Spécifications fonctionnelles générales

Serveur de signature

Version :	1.5
Date de document:	06 Octobre 2016
Ref. Doc.:	MSIGN-SRV-SPC-03

Statut

Rédaction	VKA
Validation	
Classification	Diffusion publique
Etat du document	Validé
Version actuelle	1.5
Référence	MSIGN-SRV-SPC-03
Version Produit applicable	2.0.0

Diffusion

Diffusion publique.

Historique des révisions

Date	Version	Commentaires
11/02/2014	0.1	Création à partir du document MSIG-SRV-SPC-01
22/09/2014	1.0	Prise en compte des remarques suite à relecture Validation du document.
15/12/2015	1.1	Utilisation du modèle ATOS
30/03/2016	1.2	Ajout du mécanisme d'OTP Ajout de la génération de certificat depuis un fournisseur Ajout de la validation interne de certificat
06/10/2016	1.3	Support des nouveaux formats EIDAS
14/03/2017	1.4	Mise à jour des opérations de générations de clés avec les usages de clés. Mise à jour de l'opération de consultation des utilisateurs

29/05/2018	1.5	Mise à jour pour l'activation de la clé Ajout de la description pour FIDO

Sommaire

1 Introduction 5
1.1 Présentation du contexte 5
1.2 Références documentaires 5
1.3 Glossaire 6
2 Présentation générale 8
2.1 Fonctionnalités de signature 9
2.2 Les utilisateurs du serveur de signature 10
2.3 Gestion des secrets des utilisateurs 11
2.4 Fonctions de gestion relative au serveur de signature 13
3 Fonctions de signature électronique 14
3.1 Généralités 14
3.2 Opérations de Signature/Vérification 16
3.3 Gestion des paramètres de signature 22
3.4 Gestion des clés de signature 25
4 Gestion des utilisateurs 31
4.1 Généralités 31
4.2 Opérations sur les utilisateurs 31
4.3 Opérations sur les groupes 33
4.4 Processus d'enrôlement des utilisateurs 34

1 Introduction

1.1 Présentation du contexte

Ce document présente les spécifications fonctionnelles du serveur de signature de Bull dénommé MetaSIGN-SERVER. Ce serveur est destiné à fournir des services de signature électronique et de vérification de signatures électroniques disponibles sous forme de web service.

Le premier chapitre offre une présentation générale du serveur, introduit les notions et la terminologie afférente.

Le chapitre suivant présente l'ensemble des fonctions du serveur regroupées par groupe de fonctionnalités :

- Les foncions liées à la signature de documents et la vérification des signatures. Elles s'accompagne de fonctions destinées à transmettre et récupérer les documents.
- Les fonctions permettant de gérer les paramètres de la signature.
- Les fonctions d'administration des biclés et des certificats sur le serveur de signature.

Enfin, le dernier chapitre est dédié à la gestion des utilisateurs du serveur der signature et la description des processus d'enrôlement de ces utilisateurs.

1.2 Références documentaires

1.2.1 Références internes

Référence	**Titre**	**Version**
MSIGN-SRV-GDE-01	Définition des interfaces du serveur de signature MetaSIGN-Server	1.7
MSIGN-PS-02	Description des politiques de signature au format XML	1.5
METAPKI-ADM-GDE-01	Manuel d'Administration du Framework IDC	4.29

1.2.2 Références externes

Référence	**Titre**	**Document**	**Version**
TS 102 778-1	PDF Advanced Electronic Signature Profiles	Part 1: PAdES Overview - a framework document for PAdES	1.1.1
TS 102 778-2	PDF Advanced Electronic Signature Profiles	Part 2: PAdES Basic - Profile based on ISO 32000-1	1.2.1

TS 102 778-3	PDF Advanced Electronic Signature Profiles	Part 3: PAdES Enhanced – PadES-BES and PAdES-EPES Profiles	1.2.1
TS 102 778-4	PDF Advanced Electronic Signature Profiles	Part 4: PAdES Long Term - PAdES-LTV Profile	1.1.2
TS 101 733	CMS Advanced Electronic Signatures (CAdES)	Electronic Signatures and Infrastructures (ESI)	1.6.3
TR 102 038	XML format for signature policies	Electronic Signatures and Infrastructures (ESI); XML format for signature policies	1.1.1
ISO 32000-1 ETSI TS 103 173	**Portable document format** CAdES Baseline Profile	**Portable document format — Part 1: PDF 1.7** http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.01.01_60/ts_103	2008 2.1.1
ETSI TS 103 171	XAdES Baseline Profile	http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103	2.1.1
ETSI TS 103 172	PAdES Baseline Profile	http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.01.01_60/ts_103	2.1.1
EN 319 122-1	CAdES digital signatures - Part 1 : Building blocks	https://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.01.00_30/en	1.1.0
EN 319 132-1	XAdES digital signatures - Part 1 : Building blocks	https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.00_30/en	1.1.0 (final draft)
EN 319 142-1	PAdES digital signatures - Part 1 : Building blocks	http://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.00_30/en_	1.1.0 (final draft)

1.3 Glossaire

Acronymes	**Définition**
CAdES	*CMS Advanced Electronic Signatures* Format de signature électronique avancée (ou sécurisée) définie par l'ETSI. Cette signature est une signature ASN.1 basée sur le format CMS.
PAdES	*PDF Advanced Electronic Signatures*
OID	*Object Identifier*

XAdES	*XML Advanced Electronic Signatures* Format de signature électronique avancée (ou sécurisée) définie par l'ETSI. Cette signature est une signature en XML en extension du format XML-DSIG.
IDC	Infrastructure de Confiance
BES	*Basic Electronic Signature* Format de signature numérique sans référence à une politique de signature
EPES	*Explicit Policy Electronic Signature* Format de signature avancée faisant référence explicite à une politique de signature.
CSR Profil de base	*Certificate Signature Request* Les profils de base sont des formats de signature permettant de définir les différentes caractéristiques que la signature doit remplir afin d'être le plus interopérable possible.

2 Présentation générale

La fonction principale du serveur de signature est de recevoir et de traiter de la part de signataires et/ou d'applications de signature des demandes de signature de documents ou de vérification des signatures.

MetaSIGN-Server implémente de manière centralisée la signature de personnes et la signature d'entités juridiques, usuellement dénommée signature cachet.

En cohérence avec l'offre MetaSIGN de Bull, MetaSIGN-SERVER s'appuie sur l'API de signature électronique MetaSIGN-API qui concentre toutes les fonctions de signatures électroniques avancées. Ainsi MetaSIGN-SERVER dispose des mêmes fonctionnalités de signature que celles proposées par les autres composants de la solution (MetaSIGN-API, MetaSIGN-APPLET et MetaSIGN-Workstation), mais sous la forme d'un serveur. Le service de signature est donc centralisée et les clés et certificats de signature sont gérées dans le serveur de signature, sécurisé par l'utilisation d'un HSM (Hardware Secure Module).

Les interfaces de MetaSIGN-Server sont définis sous la forme de Services Web accessibles après authentification forte de l'utilisateur.

Le schéma ci dessous illustre l'intégration de MetaSIGN-SERVER au sein d'un Systtème d'Information où les services de signature électronique sont fournis en back-office pour les applications externes et/ou internes.

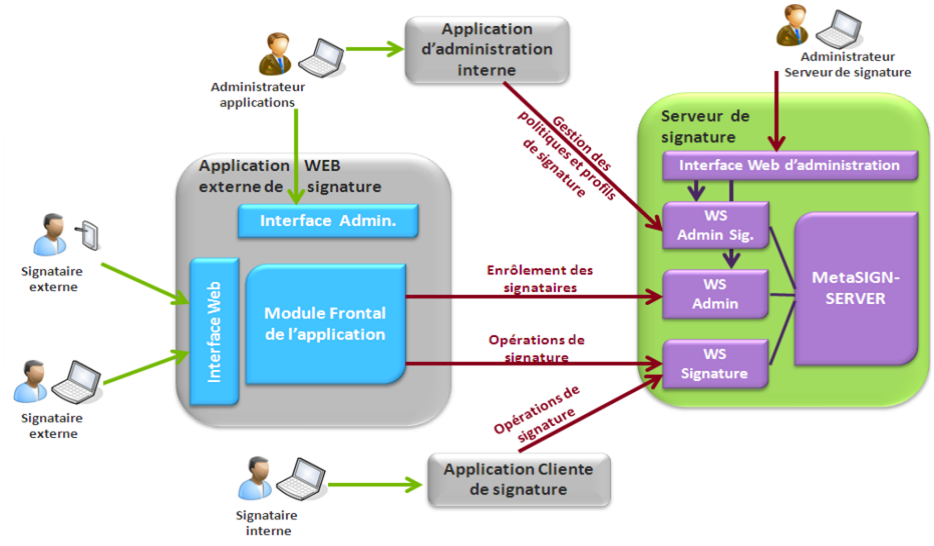

Figure 1 : MetaSIGN-SERVER au sein d'une architecture où il fournit les services de signature électronique

Les fonctionnalités de signature (création de signature électronique, vérification immédiate et augmentation, vérification ultérieure) ainsi que leurs caractéristiques sont décrites dans le chapitre suivant.

Le serveur de signature est pleinement intégré dans le Framework IDC (Infrastructure de Confiance) qui constitue le socle technique commun aux produits d'Infrastructure de Confiance de Bull (MetaPKI, MetaSIGN, MetaTIME). Cette architecture perrmet, entre autre de bénéficier de fonctionnalités

communes comme :

- L'utilisation de l'IHM pour la configuration et l'administration du serveur de signature;
- La gestion et la consultation des journaux d'évènement du serveur de signature;
- L'utilisation de l'IHM pour la gestion des signataires en mode cachet (gestion des signataires et de ses clés de signatures);
- La Gestion des droits d'accès aux Services Web du serveur de signature;
- La gestion des politiques de signature.

2.1 Fonctionnalités de signature

MetaSIGN-SERVER offre les trois fonctionnalités de signatures suivantes :

- La génération d'une signature électronique avancée d'un document ou d'un flot de données;
- L'augmentation d'une signature électronique avancée intégrant une vérification préalable de la signature;
- La vérification ultérieure d'une signature électronique avancée.

MetaSIGN-SERVER supporte la signature (création et vérification) de tout format de document, un document à signer étant considéré comme un flux de données binaires. Ainsi la solution supporte en standard la signature de documents en entrée aux formats suivants:

- XML;
- Microsoft Office;
- Open Office;
- PDF;
- Tout autre format (flux de données binaires).

Il est cependant important de considérer que les données à signer doivent être stables afin de pouvoir en garantir l'intégrité dans le temps. Ainsi, l'utilisateur du serveur de signature veillera par exemple à éviter la présence d'une macro dans un document au format « Word ». Pour cette raison et parce qu'ils garantissent que les données sont statiques, les formats PDF et XML sont préférables pour la signature.

