prises concernent :

- La protection des accès physiques aux serveurs
- Le choix d'un environnement d'hébergement adapté en termes de disponibilité aux exigences des clients de IDEMIA (réseaux de climatisation et d'alimentation électrique secourus, systèmes de détection et d'extinction automatique de départs de feu, etc.)
- L'accès aux systèmes de signature et de validation de signature est restreint aux seules personnes habilitées. Le nombre de personnes ayant accès aux serveurs de signature et de validation est strictement limité et ces personnes sont identifiées et authentifiées.
- La surveillance de la plate-forme de IDEMIA est assurée en vue de prévenir les tentatives de compromission, d'intrusion physique ou par les réseaux de télécommunications
- Le stockage des clés de signature des serveurs est effectué sur un boîtier cryptographique.

3.2.2 Administrateurs de la plate-forme de IDEMIA

Les administrateurs de la plate-forme de IDEMIA et de ses composants doivent s'assurer que les données qu'ils utilisent pour s'authentifier auprès du service de signature ou de validation restent sous leur contrôle exclusif (confidentialité). En cas de compromission, ils doivent immédiatement en avertir le RSSI de IDEMIA afin que leur accès à celle-ci soit fermé ou modifié.

En cas de compromission, il leur est demandé de révoquer immédiatement leur certificat d'authentification et/ou de signature et de procéder à une nouvelle demande.

3.2.3 Reprise en cas de sinistre

En cas d'un incident quelconque ayant pu affecter le processus de signature ou de validation, qu'il s'agisse d'un incident technique ou d'une action mal intentionnée, prouvée ou supposée, l'entité Digital Lab de IDEMIA doit vérifier l'impact de cet incident sur le traitement des demandes de signature ou de validation en cours.

3.3 Recommandations aux destinataires

3.3.1.1 Vérifications complémentaires

Les services de signature cachet vérifient la validité des signatures des documents lorsque celles-ci sont produites.

Néanmoins, il appartient aussi au destinataire du document signé de vérifier la validité de la signature électronique conformément à ce document.

3.3.1.2 Période de grâce

Compte tenu des délais de publication des CRL, le présent document recommande au destinataire d'attendre le temps nécessaire avant de déclarer une signature valide pour son usage.

4. POLITIQUE DE SIGNATURE CACHET

4.1 Préambule

Ce chapitre décrit les prestations fournies par le service de signature électronique de IDEMIA pour l'émission de documents signés en son nom ou de ses clients.

Le service de signature cachet est de type client-serveur. Une application cliente envoie au service de signature, soit l'ensemble des documents qu'elle désire signer, soit l'empreinte de ces documents, ainsi que l'identifiant de la politique de signature à utiliser, conditionnant ainsi le certificat de signature électronique à utiliser par association préalable de celui-ci avec la politique de signature.

L'application cliente est identifiée et authentifiée par certificat électronique.

Le service de signature de IDEMIA effectue la signature électronique des données reçues et renvoie à l'application appelante la signature du ou des documents.

4.2 Acteurs

Les acteurs concernés par la présente politique sont les suivants :

- **L'administrateur de l'application appelante**
  - Est responsable de l'application métier et des documents qu'elle soumet au service pour signature Cachet.
  - Administre et gère notamment les données d'authentification de l'application métier auprès du service de signature.
- **Le service d'horodatage**, génère des contremarques de temps à valeur probante conformément à la politique d'horodatage.
- **Le service de signature**
  - Authentifie la source de la requête
  - Reçoit les documents à signer et les signe
  - Soumet la signature au service d'horodatage pour y apposer une contremarque de temps
  - Soumet la signature au service de validation
- **Le destinataire de la signature**, reçoit les documents signés par le service.
- **Les administrateurs des services de confiance de IDEMIA**, allouent les ressources cryptographiques du service de signature et de validation de IDEMIA. Ils définissent les politiques de signature et de validation. Toute modification de la configuration des services de confiance est tracée et signée par l'administrateur.
- **Les auditeurs**, consultent les journaux d'activités du service de validation de signature.

4.3 Accès au service de signature

4.3.1 Ouverture du service

Afin de raccorder l'application appelante au service de signature Cachet, celle-ci doit utiliser un certificat électronique d'identification et d'authentification. L'administrateur de l'application appelante dépose donc une demande d'ouverture (accès et droits) auprès de son autorité d'enregistrement de l'autorité de certification de IDEMIA. L'entité Digital Lab de IDEMIA peut procéder à la fermeture du service à tout moment, notamment pour des raisons de sécurité (compromission de clé ou de certificat).