En conformité avec les différentes normes existantes, MetaSIGN-SERVER supporte les formats de signature suivants :

- CAdES : CMS Advanced Electronic Signature, qui est défini dans la spécification technique ETSI TS 101 733
- XAdES : XML Advanced Electronic Signature, qui est défini dans la spécification technique ETSI TS 101 903.
- PAdES : PDF Advanced Electronic Signature, qui est défini dans la spécification technique ETSI TS 102 778.

Par ailleurs, suite à la sortie du règlement n°910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, de nouveaux standards européens définissant les formats de signature électronique avancées à utiliser dans ce cadre ont été publiés. **Metasign-api** supporte les nouveaux standards suivants :

- [EN 319 122-1] pour les signatures **CAdES**
- [EN 319 132-1] pour les signatures **XAdES**

- [EN 319 142-1] pour les signatures **PAdES**

Ces documents sont de nouvelles spécifications basées sur les spécifications techniques ETSI : CAdES, XAdES, PAdES et les profils de base associés :

Standard européen (**EN**) = Spécification technique (**TS**) *évoluée* + Profil de base (**BP**) *évolué*

2.2 Les utilisateurs du serveur de signature

Les utilisateurs du serveur de signature sont définis selon deux différents types :

- **Les personne physiques :** Il s'agit d'un utilisateur identifié comme étant une personne physique pour laquelle un ou plusieurs des rôles vont lui être attribués afin de lui autoriser des opérations spécifiques sur le serveur de signature.
- **Les application** : Il s'agit d'une application pour laquelle un ou plusieurs des rôles vont lui être attribués afin de lui autoriser des opérations spécifiques sur le serveur de signature.

Un utilisateur peut disposer d'un ou plusieurs rôles définis comme suit :

- **Signataire (Signer):** Il s'agit d'un signataire ou d'une application de signature qui dispose de clés de signature. Le signataire a la possibilité d'effecteur des opérations de signature sur un ou plusieurs documents. Dans le cas d'un signataire, Il peut s'agir d'un individu ou d'une entité organisationnelle au niveau d'une entreprise. Dans le cas d'une application de signature, les opérations peuvent être réalisées pour le compte des signataires ou en leur nom propre. Elle est alors considérée comme une application de confiance vis à vis du signataire.
- **Application de confiance (TrustedApplication)**: Il s'agit d'une application utilisatrice qui est autorisée à accéder au serveur de signature et qui relaye, pour le compte de signataires, des demandes d'opérations de signatures. Lors de l'enrôlement du signataire (ou sa mise à jour), celui-ci déclare les applications de signature auxquelles il fait confiance et donc au travers desquelles il accepte de réaliser de opérations de signature.
- **Administrateur (Admin)** : Un administrateur ou une application d'administration réalise les opérations de gestion des utilisateurs et des groupes du serveur de signature.
- **Gestionnaire (SignManager)** : Un gestionnaire ou une application de gestion réalise les opérations de gestion des éléments nécessaires aux opérations de signature tels que :
  - la gestion des politiques de signature (et de vérification) utilisées par le serveur de signature,
  - la définition de profils de signatures qui seront requis pour chaque opération spécifique de signature,
  - la définition de profils de génération de clés de signature qui seront requis lorsqu'un utilisateur demande au serveur de signature de générer une clé de signature pour un signataire (ou application de signature).

Lorsqu'un utilisateur est enrôlé dans le serveur de signature sans que lui ait été associé un rôle particulier, celui-ci est considéré comme « Anonyme ». Il ne peut alors pas s'authentifier auprès du serveur. La seule opération autorisée consiste à réaliser une demande d'enregistrement dans le serveur (ou enrôlement). C'est seulement après que cette demande ait été approuvée que cet utilisateur pourra obtenir un rôle de signataire, administrateur, gestionnaire ou application de confiance.

2.3 Gestion des secrets des utilisateurs

Le serveur de signature réalise une gestion sécurisée des différents secrets des utilisateurs. Typiquement, les secrets gérés par le serveur sont les secrets liés à l'authentification avec le serveur ou les clés de signature des utilisateurs. Pour se faire, le serveur utilise un module de sécurité physique (HSM) qui stocke les différents éléments cryptographiques sensibles et qui réalise les fonctions cryptographiques de la signature électronique.

Le serveur implémente des « conteneurs cryptographiques » protégés par un secret d'activation distinct pour chaque signataire ou pour chaque application de signature. Les objets cryptographiques de chaque signataire ou application de signature sont protégés par ce secret d'activation de sorte qu'une signature ne peut être réalisée sans la fourniture systématique de ce secret. Ainsi, lors d'une opération de signature, la transmission et la présentation au serveur du secret d'activation vaut preuve du consentement du signataire.

2.3.1 Activation d'une clé de signature

2.3.1.1 Pour une application de signature

Dans le cadre de la réalisation des opérations de signature de documents par les Applications de signature en leur nom (en mode cachet), l'utilisation des clés de signature est transparente si l'authentification de l'application est réussie.

En effet, en mode cachet, la clé est conservée dans le HSM afin d'optimiser les performances de signature.

Lors de la première requête de signature par l'application, le serveur de signature établit une session avec le HSM qui est conservée pour les requêtes suivantes.

Ce mécanisme oblige toutefois à l'application de présenter à chaque opération le secret d'activation de sa clé de signature,pour toute demande de signature par un signataire. Le secret d'activation doit donc être conservé dans le contexte de l'application appelante.

Dans ce mode, la biclé est générée dans le HSM lors d'une cérémonie de clés. Le serveur de signature utilise alors l'identifiant de la clé présente dans le HSM.

2.3.1.2 Pour un signataire

Dans le cadre de la réalisation des opérations de signature de documents pour le compte d'un signataire, les applications de confiance ont recours de façon transparente à l'activation des clés de signature de signataires.

Cette opération est réalisée de façon transparente si l'authentification de l'application au serveur est réussie et si l'identification de la clé de signature transmise dans la demande de signature correspond bien à une clé attribuée à ce signataire.

Le serveur utilise le secret d'activation de signature pour charger la clé de signature demandée dans le HSM et la rendre ainsi utilisable pour l'opération de signature.

Contrairement au mode cachet, la clé du signataire est conservée dans le HSM le temps de réaliser l'opération de signature.

A signaler qu'un signataire peut disposer de plusieurs clés et certificats de signature qui sont alors

enregistrés dans un seul conteneur cryptographique de clés, sécurisé par le même secret d'activation.

Authentification forte (deux facteurs d'authentification)

Cas de l'OTP

Le serveur de signature dispose d'un mécanisme d'authentification forte pour ses clés de signature. Ce mécanisme est un système avec deux facteurs d'authentification :

- le secret d'activation du signataire ;
- le secret d'activation dynamique (OTP).

Lorsque la clé du signataire nécessite une authentification forte, le signataire doit effectuer une opération d'activation de clé, permettant de récupérer un challenge généré par le HSM, avant de pouvoir l'utiliser. Si un service de gestion d'OTP (broker OTP) est configuré, lors de l'activation de la clé, le challenge lui sera directement envoyé.

Le calcul de la réponse au challenge peut être réalisé de deux façons :

- Le signataire dispose d'une application permettant de calculer la réponse au challenge ;
- Un service spécialisé se charge de calculer la réponse au challenge et distribue la réponse au signataire via un canal sécurisé.

Ainsi, le signataire peut réaliser l'opération de signature ou de génération de CSR en fournissant :

- son secret d'activation qui constitue le premier facteur d'authentification ;
- et la réponse au challenge qui constitue le second facteur d'authentification.

Cas de FIDO

Le serveur de signature dispose d'un mécanisme d'authentification forte pour ses clés de signature. Ce mécanisme est un système avec deux facteurs d'authentification :

- le secret d'activation du signataire ;
- le secret d'activation dynamique (données signées et données du client).

Le token FIDO doit être déposé dans le serveur de signature (après enrollement du signataire auprès de la clé FIDO) avant d'effectuer une opération d'activation de clé. Puis le signataire doit effectuer une opération d'activation de clé, permettant de récupérer un challenge généré par le HSM. Ce challenge doit être ensuite transmis à clé FIDO qui renvoie des données (données de signature et données client) pour l'authentification du signataire.

Ainsi, le signataire peut réaliser l'opération de signature ou de génération de CSR en fournissant :

- son secret d'activation qui constitue le premier facteur d'authentification ;
- la réponse de clé FIDO qui constitue le second facteur d'authentification ;

- L'identifiant du token FIDO dans le serveur de signature.

2.4 Fonctions de gestion relative au serveur de signature

Outre les opérations de signatures/vérification en elles mêmes, le serveur met à disposition les fonctionnalités de gestion suivantes :

- Gestion des signataires et des groupes associés (création, mise à jour, suppression, consultation)
- Gestion des politiques de signature (dépôt, récupération, suppression)
- Gestion des profils de signature (dépôt, mis à jour, récupération, suppression)
- Gestion des profil de génération de clés de signature (dépôt, mis à jour, récupération, suppression) et de création/suppression de clés (à partir d'un PKCS#12, d'un identifiant de clé dans le HSM, d'un profil de clé)
- Gestion des documents volumineux (dépôt et récupération).

Enfin, le serveur fournit un module d'administration des administrateurs du serveur qui assurent le paramétrage et la surveillance des applications de confiance, des applications de signature (habilités à effectuer les demandes de signature) et des signataires (dont les clés sont utilisées pour produire les signatures).

Les chapitres suivants décrivent l'ensemble de ces fonctionnalités.

3 Fonctions de signature électronique

3.1 Généralités

3.1.1 Modes de fonctionnement

Les opérations de signature électroniques sont destinées à traiter des documents électroniques pouvant être éventuellement volumineux. Les fonctions de signatures fournies par le serveur de signature doivent pouvoir permettre le traitement optimum de ce type de document.

Pour ce faire, 2 modes de fonctionnement ont été prévus :

- mode synchrone : le résultat de l'opération de signature est renvoyé à l'appelant. L'opération est donc bloquante.
- mode asynchrone : Lorsque l'appelant émet une requête, celle-ci renvoie des informations d'identification qui permettent à l'appelant de récupérer dans un second temps le résultat de l'opération de signature auprès du serveur. Ce mode est typiquement destiné au traitement de signature de documents volumineux.

De plus, le serveur offre la possibilité d'envoyer lors d'une demande de signature :

- soit le document à signer lui-même;
- soit un identifiant correspondant à un document précédemment déposé sur le serveur;
- soit un haché du document calculé par l'appelant : le document n'étant pas transmis au serveur, seul une signature en mode détachée au format XAdES peut être réalisée dans ce cas; le haché du document suffit alors à la production d'une signature. En effet l'API MetaSIGN, sur laquelle s'appuie le serveur, ne permet pas de faire de l'augmentation de signature sans appel à la vérification préalable qui requiert la vérification du haché; A signaler que dans ce cas, le contrôle de l'intégrité du document n'est réalisé par le serveur que sur la base du haché fourni par l'application appelante, et donc sous sa responsabilité.
- soit l'adresse URL où le document à signer se trouve. Le document sera alors téléchargé par ce lien fourni sous la condition qu'il soit accessible par le serveur.

Le mode asynchrone et la signature de documents déposés impliquent l'utilisation de fonctionnalités de récupération ou de dépôt de document sur le serveur qui sont présentées dans le chapitre §3.2.1.

3.1.2 Validation des opérations

Le serveur de signature permet d'effectuer, en préalable au traitement d'une demande de signature de document, une validation destinée à en vérifier la faisabilité (on évitera ainsi de charger le serveur avec des demandes irréalisables).

En outre, le serveur étant destiné à pouvoir effectuer des signatures électroniques avancées garantissant la non répudiation d'une transaction, il importe de s'assurer que chaque demande soit accompagnée d'un secret d'activation, faisant la preuve que le signataire est effectivement à l'origine de la demande ou en accord avec celle-ci. A cet effet, le serveur de signature vérifie le secret d'activation de façon systématique pour chaque demande.

Pour chaque demande, le serveur procède aux vérifications suivantes :

- vérifier l'accessibilité du document (ou du haché) et vérifier son intégrité;

- vérifier l'existence de la politique de signature choisie;
- contrôler l'adéquation du type de document avec le type d'opération choisie (par exemple la signature au format XAdES à l'exception de la signature en mode détachée, traitera uniquement des documents XML. La signature au format PAdES traitera uniquement des documents PDF). En cas de transmission d'un haché, certaines opérations ne sont pas possibles comme précisé au paragraphe précédent;
- contrôler l'adéquation de la taille du document avec le mode de traitement demandé (les documents trop volumineux ne seront pas traités en mode synchrone);
- vérifier l'existence du signataire, du secret d'activation fourni et de l'existence de la clé de signature souhaitée;
- contrôler l'adéquation de la clé de signature avec le profil de signature.

C'est seulement après tous ces contrôles réussis que l'opération de signature peut être exécutée sur le serveur.

3.1.3 Administration et configuration

Les opérations de signature impliquent l'utilisation de profils et de politiques de signature, de clés (et certificats associés) de signatures.

Le serveur de signature fournit des fonctions d'administration de ces objets par des fonctions de création, recherche/consultation, mise à jour et suppression.

MetaSIGN-SERVER étant intégré au Framework IDC, celui-ci présente aussi des IHM permettant de remplir ces fonctionnalités. La gestion de ces IHM est décrite dans le document d'administration du Framework IDC (METAPKI-ADM-GDE-01).

3.1.4 Vérification et augmentation de la signature électronique

Avant génération de la signature et lors de la vérification d'une signature, le serveur de signature effectue des contrôles sur les certificats constituant une signature. Ces certificats sont :

- certificat du signataire et sa chaîne de certification ;
- certificats des unités d'horodatage et leur chaîne de certification associée.

Le serveur de signature dispose de 2 méthodes différentes pour assurer la vérification des certificats :

- une validation interne utilisant les magasins de certificats et CRLs/réponses OCSP ;
- une validation externe utilisant l'interface externe du serveur de validation de certificat VeriCert.

La méthode utilisée est configurable via l'IHM du Framework IDC. Si, une URL est configuré pour le serveur de validation VeriCert alors la validation externe sera utilisée. Sinon, la validation interne sera utilisée.

3.1.5 Utilisation de services externes

Afin de réaliser une opération complète de signature électronique avancée, le serveur peut utiliser des services externes :

- un service d'horodatage : Le serveur de signature s'appuie sur un serveur d'horodatage externe permettant de produire des signatures augmentées par l'apposition d'un jeton

d'horodatage sur la signature. La solution MetaTIME ou toute solution d'horodatage conforme à la RFC3161 peut être utilisée pour demander ces contremarques de temps;

- un service de validation des certificats : Le serveur s'appuie sur la solution VeriCert afin de garantir que les certificats utilisés pour la signature ainsi que les Autorités de Certifications ayant émis ces certificats sont toujours valides et autorisés par la politique de signature appliquée pour réaliser les opérations de signatures;
- un service d'archivage: MetaSIGN-SERVER peut utiliser la solution MetaSIGN-ADP pour archiver les signatures produites. Il sera alors possible pour les utilisateurs de procéder au contrôle de la preuve des signatures. (Note : Ce service sera disponible dans de futures versions)

Ces services ne sont disponibles que suite à l'activation des dites options et au paramétrage des données nécessaires.

L'administration de ces services est réalisée au travers de l'IHM de configuration du serveur de signature fournie dans le FrameWork IDC (à partir de la version 9.7.0).

3.2 Opérations de Signature/Vérification

Ce paragraphe présente les fonctionnalités liées à la réalisation de signatures électronique avancée et de leur vérification fournies par le serveur.

Pour toutes les opérations de signature, sauf restriction précisée dans la description de l'opération :

- les trois formats de signature sont accessibles : CAdES, XAdES ou PAdES;
- les deux modes de réponse : synchrone ou asynchrone peuvent être utilisés

De plus, lors d'une opération de signature et si le profil de signature le requiert, une augmentation de signature comme décrite dans le paragraphe §20 sera effectuée de façon transparente et la signature augmentée sera fournie en résultat (ou créée sur le serveur en mode asynchrone).

Après s'être connecté et authentifié auprès du serveur de signature, un signataire effectue une opération de signature ou de vérification d'un document.

Le document à signer et/ou la signature peut être transmis selon plusieurs modes :

- Le document à signer est émis dans la requête;
- Le document a été précédemment déposé sur le serveur. son identifiant est alors transmis;
- Seul le haché du document (calculé par l'appelant et sous sa responsabilité) peut être transmis (uniquement pour une signature détachée sans augmentation);
- Le document à signer est localisé sur une URL.

Lors d'une opération de signature, le secret d'activation de la clé de signature est demandé.

3.2.1 Dépôt et récupération de document

Les fonctions de gestion de document permettent à un utilisateur de procéder au dépôt de documents (ou signature) pour un usage futur dans une ou plusieurs opération(s) de signature ou de vérification.

Lors de l'opération de dépôt, le document (ou la signature) est envoyé au serveur de signature qui le sauvegarde et crée un identifiant qui lui est attaché. Cet identifiant unique de document est ensuite

renvoyé à l'utilisation dans la réponse.

Note : Le serveur de signature n'étant pas destiné à conserver (et archiver) les documents ou signatures produites, ceux-ci seront automatiquement effaces du serveur après un délai faisant suite au dépôt qui est configurable dans le serveur de signature depuis l'IHM de configuration du serveur de signature fournie dans le FrameWork IDC (à partir de la version 9.7.0).

Dépôt d'un document

Après s'être connecté et authentifié auprès du serveur de signature, un Utilisateur effectue une opération de dépôt d'un document sur le serveur.

Pour cela, il doit renseigner les éléments nécessaires au dépôt du document :

- Le document ou la signature

Le document est ensuite envoyé sur le serveur et un identifiant est retourné à l'utilisateur.

Récupération d'un document

Après s'être connecté et authentifié auprès du serveur de signature, un Utilisateur effectue une opération de récupération d'un document sur le serveur.

Pour cela, Il doit renseigner les éléments nécessaires au dépôt du document :

- L'identifiant du document ou la signature

Le document est ensuite renvoyé par le serveur à l'utilisateur.

3.2.2 Signature d'un document par un signataire

Après s'être connecté et authentifié auprès du serveur de signature, un signataire effectue une opération de signature d'un document.

Pour effectuer la demande de signature, le signataire envoie :

- la représentation du document (soit le document, soit l'identifiant du document préalablement déposé, soit le haché du document, soit l'URL où se trouve le document);
- son secret d'activation de signature;
- l'identification de la clé de signature à utiliser;
- l'identification du profil de signature à utiliser ou un profil de signature explicitement défini pour cette opération.

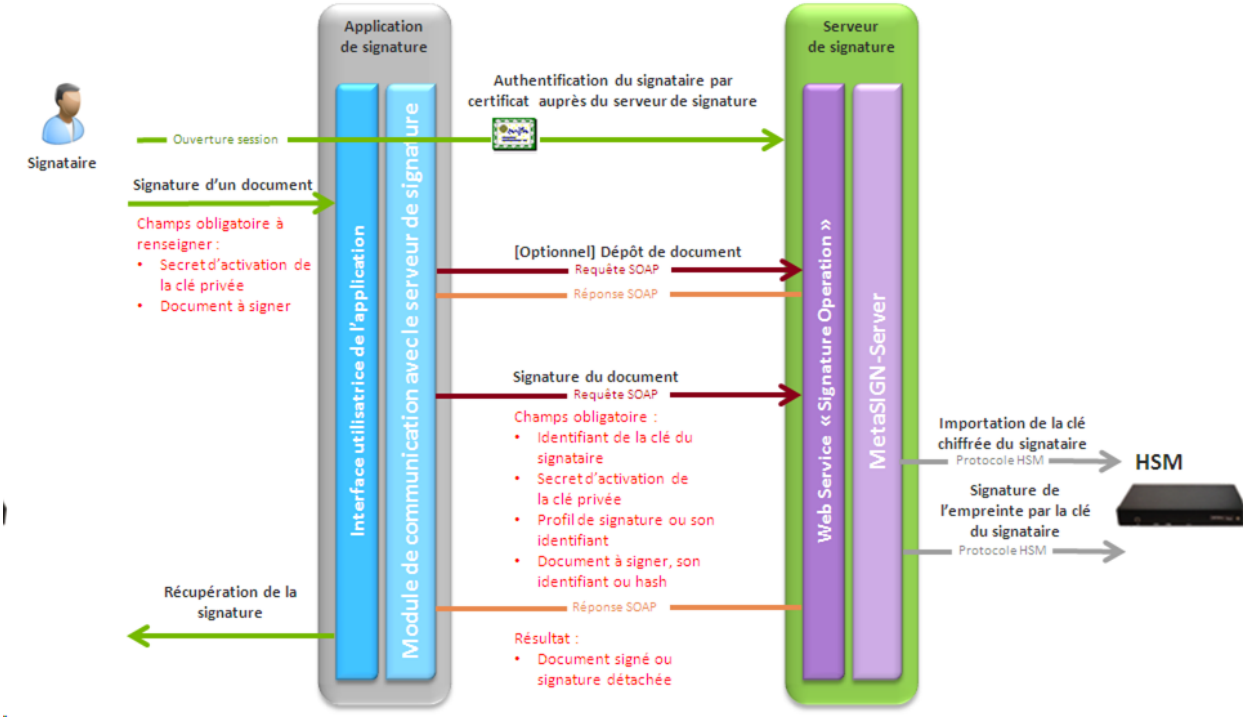

Figure 2 : Processus de signature de document par le signataire

3.2.3 Signature d'un document par une application de signature

Après s'être connecté et authentifié auprès du serveur de signature, une application de signature peut effectuer une opération de signature d'un ou plusieurs document(s) pour son propre compte (c'est à dire avec son propre certificat de signature).

Ce mode d'utilisation correspond à une signature en mode « Cachet » pour le compte d'une entreprise ou une entité morale.

Pour effectuer la demande de signature, l'application de signature envoie :

- la représentation du document (soit le document, soit l'identifiant du document préalablement déposé, soit le haché du document, soit l'URL où se trouve le document);
- l'identification de l'application de signature;
- le secret d'activation de signature de l'application de signature ;
- l'identification de la clé de signature de l'application de signature à utiliser;
- l'identification du profil de signature à utiliser ou un profil de signature explicitement défini pour cette opération .