4.3.2 Authentification

Afin de sécuriser et d'authentifier les échanges entre les applications appelantes et le service de signature, la communication s'effectue grâce au protocole HTTPS. L'authentification du client auprès du serveur s'effectue grâce à un certificat d'authentification installé sur l'application appelante, et est mutuelle.

4.3.3 Gabarit des certificats d'authentification

Le gabarit des certificats d'authentification au service de signature est décrit dans le tableau ci-dessous :

Champ	Valeur	Détail valeur	Commentaire
Version	V3	2	Version du Certificat X.509
Numéro de série			Numéro de série unique du certificat
Algorithme de signature	*sha256WithRSAEncryption*2 048 bits	OID= 1.2.840.113549.1.1.11	Identifiant de l'algorithme de signature Identifiant de l'algorithme d'usage de la clé publique contenue dans le certificat et la valeur de cette clé publique
Émetteur	Exemple : C=FR, O= Société ABC, OU= 0002 243516879, CN= application appelante		Nom de l'AC émettrice (en conformité avec le RGS pour une administration)
Validité à partir de	T0		Date d'activation
Valide jusqu'au	T0	T0 + 3 ans (maximum)	
Objet	CN=Nom de la personne morale-Nom application [numéro incrémental si redondance]		Exemple : OU=Signataire OU= 002 123456789

Champ	Valeur	Détail valeur	Commentaire
			O=Client C=FR
Clé publique	Algorithme OID RSA SubjectPublicKey=… Taille = Y = 2048 bits	OID=1.2.840.113549.1.1.1	Identifiant de l'algorithme d'usage de la clé publique contenue dans le certificat et la valeur de cette clé publique
Identifiant de la clé publique de l'autorité (AuthorityKey Identifier)	AKI ID de la clé = …	Extension non critique	Identifiant de la clé publique à utiliser pour vérifier la signature d'un certificat
Identifiant de la clé publique du sujet (SubjectKeyIdentifier)	SKI ID de la clé = …	Extension non critique	Identifiant de la clé publique du certificat au cas où le même porteur aurait plusieurs bi-clé
Point de distribution de la CRL			
Politique de certification (Certificate Policies)	PolicyIdentifier =		Identifiant de la politique de certification
Utilisation de la clé (Key Usage)	*digitalSignature, nonRepudiation*	Extension critique	

4.3.4 Politique d'authentification

L'accès au service est soumis aux conditions suivantes :

- La requête est transmise via le protocole HTTPS assurant une authentification mutuelle par certificat des deux parties
- Le certificat d'authentification de l'application soumettant la requête est conforme au gabarit ci-dessus et n'est pas révoqué et est en cours de validité.

4.3.5 Protection des secrets

Les secrets (clé de signature cachet) et clé de signature de preuve comme vu en chapitre suivant) sont protégés et conservés dans un boitier cryptographique certifié suivant la norme « Critères communs » au niveau EAL4 et qualifié par l'ANSSI.

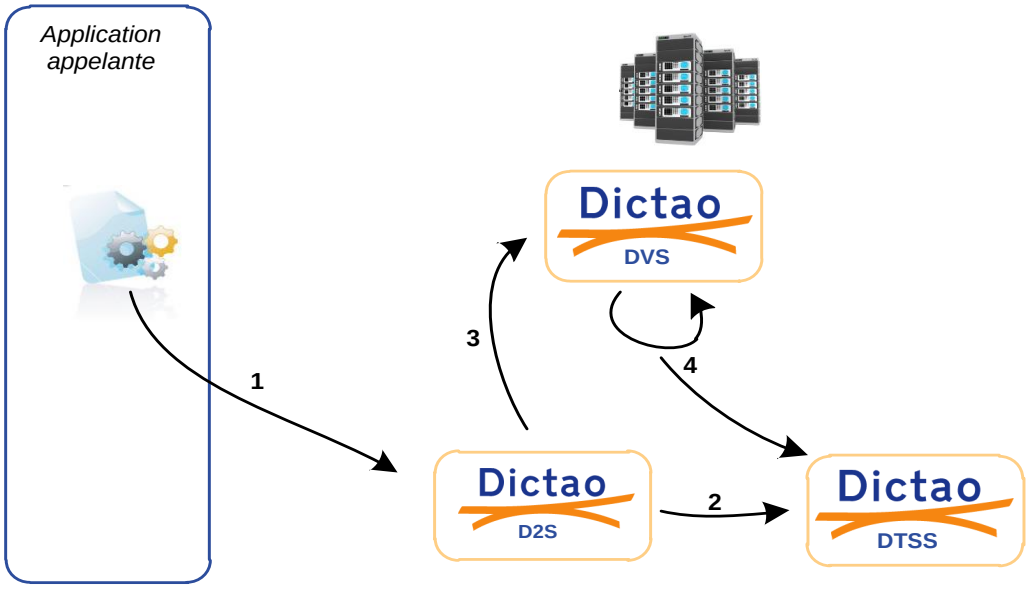
4.4 Cinématique de création de signature Cachet