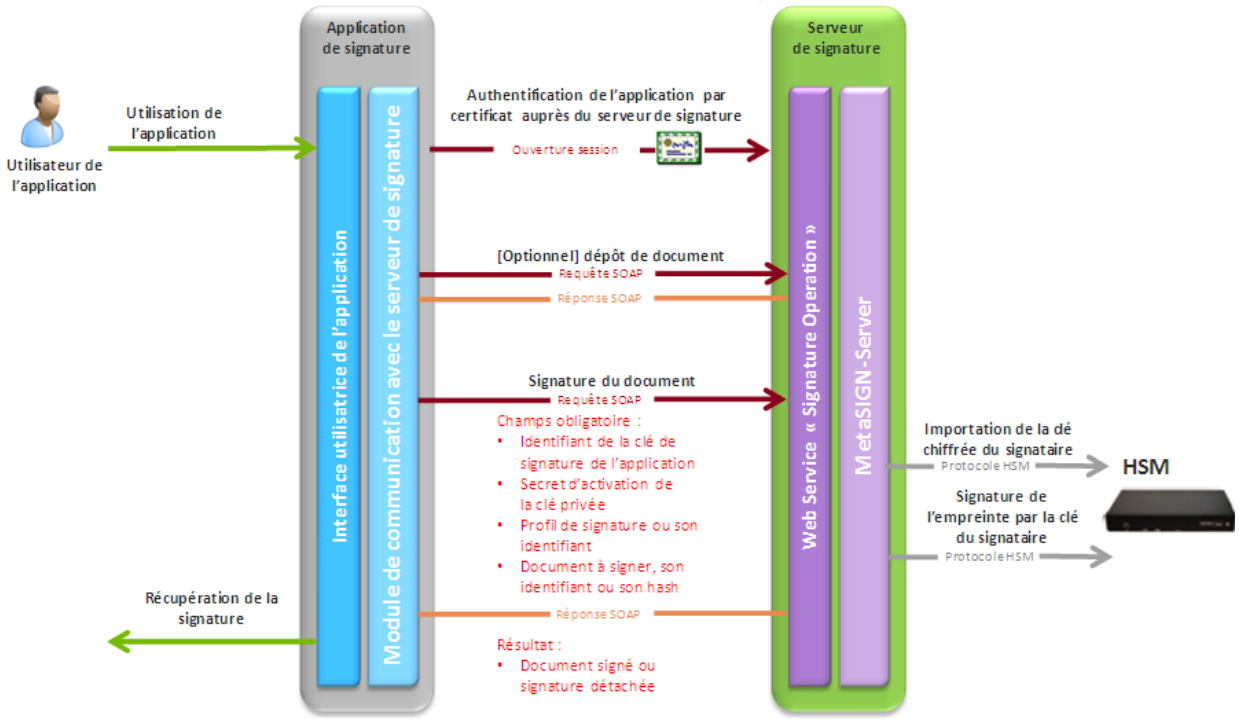

Figure 3 : Processus de signature de document par une application (signature Cachet)

Signature d'un document par une application de confiance

Après s'être connecté et authentifié auprès du serveur de signature, une application de confiance peut effectuer une opération de signature d'un ou plusieurs document(s) pour le compte d'un signataire.

Lors de la signature de plusieurs documents, la combinatoire sur les différents modes de transmission des documents est possible.

Pour effectuer la demande de signature, l'application de signature envoie :

- la représentation du ou des document(s) (soit le ou les document(s), soit l'identifiant du document préalablement déposé, soit le haché du document, soit l'URL où se trouve le document);
- l'identification du signataire;

- le secret d'activation de signature du signataire ;
- l'identification de la clé de signature du signataire à utiliser;
- l'identification du profil de signature à utiliser ou un profil de signature explicitement défini pour cette opération.

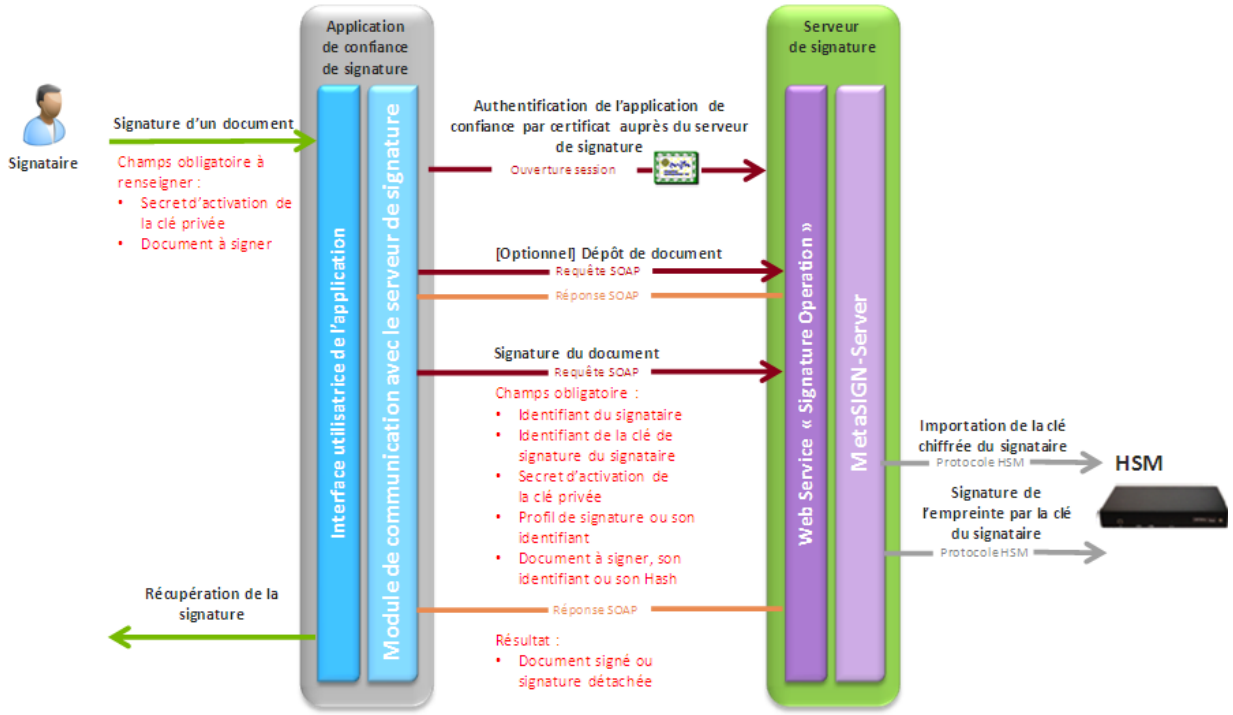

Figure 4 : Processus de signature d'un document par l'application de confiance pour le signataire

3.2.4 Augmentation d'une signature

Après s'être connecté et authentifié auprès du serveur de signature, un signataire, une application de signature ou une application de confiance peut effectuer une demande d'augmentation de signature. La fonction comporte une vérification préalable de la signature et une augmentation de celle-ci (ajout de données en référence au CRLs, certificats et apposition d'un jeton d'horodatage).

Pour cela, il doit renseigner les éléments nécessaires à l'augmentation de la signature :

- la signature (ou document signé) représenté par la signature elle-même, son identifiant ou l'URL où se trouve la signature.
- le profil de signature ou son identifiant
- si nécessaire (dans le cas d'une signature détachée) le document représenté par le document lui-même, son identifiant, son haché ou l'URL où se trouve le document

Lors de l'augmentation de plusieurs signatures, la combinatoire sur les différents modes de transmission des signatures est possible.

Comme dans le cas d'une signature de document, l'augmentation peut être réalisée par un signataire, un application, une application de confiance.

L'illustration ci dessous présente le cas où l'augmentation est réalisée par une application de confiance pour le compte d'un signataire

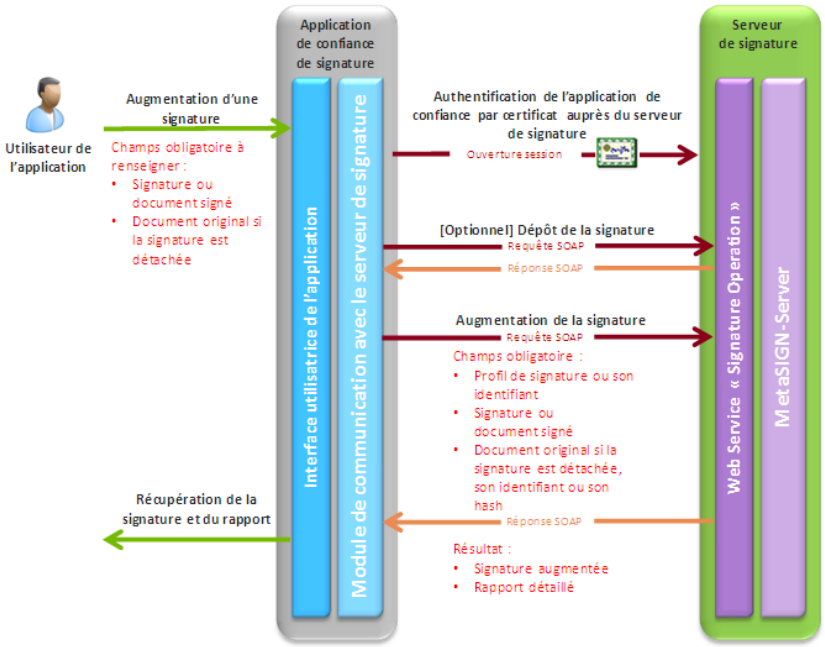

Figure 5 : Processus d'augmentation d'une signature

3.2.5 Vérification d'une signature

Après s'être connecté et authentifié auprès du serveur de signature, un utilisateur (un signataire ou une application de signature) peut effectuer une opération de vérification de la signature d'un document.

L'utilisateur fournit les informations nécessaires à la vérification de la signature et reçoit en retour un résultat de vérification qui indique si la vérification est réussie ou en échec, ainsi que les motifs de l'échec. Un rapport de vérification est alors renvoyé.

Pour cela, Il doit renseigner les éléments nécessaires à la vérification de la signature :

- la signature (ou document signé) représenté par la signature elle-même, son identifiant ou l'URL où se trouve la signature;
- si nécessaire (dans le cas d'une signature détachée) le document représenté par le document lui-même, son identifiant, son haché ou l'URL où se trouve le document;
- le format de signature à vérifier : CAdES, XAdES ou PAdES;
- Optionnellement, la politique de signature avec laquelle la vérification sera effectuée (nécessaire lorsqu'il s'agit d'une signature de type BES).