La cinématique de signature cachet consiste à créer une signature horodatée qui consiste en

- Un document PDF signé

- Une signature XAdES version 1.3.2 jointe ou détachée
- Créer une preuve de validation de signature

Les étapes de cette cinématique sont décrites dans le schéma ci-dessous.



Les échanges et les données de confiance ainsi créées sont:

- Echange 1 : L'application appelante demande la création d'une signature au service de signature.
- Echange 2 : Le service de signature cachet de IDEMIA procède aux opérations de signature en y associant un jeton d'horodatage.
- Echanges 3 et 4: Le serveur de signature demande une validation de signature avec une création de preuve au service de validation. La donnée de confiance créée est :
  - Une preuve de validation de la signature signée et horodatée à l'instant « T ».
  - La preuve est conservée par le service de validation au moins pendant la période durée du service de signature

4.5 Signature

4.5.1 Données signées

Le service de signature de IDEMIA signe électroniquement tout document électronique transmis par l'application appelante reconnue et authentifiées auprès du service de signature Cachet.

Ceci suppose au préalable une identification et authentification (via son certificat électronique client) de l'application appelante auprès du service de signature Cachet.

4.5.2 Gabarit du certificat de signature Cachet

Les certificats dont les gabarits sont repris ci-dessous sont décrits dans la politique de certification de l'autorité de certification Services de IDEMIA pour les certificats référencés par l'OID 1.2.250.1.195.3.1.1.1.

4.5.3 Caractéristiques des signatures

Les signatures électroniques sont de type XAdES détaché, XAdES enveloppé ou PDF.

Conformément à la norme, les propriétés signées comprennent au moins les éléments suivants :

- Le certificat de signature (*SigningCertificate*)
- La date et l'heure de signature (*SigningTime*). La date et l'heure de référence pour cette opération sont précisées dans le document Déclaration des pratiques de signature.
- Une référence au présent document (*SigningPolicyIdentifier* / *SigPolicyIdType*)
    - OID (URI ou URN) de la présente politique de signature (*SigPolicyId*)
    - Valeur de l'empreinte de la politique de signature calculé et algorithme utilisé (*SigPolicyHash*) : SHA256.
    - Un jeton d'horodatage délivré par le service d'horodatage.

4.5.4 Algorithmes de signature

L'algorithme de signature recommandé par la présente politique est le *SHA256withRSAEncryption*.

Si l'utilisation de l'algorithme SHA1withRSAEncryption est tolérée pour des raisons d'interopérabilité une analyse de risques préalable doit être effectuée

4.5.5 Vérifications préalables à la signature

Le service de signature vérifie, avant chaque signature, que le certificat de signature est utilisé durant sa période de validité et qu'il n'est pas révoqué.

4.5.6 Vérifications lors de la signature

Le service de signature appelle automatiquement le service de validation de signature après la création de la signature, ce dernier réalisant alors une validation immédiate de la signature produite.

5. POLITIQUE DE VALIDATION DE SIGNATURE CACHET

5.1 Préambule

La signature électronique apposée sur un ensemble de données permet de garantir l'intégrité de ces données et l'authenticité de leur émetteur.

La politique de validation décrit les règles à suivre pour valider des signatures électroniques émises dans le cadre de transactions électroniques, conformément à une politique de signature donnée.

5.1.1 Acteurs

Les acteurs concernés par la présente Politique de Validation de Signature Cachets ont les suivants :

- **Le service de validation de signature**, qui vérifie que :
  - les signatures Cachet sont conformes à ce même document
  - les contremarques de temps ont été générées conformément à la politique d'horodatage
- **Le service d'horodatage**, génère des contremarques de temps à valeur probante conformément à la politique PH-Dictao
- **Les administrateurs**, alloue les ressources cryptographiques du service de signature et de validation. Ils définissent les politiques de signature et de validation. Toute modification de la configuration des services de confiance est tracée et signée par l'administrateur.
- **Les auditeurs**, consultent les journaux d'activités du service de validation de signature.
- **Le destinataire de la signature**, qui reçoit les documents signés après validation de la signature.