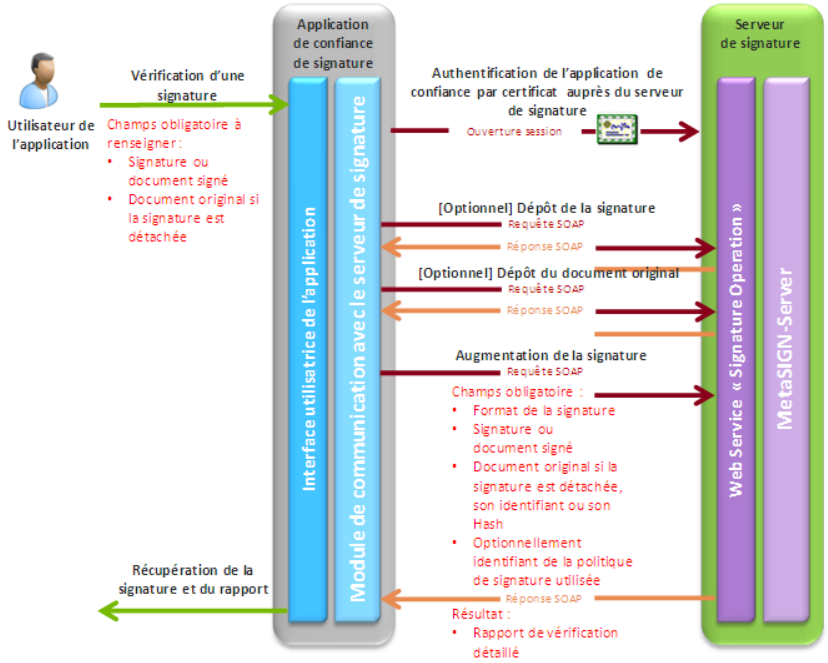

Figure 6 : Processus de vérification d'une signature

Note : Une seule signature peut être vérifiée par requête au serveur de signature.

3.3 Gestion des paramètres de signature

Lorsqu'un signataire (ou application de signature) souhaite réaliser une opération de signature, augmentation ou vérification d'une signature, il est nécessaire qu'elle soit établie en accord avec les éléments suivants :

- une politique de signature : cette politique définit les règles qui seront appliquées lors d'une opération de signature, augmentation ou vérification.
- un profil de signature : le profil définit le format et attributs qui seront appliquées lors de opérations de signature et d'augmentation,
- un profil de génération de clé : ce profil est utilisé lors de l'enrôlement d'un signataire ou d'une application afin de disposer d'une biclé associée à une demande de certificat de signature.

Seuls, les utilisateurs ayant les droits de « gestionnaire » sur le serveur pourront réaliser ces opérations.

Le FrameWork IDC intègre une IHM permettant de configurer les paramètres de ses différents éléments. Ceux-ci peuvent aussi être définit par l'application en utilisant le service web dédié à ces fonctions.

3.3.1 Gestion des politiques de signature

Une politique de signature électronique est un document décrivant les conditions de recevabilité d'un document électronique sur lequel sont apposés une ou plusieurs signatures électroniques.

Une politique de signature est identifiée par son identifiant unique défini par un OID.

Dans le cadre de l'utilisation des opérations de signature/vérification par le serveur de signature, celui-ci s'appuie sur la traduction techniques des informations présentes dans la politique de signature dans un fichier XML conforme à la description du document MSIGN-PS-02 et défini dans la spécification technique ETSI TR 102 038.

Les politiques déposées sur le serveur de signature pourront ensuite être utilisées par un signataire ou une application de signature pour réaliser des opérations de signature ou de vérification de signature.

Le serveur de signature propose des fonctions de gestion des politiques de signatures dans son service web dédié:

- Dépôt d'une politique de signature (permet la création et la modification)
- Récupération d'une politique de signature
- Suppression d'un politique de signature
- Récupération des informations d'une liste de politiques de signatures

Dépôt d'une politique de signature

Cette opération permet de créer une politique de signature sur le serveur de signature.

La politique peut être déposée sans qu'elle soit verrouillée; dans ce cas, le gestionnaire du serveur de signature pourra modifier cette politique par un nouveau dépôt qui sera alors mise à jour.

Si la politique a été verrouillée lors de son dépôt alors il ne sera plus possible de la modifier; un dépôt d'une nouvelle politique est alors nécessaire et devra être associée à un nouvel OID (ex : incrémentation de l'OID précédent).

Note : Un document qui serait signé par une politique de signature n'ayant pas été préalablement verrouillée et dont la signature embarque les informations de signature , ne pourra plus être vérifiée si la politique a été mise à jour et modifiée (le haché de la politique ne correspondrait alors plus au Haché de la politique embarquée dans la signature).

Après s'être connecté et authentifié auprès du serveur de signature, un gestionnaire effectue une opération de création de politique de signature.

Il renseigne les informations destinées à identifier cette politique. Il s'agit en particulier de :

- du nom de la politique,
- une information sur le verrouillage de la politique
- de sa description textuelle
- et d'un ensemble de mots-clé lui correspondant.

Récupération d'une politique de signature

Cette opération permet à un gestionnaire de signature de récupérer une politique de signature précédemment déposée sur le serveur de signature.

Cette politique est récupéré au format XML et correspond au document de description des politiques de signature MSIGN-PS-02.

Après s'être connecté et authentifié auprès du serveur de signature, un gestionnaire effectue une opération de récupération de politique de signature en renseignant l'OID de la politique.

Suppression d'une politique de signature

Cette opération permet à un gestionnaire de signature de supprimer une politique de signature précédemment déposée sur le serveur de signature.

Après s'être connecté et authentifié auprès du serveur de signature, un gestionnaire effectue une opération de suppression de politique de signature en renseignant l'OID de la politique.

Note : Une signature de document qui serait réalisée avec une politique de signature ayant été supprimée ne peut alors plus être vérifiée.

Récupération d'une liste de politique de signatures

Cette opération permet à un gestionnaire de signature de récupérer une liste de politiques de signature répondant à certains critères. La liste des critères possibles pour la recherche des politiques est le nom ou une partie du nom et/ou le verrou de la politique ou pas.

En l'absence de critères, l'intégralité des politiques est fournie.

3.3.2 Gestion des profils de signature

Un profil de signature définit le format et attributs qui seront appliquées lors de opérations de signature et d'augmentation.

Un profil de signature est identifié par son nom de profil. Lorsque un nouveau profil est créé avec le nom identique alors il remplace le précédent.

Ce profil de signature pourra ensuite être utilisé par un signataire ou une application de signature pour réaliser des opérations de signature (ou une augmentation de signature).

Le profil de signature est défini avec les éléments suivants :

- le format de signature : CMS, CADES-BES, CADES-EPES, XADES-BES, XADES-EPES, PADES-BES, PADES-EPES
- le type de signature :
  - DETACHED : pour les formats de signature CAdES et XADES,
  - ENVELOPING : pour les formats de signature CAdES et XADES,
  - ENVELOPED : pour les formats de signature XAdES et PADES
- l'identifiant d'une politique de signature;
- l'identifiant d'une politique de vérification;
- le type d'engagement parmi ceux définis par la politique de signature choisie;
- le rôle du signataire;
- les algorithmes de signature, de transformation et de canonisation;
- optionnellement, indique si une date présumé de signature doit être posée;
- optionnellement, indique si les informations sur le lieu de production de signature doit être posé.
- optionnellement et dans le cas d'une signature PADES, indique si les informations sur le contact doivent être précisées.
- Optionnellement, sélection de l'option d'archivage et de preuve.

Le serveur de signature propose des fonctions de gestion des profils de signatures dans son service web dédié:

- Dépôt d'une profil de signature

- Mise à jour d'un profil de signature
- Récupération d'un profil de signature
- Suppression d'un profil de signature
- Récupération d'une liste de profils de signature présents sur le serveur

3.3.3 Gestion des profils de génération de clé de signature

Un profil de génération de clé est utilisé lors de l'enrôlement d'un signataire ou d'une application afin de disposer d'une biclé associée à une demande de certificat de signature.

Un profil de génération de clé de signature est identifié par son nom de profil. Lorsque un nouveau profil est créé avec le nom identique alors il remplace le précédent.

Ce profil est ensuite être utilisé pour la création de biclés de signature et la requête de certificat associé afin de permettre aux applications de signature et signataires d'obtenir un certificat de signature auprès d'une IGC. Ce certificat pourra alors être utilisé pour les opérations de signature.

Le profil de génération de clé de signature est défini avec les éléments suivants :

- du nom du profil,
- de sa description textuelle,
- la longueur de la clé,
- le type de clé : ce type peut être identifié par différents moyens (OID, URI ou chaîne de caractère). Actuellement, seule les clés de type RSA sont utilisables sur le serveur de signature,
- (Optionnel) Les usages de la clé.

Note : la requête de certificat générée lors de l'utilisation du profil de génération de clé contiendra obligatoirement l'extension « keyid » afin de retrouver la clé associée lors du dépôt du certificat.

Le serveur de signature propose des fonctions de gestion des profils de génération de clés de signature dans son service web dédié:

- Dépôt d'une profil de génération de clé de signature
- Mise à jour d'un profil de génération de clé de signature
- Récupération d'un profil de génération de clé de signature
- Suppression d'un profil de génération de clé de signature
- Récupération d'une liste de profils de génération de clé de signature présents sur le serveur

3.4 Gestion des clés de signature

Pour permettre au serveur de signature de signer des documents, les signataires et applications de signature doivent enregistrer auprès du serveur leurs clés et certificats de signature.

Le serveur de signature offre différentes possibilité d'enregistrement des clés et certificats :

- la génération des paires de clés publique/privée de signature dans le HSM et l'émission d'une requête de certificat (CSR) correspondante pour importer dans un second temps le certificat certifié par une autorité de certification externe.
- la génération des paires de clés publique/privée de signature dans le HSM et l'émission d'une requête de certificat (CSR) à travers un protocol supporté par une PKI permettant la génération automatique du certificat.

- l'utilisation d'une clé préalablement créée dans le HSM lors d'une cérémonie de clé et émission d'une requête de certificat (CSR) correspondante pour importer dans un second temps le certificat certifié par une autorité de certification externe.
- l'importation des clés et certificats générés en externe sous forme d'un fichier PKCS#12.

Note : Les Applications de signature réalisent uniquement ces opérations pour leur propre compte (mode cachet). Ces opérations sont réalisées par les Applications de confiance lorsqu'il s'agit d'enregistrer ou de mettre à jour des clés de signature pour des signataires.

3.4.1 Génération de clé de signature et d'une demande de CSR

Après s'être connecté et authentifié auprès du serveur de signature un Signataire ou une Application de confiance pour le compte d'un signataire peut effectuer une demande de génération de clé privée de signature.

L'appelant (application de confiance ou signataire) fournit :

- l'identifiant de la future clé de signature;
- l'identifiant du profil de génération de biclé qu'il souhaite utiliser (celui-ci contient les informations sur les caractéristiques du biclé à générer) ou explicitement les données d'un profil de signature;
- le secret d'activation du signataire;
- (optionnel) le secret d'activation dynamique (le second facteur d'authentification, OTP, FIDO).

Le serveur de signature déclenche la génération d'une biclé dans le HSM conformément au profil de clé défini dans la demande et fournit alors en retour l'identifiant de la clé.

La biclé générée est extraite du HSM sous forme de jeton. Ce jeton est un chiffrement de la biclé par un clé de chiffrement se trouvant dans le HSM. Le jeton est alors sauvegardé dans la base de donnée du serveur.

La deuxième étapes consiste à effectuer une demande de requête de certification CSR pour la biclé générée.

L'application de confiance ou le signataire fournit :

- l'identifiant de la clé de signature;
- le secret d'activation du signataire;
- la réponse au challenge (si c'est une clé avec un double facteur d'authentification : OTP[1], FIDO).

Le serveur de signature déclenche la création de la requête de certification et fournit alors:

- l'identifiant de la biclé;
- la clé public générée;
- la CSR créé.

[1] Dans le cas d'une clé avec double facteur d'authentification (OTP, FIDO), il est nécessaire de faire une opération d'activation de clé afin de récupérer le challenge.

3.4.2 Génération de clé de signature et demande de certification

Après s'être connecté et authentifié auprès du serveur de signature un Signataire ou une Application de confiance pour le compte d'un signataire peut effectuer une demande de génération de clé privée de signature.

L'appelant (application de confiance ou signataire) fournit :

- l'identifiant de la future clé de signature;
- l'identifiant du profil de génération de biclé qu'il souhaite utiliser (celui-ci contient les informations sur les caractéristiques du biclé à générer) ou explicitement les données d'un profil de signature;
- le secret d'activation du signataire;
- (optionnel) le secret d'activation dynamique (le second facteur d'authentification, OTP, FIDO).

Le serveur de signature déclenche la génération d'une biclé dans le HSM conformément au profil de clé défini dans la demande et fournit alors en retour l'identifiant de la clé.

La biclé générée est extraite du HSM sous forme de jeton. Ce jeton est un chiffrement de la biclé par un clé de chiffrement se trouvant dans le HSM. Le jeton est alors sauvegardé dans la base de donnée du serveur.

La deuxième étapes consiste à effectuer une demande de certification pour la biclé générée.

L'application de confiance ou le signataire fournit :

- l'identifiant de la clé de signature;
- le secret d'activation du signataire;
- la réponse au challenge (si c'est une clé avec un double facteur d'authentification : OTP, FIDO).

Le serveur de signature déclenche la demande de certification auprès de la PKI et fournit alors:

- l'identifiant de la biclé;
- le certificat généré ou un identifiant de transaction permettant de récupérer le certificat (cas ou la PKI n'a pas pu générer le certificat).

Si le certificat a été généré par la PKI, il est automatiquement déposé dans le serveur de signature.

3.4.3 Génération d'une demande de CSR depuis une biclé existant dans le HSM

La demande de requête de certification pour une biclé existante dans le HSM est utilisée par une application de signature pour son propre compte (mode Cachet).

La biclé a été générée lors d'une cérémonie de clé.

L'obtention d'une CSR à partir d'une biclé existante est faite en deux étapes :

- l'affectation de la biclé en tant que clé de signature dans le serveur;
- la demande de CSR à partir de l'identifiant de clé de signature

Après s'être connecté et authentifié auprès du serveur de signature, l'application de signature pour son propre compte effectuent une opération de création de clé de signature à partir d'un identifiant de

clé dans le HSM.

L'application de signature fournit :

- l'identifiant CKaID de la clé générée dans le HSM et devant être associé au signataire;
- l'identifiant de la clé de signature qui sera associée à la création de la clé de signature;

le secret d'activation de signature.Le serveur de signature associe alors la biclé du HSM correspondant au CKaID à l'identifiant de clé de signature.

La deuxième étape consiste à faire une demande de CSR sur l'identifiant de clé de signature.

L'application de signature fournit :

- l'identifiant de la clé de signature;
- le secret d'activation du signataire ;
- la réponse au challenge (si c'est une clé avec authentification forte : OTP, FIDO)
- (optionnel) les usages de clé.

Le serveur de signature déclenche la création de la requête de certification et fournit alors:

- l'identifiant de la biclé;
- la clé public générée;
- la CSR créé.

3.4.4 Dépôt d'une clé et d'un certificat de signature

Après s'être connecté et authentifié auprès du serveur de signature, une Application de confiance peut déposer une clé et un certificat de signature sous forme d'un fichier PKCS#12.

Dans la mesure où les informations transmises sont sensibles et que le vecteur de transport est un fichier PKCS#12 protégé par un mot de passe, l'opération est réalisée en deux temps :

- dépôt du PKCS#12 contenant la clé privée et le certificat de signature associé sur le serveur;
- transmission du mot de passe et enregistrement de la/des clé(s) dans un second temps.

Ces deux étapes sont décrites ci-dessous.

L'application de confiance fournit le certificat de signature et la clé privée associée au serveur de signature sous forme de PKCS#12 encodé avec un mot de passe de transport. Un identifiant de dépôt est retourné par le serveur.

Dans un second temps, l'application de confiance active la clé et le certificat de signature en fournissant au serveur :

- l'identifiant de dépôt précédemment reçu;
- le mot de passe de transport utilisé pour protéger le PKCS#12;
- l'identifiant du signataire à qui sera associé la clé et le certificat;
- le secret d'activation du signataire;
- (optionnel) les usages de clé.

Le serveur effectue un ensemble d'opérations de validation :

- lorsqu'il s'agit d'un dépôt réalisé pour le compte d'un signataire : l'habilitation de l'appelant à gérer le signataire est vérifiée
- l'adéquation du DN du porteur avec les informations de l'application ou du signataire,
- la période de validité du certificat,
- la capacité du certificat à être utilisé pour la signature (contrôle des «key usages»),
- la validation de sa chaîne de certification,
- la correspondance entre le certificat et la clé privée,
- Les usages de clés sont cohérents avec ceux définis dans la demande (dans le cas où les usages de clé sont définis).

Lorsque la validation aboutit avec succès, le fichier PKCS#12 est exploité par le serveur de signature afin d'en extraire d'une part la biclé et d'autre par le certificat de signature.

Le couple clé privée/certificat est transmis au HSM pour le transformer en jeton de clé. Ce jeton est un chiffrement de la biclé par une clé de chiffrement se trouvant dans le HSM.

Le mot de passe du PKCS#12 n'est donc pas sauvegardé dans le serveur de signature.

Le jeton de clé est alors utilisé comme clé de signature pour l'application de signature ou le signataire.

3.4.5 Dépôt d'un certificat de signature correspondant à une CSR existante

Lorsqu'une requête de certification a été émise par le serveur de signature, celle-ci doit être transmise à une IGC pour obtenir un certificat de signature.

Lorsque le certificat a été produit, celui-ci doit alors être introduit dans le serveur de signature pour rendre opérationnel la biclé et le certificat pour des opérations de signature de document.

Pour cela, une application de confiance pour le compte d'un signataire ou un signataire ou, une application de signature pour son propre compte, effectue une opération de dépôt de certificat de signature correspondant à la CSR ayant servi à la production du certificat.

L'appelant fournit alors :

- l'identifiant de la clé de signature
- le certificat de signature
- le secret d'activation de signature

Le serveur effectue un ensemble de validation :

- la CSR existe et correspond au certificat (La correspondance est réalisée grâce à la présence de l'identifiant de clé qui doit s'y trouver)
- Le secret d'activation de signature est vérifié
- la correspondance entre la clé publique du certificat et la clé privée associée sur le serveur
- le certificat est ensuite vérifié (validité, chaîne de certification, non révocation).

Lorsque la validation aboutit avec succès, le couple clé/certificat est sauvegardé comme clé de signature et le serveur en retournera l'identifiant à l'appelant.

4 Gestion des utilisateurs

4.1 Généralités

Les fonctionnalités de gestion des utilisateurs recouvrent :

- les opérations d'enregistrement de nouveaux utilisateurs, de gestion de leurs droits, de suppression de comptes utilisateurs et de mise à jour des informations.
- les opération de gestion de groupes dans lesquels les utilisateurs peuvent êtres affectés.

Les enrôlements des utilisateurs sont réalisés par un administrateur qui peut enregistrer un utilisateur en remplissant les informations d'enregistrement.

Un utilisateur peut être inscrit dans un ou plusieurs groupes et disposera d'un ou plusieurs rôles.

Un groupe permet aux utilisateurs qui y sont déclarés de pouvoir utiliser les composants de paramètres de signature tels que les politiques de signature, les profils de signature ou les profils de clés de signature qui ont été associés lors de leur création (ou leur mises à jour) sur le serveur.

Le serveur de signature offre les services suivants pour la gestion des utilisateurs et des groupes :

- Création d'un utilisateur;
- Mise à jour des données d'un utilisateur;
- Suppression d'un utilisateur;
- Consultation d'une liste d'utilisateur;
- Création d'un groupe;
- Ajout d'un ou plusieurs utilisateur(s) à un groupe
- Retrait d'un ou plusieurs utilisateur(s) d'un groupe
- Suppression d'un groupe
- Consultation d'une liste de groupes

4.2 Opérations sur les utilisateurs

4.2.1 Demande d'enregistrement d'un nouvel utilisateur

Pour qu'un nouvel utilisateur puisse effectuer une demande d'enregistrement au système de signature sur une application Web, celui-ci doit être déclarée en tant qu'application de confiance ayant alors les droits d'administrateur.

L'application fournit au serveur de signature les informations correspondant au type de « compte utilisateur » qu'il souhaite ouvrir.

Ces informations regroupent obligatoirement :

- un nom d'utilisateur;
- l'affectation à un ou plusieurs rôles : Application de confiance, Signataire; Application de signature ou l'un des types d'Administrateur;

- optionnellement un ou plusieurs groupes auxquels l'utilisateur doit appartenir;
- un ou plusieurs type d'authentification auprès du serveur (login – mot de passe ; certificat produit par une IGC externe);
- l'identification des applications pour lesquelles l'utilisateur fera confiance.

4.2.2 Mise à jour des données d'un utilisateur

Après s'être connecté et authentifié auprès du serveur de signature, un utilisateur effectue une opération de mise à jour de son profil.

Il peut modifier toutes les informations le concernant, en particulier:

- le nom de l'utilisateur permettant de l'identifier;
- le ou les modes d'authentification de l'utilisateur (mot de passe, ou certificat). Au moins un mode doit subsister;
- le ou les rôles dont il dispose;
- le ou les groupes auxquels il appartient;
- le ou les applications auxquelles l'utilisateur donne délégation.

4.2.3 Suppression d'un utilisateur

La suppression d'un utilisateur n'est autorisée que par :

- une Application de Confiance
- un utilisateur ayant les droits d'Administrateur sur le serveur de signature.
- un Administrateur appartenant au groupe où l'utilisateur est affecté.

L'appelant fournit au serveur l'identifiant correspondant à l'utilisateur qu'il souhaite supprimer.

4.2.4 Consulter une liste d'utilisateurs

Un administrateur a la possibilité de consulter une liste d'utilisateur du serveur de signature en accord avec un ensemble de critères tels que :

- toute ou partie du nom des utilisateurs;
- les identifiants des utilisateurs.