5.1.2 Champ d'application

La présente politique de validation s'applique à toutes les signatures effectuées par les services de signature de IDEMIA.

5.1.3 Politique de signature associée

La présente politique de validation concerne les documents signés dont la signature comprend l'OID de ce document.

5.1.4 Période de validité

La présente politique entre en vigueur en même temps que la politique de signature associée.

5.1.5 Mise à jour de la politique

La présente politique doit être mise à jour selon les mêmes procédures et règles que la politique de signature associée.

5.1.6 Publication et consultation

La présente politique est mise à disposition de tous les responsables des services de signature et applications appelantes acceptant des documents signés sous le régime de la politique de signature associée.

5.1.7 Cohérence documentaire

La présente politique doit être mise à jour afin de correspondre aux règles définies dans la politique de signature associée.

5.2 Règles de validation

5.2.1 Conditions pour déclarer une signature valide

Une signature électronique Cachet émise par IDEMIA est déclarée valide lorsque :

- Le format de la signature est conforme à la norme de signature utilisée et décrite au chapitre précédent.
- Le certificat de signature est conforme au gabarit décrit au chapitre précédent
- Le certificat de signature et sa chaîne de certification sont valides à l'instant « T »,:
  - Validité temporelle
  - Le certificat n'est pas révoqué
  - La signature cryptographique est techniquement valide
- La vérification cryptographique de la signature conformément à la norme de signature utilisée donne un résultat positif
- Le jeton d'horodatage présent dans la signature ou accompagnant celle-ci est valide.

5.2.2 Données signées par l'application de signature

La politique de signature associée n'impose aucune restriction sur le type de document signé.

5.3 Création des preuves de validation de signature Cachet

Une preuve est générée par le service de validation à chaque opération de validation réalisée. La preuve de validation est signée électroniquement par le service de validation de IDEMIA.

5.3.1 Sécurité des clés de signature de preuve

Ces clés doivent être hébergées dans un boîtier cryptographique dans un environnement sécurisé et contrôlé par l'entité Digital Lab de IDEMIA.

5.3.2 Contenu de la preuve

Les informations contenues dans la preuve de validation de signature sont :

- Le hash des données applicatives caractérisant la transaction. La nature des données dont l'empreinte en utilisant l'algorithme SHA256.

- Les résultats de l'opération de validation de signature.
- Les données de confiance utilisées par le service de validation. Les données sont :
  - Les références aux certificats de la chaîne des autorités de certification,
  - Les références aux listes de révocation de certificat,
- La description de la politique de validation de signature appliquée.

5.3.3 Signature des preuves

5.3.3.1 Gabarit du certificat de signature Cachet

Le gabarit du certificat de signature est décrit dans le document référencé par l'OID 1.2.250.1.195.3.1.1.1.

5.3.3.2 Caractéristiques de la signature

La signature de la preuve de signature respecte la norme suivantes XAdES (ETSI TS 101 093), en version 1.1.1 ou supérieure.

Conformément à la norme, les propriétés signées comprennent au moins les éléments suivants :

- le certificat de signature (*SigningCertificate*)
- la date et l'heure de signature (*SigningTime*)
- une référence à la politique de signature associée (*SigningPolicyIdentifier* / *SigPolicyIdType*)
  - OID de la présente PS (*SigPolicyId*)
  - Valeur de l'empreinte de la politique de signature associée et algorithme utilisé (*SigPolicyHash*)

5.3.3.3 Algorithme de signature

L'algorithme de signature recommandé est le *SHA256withRSAEncryption*.

5.4 Conservation des preuves de validation

IDEMIA conserve les preuves de validation durant toute la durée de vie de ses services, destinée à servir de preuve, le cas échéant, de la réalité de l'opération.

Le service de validation de signature s'engage à ne conserver aucune copie des données soumises pour validation de signature. En particulier, les journaux d'événements (traces d'activité) du service ne contiennent aucune copie de ces données.

Le service de validation de signature de IDEMIA s'engage à créer une preuve de validation signée. La preuve est remise au destinataire soit suite à sa demande explicite aux administrateurs de service de signature de IDEMIA, soit de façon automatisée, soit sur demande écrite.