L'appelant récupère alors l'ensemble des informations pour chacun des utilisateurs correspondant aux critères sélectionnés:

- leur nom d'utilisateur;
- leur(s) mode(s) d'authentification;
- leur(s) rôle(s);
- le ou les groupes auxquels l'utilisateur appartient;
- le ou les applications auxquelles l'utilisateur donne délégation.

4.3 Opérations sur les groupes

4.3.1 Création d'un nouveau groupe

La demande de création d'un nouveau groupe n'est autorisée que par une application ou un utilisateur ayant les droits d'Administrateur sur le serveur de signature.

L'appelant renseigne les informations destinées à identifier le groupe :

- le nom du groupe,
- optionnellement, une liste d'identifiants de groupes existants à ce groupe;
- optionnellement, une liste d'identifiant d'utilisateurs assignés à ce groupe.

Le nouveau groupe est alors créé et référencé dans le serveur de signature, il pourra être utilisé pour être associés à des composants de paramètres de signature (politiques de signature, profils de signature, profils de clés de signature) du serveur de signature ou pour y ajouter des utilisateurs.

Si, lors de la création du groupe, celui-ci existe déjà, alors une erreur sur la création du groupe est renvoyé à l'administrateur.

4.3.2 Ajout d'un ou plusieurs utilisateur(s) à un groupe

Un administrateur peut ajouter des utilisateurs à un ou plusieurs groupes définis.

Il renseigne alors les informations destinées à identifier le groupe :

- une ou plusieurs associations groupe/utilisateurs

Une association groupe/utilisateur est composée de :

- l'identifiant d'un groupe
- un ou plusieurs identifiant(s) d'utilisateur(s)

Les utilisateurs alors associés au groupe peuvent utilisés les composants de paramètres de signature inclus dans ce groupe lors des différents opérations sur le serveur de signature.

4.3.3 Retrait d'un ou plusieurs utilisateur(s) d'un groupe

Un administrateur peut retirer des utilisateurs à un groupes définis.

Il renseigne alors les informations destinées à identifier le groupe et les utilisateurs à retirer

Pour cela, il utilise une association groupe/utilisateur composée de :

- l'identifiant d'un groupe
- un ou plusieurs identifiant(s) d'utilisateur(s) devant être retiré du groupe

Les utilisateurs sont alors retirés du groupe et ne pourront plus utiliser les paramètres de signature inclus dans ce groupe lors des différents opérations sur le serveur de signature.

4.3.4 Suppression d'un groupe

La suppression d'un groupe n'est autorisée que lorsque ce groupe ne contient plus d'utilisateurs. Pour ce faire, l'administrateur aura alors au préalable retirer les utilisateurs du groupe.

L'appelant fournit au serveur l'identifiant correspondant au groupe qu'il souhaite supprimer.

4.3.5 Consulter une liste de groupes

Un administrateur a la possibilité de consulter une liste de groupe du serveur de signature en accord avec un ensemble de critères tels que :

- toute ou partie du nom des groupes;
- les identifiants des groupes.

L'appelant récupère alors l'ensemble des informations pour chacun des groupes correspondant aux critères sélectionnés:

- leur nom de groupe;
- la liste d'identifiants de groupes existants à ce groupe;
- la liste d'identifiant d'utilisateurs assignés à ce groupe.

4.4 Processus d'enrôlement des utilisateurs

L'enrôlement d'un utilisateur consiste non seulement à créer cet utilisateur sur le serveur de signatures avec les informations qui lui son propre mais aussi à lui associer tous les éléments du serveur de signature dont il aura besoin pour utiliser les opérations associés à son rôle sur le serveur.

4.4.1 Enrôlement d'un gestionnaire

L'enrôlement d'un gestionnaire ou d'une application de gestion ne peut être faite que par une application d'administration (ou un utilisateur ayant le rôle d'administrateur).

Lorsque le gestionnaire ou une application de gestion sera déclarée sur le serveur de signature, il pourra gérer les éléments nécessaires aux opérations de signature (politiques de signature, profils de signature, profils de génération de clé)

Pour cela un administrateur de l'application d'administration réalise une demande de création d'utilisateur du serveur de signature en renseignant les informations suivantes :

- le nom de l'application de gestion ou du gestionnaire (utilisateur);
- le certificat qui permettra à l'application ou au gestionnaire de s'authentifier sur le serveur de signature;
- le rôle de gestionnaire (SignManager);
- optionnellement, les applications auxquelles, elle fait confiance;
- optionnellement, les groupes auxquelles l'application doit appartenir.

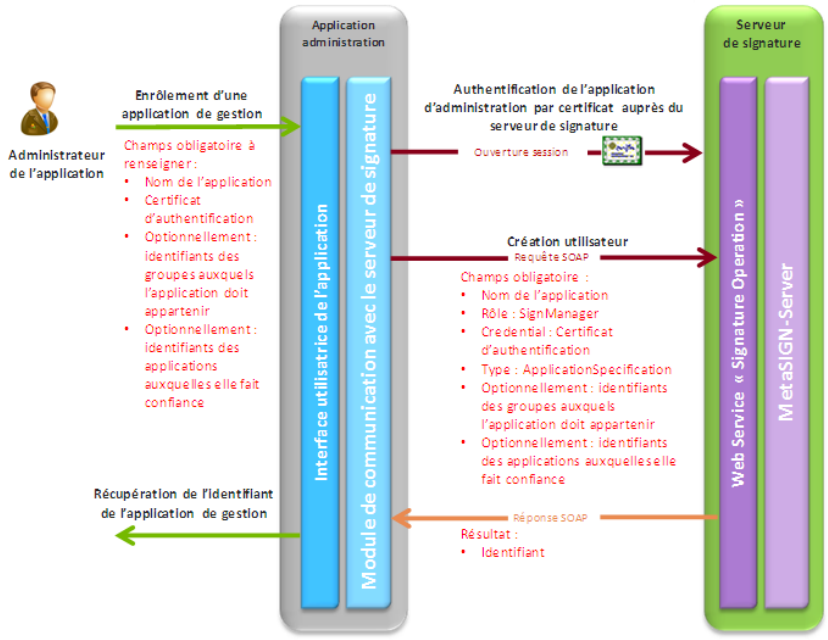

Figure 7: Enrôlement d'une application de gestion

4.4.2 Enrôlement d'un administrateur

L'enrôlement d'un administrateur ou d'une application d'administration ne peut être faite que par une autre application d'administration.

Lorsque l'administrateur ou une application d'administration sera déclarée sur le serveur de signature, il pourra administrer les utilisateurs et/ou les groupes associés.

Pour cela un administrateur de l'application d'administration réalise une demande de création d'utilisateur du serveur de signature en renseignant les informations suivantes :

- le nom de l'application d'administration ou de l'administrateur (utilisateur);
- le certificat qui permettra à l'application ou à l'administrateur de s'authentifier sur le serveur de signature;
- le rôle d'administrateur (Admin);
- optionnellement, les applications auxquelles, elle fait confiance;
- optionnellement, les groupes auxquelles l'application doit appartenir.

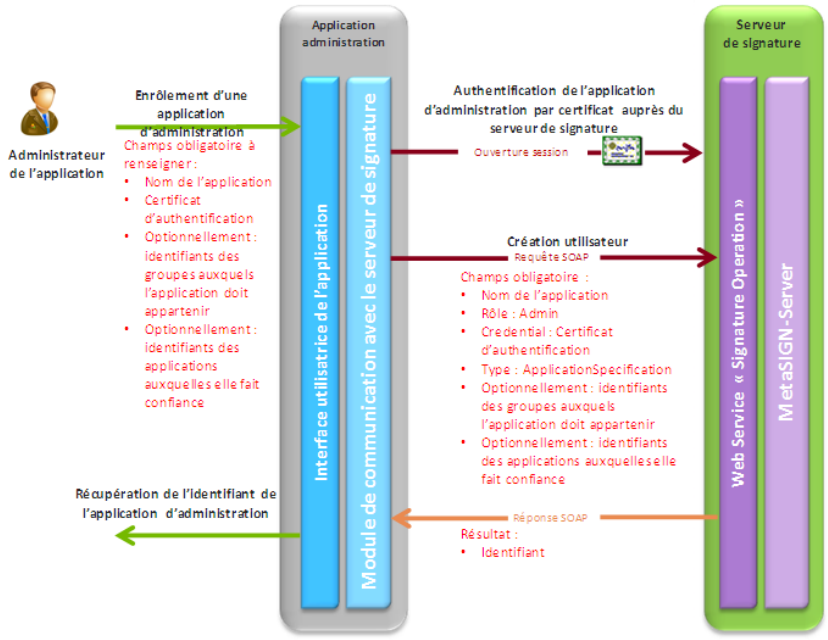

Figure 8 : Enrôlement d'une application d'administration

4.4.3 Enrôlement d'une application de confiance

L'enrôlement d'une application de confiance ne peut être faite que par une application ou un utilisateur ayant le rôle d'administrateur.

Pour cela un administrateur de l'application d'administration réalise une demande de création d'utilisateur du serveur de signature en renseignant les informations suivantes :

- le nom de la nouvelle application de confiance (utilisateur);
- le certificat qui permettra à l'application de confiance de s'authentifier sur le serveur de signature;
- le type d'utilisateur : application de confiance (TrustedApplication);
- le ou les rôles associées à cette application;
- optionnellement, les applications auxquelles, elle fait confiance;
- optionnellement, les groupes auxquelles l'application doit appartenir.

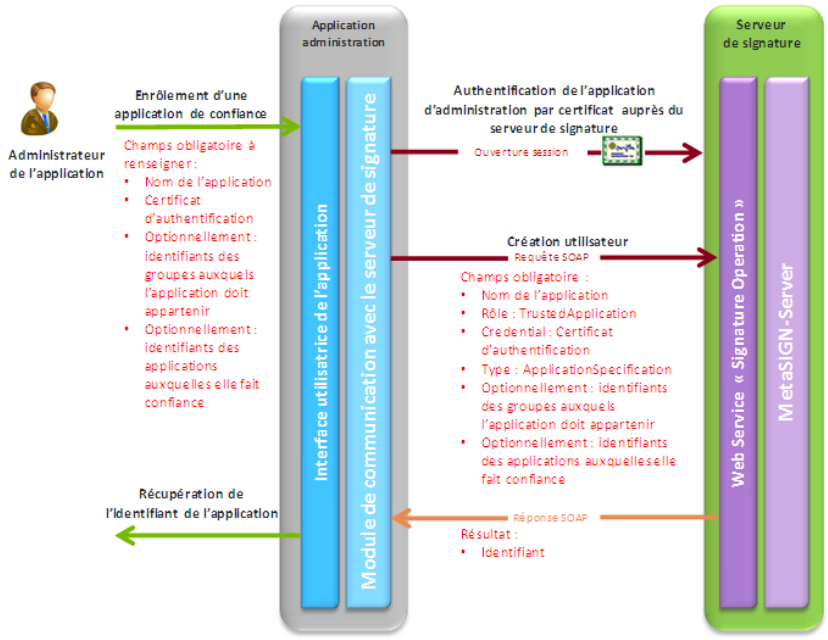

Figure 9 : Processus d'enrôlement d'une application de confiance

4.4.4 Enrôlement des signataires

L'enrôlement des signataires ne peut être faite que par une application ayant différents rôles sur le serveur de signature.

En effet, l'enrôlement d'un signataire est réalisé en deux étapes :

- La déclaration de l'utilisateur en tant que signataire : l'application doit alors avoir un rôle d'administrateur sur le serveur de signature;
- l'affectation d'une clé de signature et de son certificat associé : l'application doit alors avoir un rôle de gestionnaire sur le serveur de signature;

Pour déclarer un utilisateur en tant que signataire, l'application réalise une demande de création d'utilisateur du serveur de signature en renseignant les informations suivantes :

- le nom de l'utilisateur;
- le rôle de l'utilisateur : Signer;
- optionnellement, les applications auxquelles, elle fait confiance;
- optionnellement, les groupes auxquelles l'application doit appartenir.

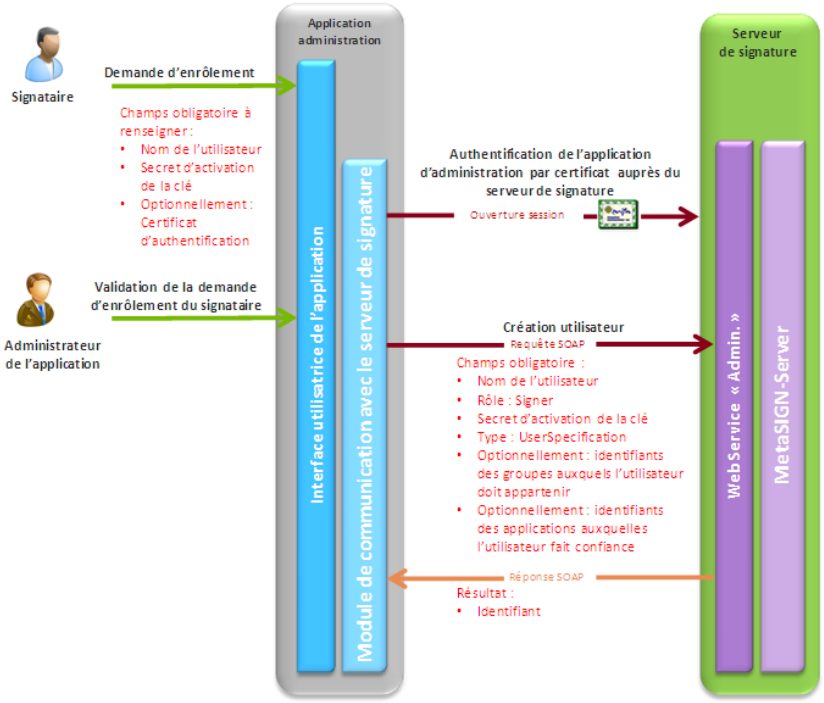

Figure 10 : Processus de déclaration d'un signataire

Lors que le signataire est déclaré dans le serveur de signature, celui-ci doit détenir au moins une clé de signature et son certificat associé afin d'effectuer des opération de signature.

Le processus d'obtention d'une clé de signature et de son certificat peut se faire de deux façons différentes :

- Soit le signataire dispose déjà d'une biclé de signature et de son certificat contenu dans un conteneur PKCS#12;
- Soit l'application doit demander auprès du serveur de signature la génération d'une biclé et obtenir une demande de certificat (CSR). Cette demande sera ensuite transmise à une IGC externe afin d'obtenir un certificat de signature et de le déposer dans le serveur de signature ;
- Soit l'application doit demander auprès du serveur de signature la génération d'une biclé et d'effectuer une requête de demande de certificat. Cette demande sera ensuite transmise à une IGC externe à travers un protocole (l'adresse externe, le protocole et les paramètres inhérents font partie de la configuration du serveur de signature) afin d'obtenir un certificat de signature (il sera automatiquement déposé dans le serveur de signature);

Attribution d'une clé de signature par dépôt de PKCS#12

Lorsque le signataire dispose de sa biclé et de son certificat, l'application réalise un dépôt du fichier PKCS#12 et l'associe au signataire auprès du serveur de signature en renseignant les informations suivantes :

- l'identifiant du signataire;
- le fichier PKCS#12 et sa passphrase;

- un Secret d'Activation du conteneur de clé du signataire;
- un identifiant de clé.

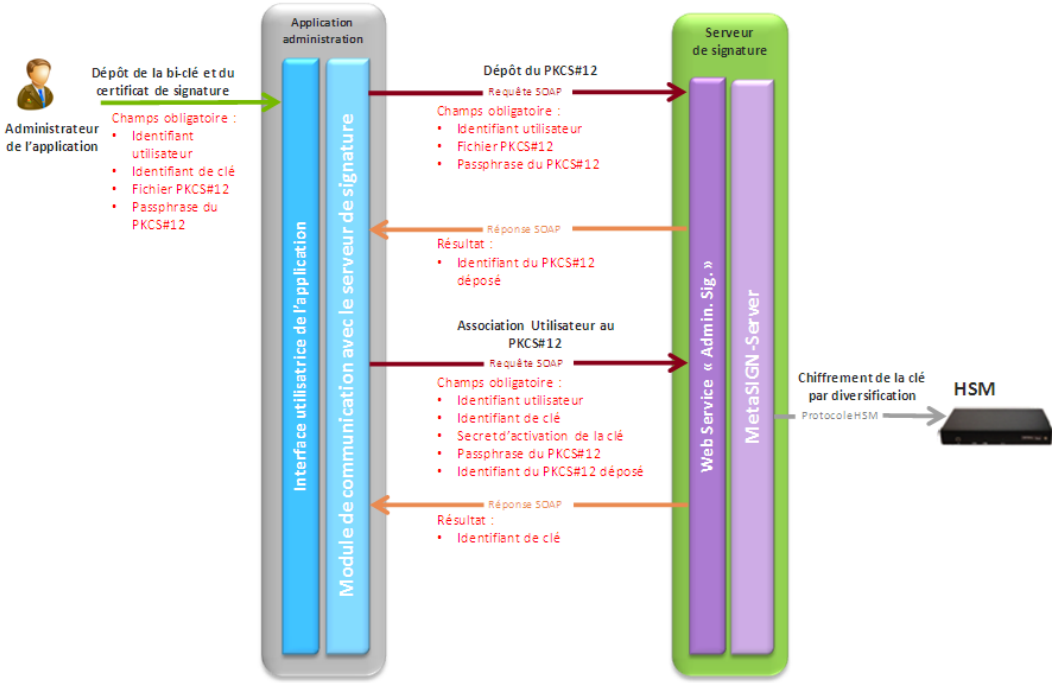

Figure 11 : Processus d'association d'une biclé de signature sous forme PKCS#12 à un signataire

Attribution d'une clé de signature par génération de clé et demande de certification

Dans le cas où le signataire ne dispose pas de biclé signature et de certificat, l'application peut effectuer une demande de génération de biclé de signature et d'obtention d'une demande de certificat (sous forme de fichier CSR) pour le signataire auprès du serveur de signature en renseignant les informations suivantes :

- l'identifiant du signataire;
- un identifiant de clé;
- un Secret d'Activation du conteneur de clé du signataire;
- un profil de clé de signature (ou son identifiant si celui-ci existe déjà sur le serveur);

L'application obtient alors un fichier contenant une demande de certificat signée par la clé privée générée afin qu'il puisse demander un certificat auprès d'une IGC.

Lorsque l'application a obtenu le certificat, elle réalise le dépôt de ce certificat pour le signataire sur le serveur de signature en renseignant les informations suivantes:

- l'identifiant du signataire;
- un identifiant de clé;

- un Secret d'Activation du conteneur de clé du signataire;
- le certificats de signature au format X509.

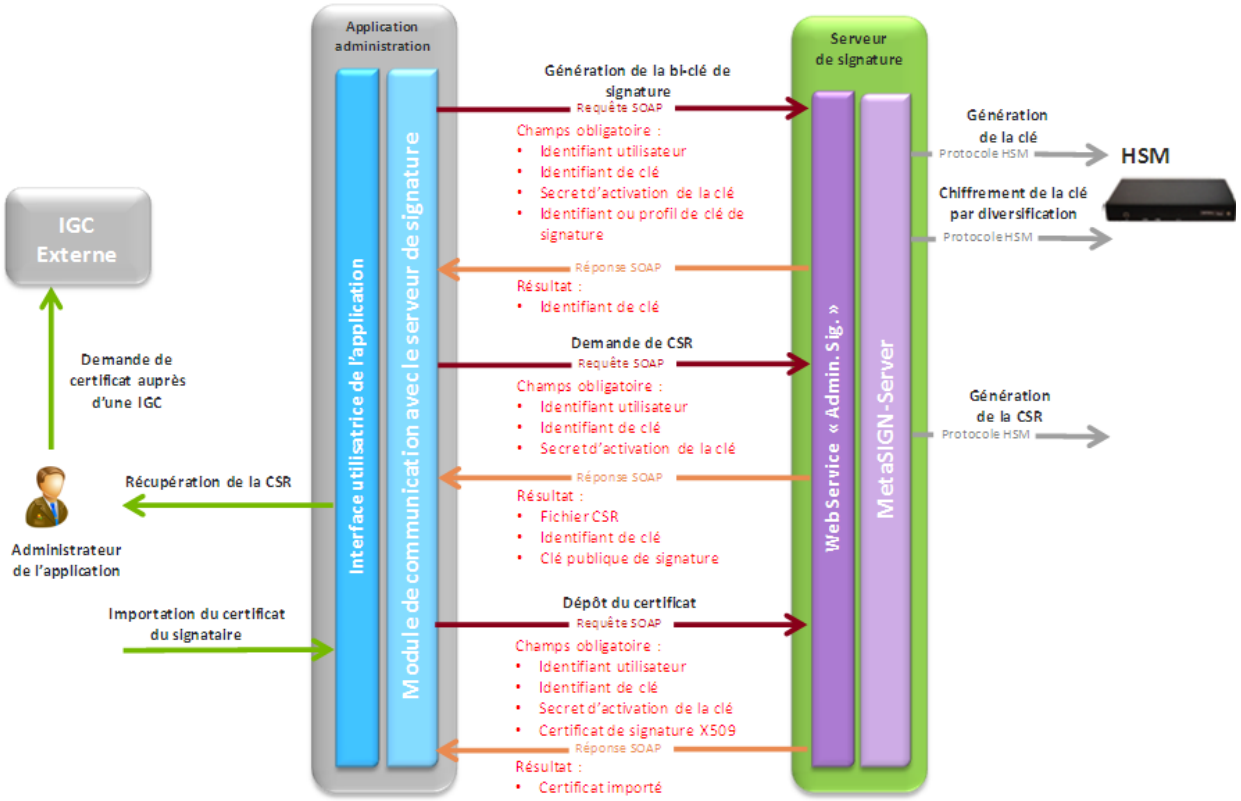

Figure 12 : Processus d'obtention d'une biclé et d'un certificat pour un signataire

Attribution d'une clé de signature par génération de clé et demande de certification via le serveur de signature

Dans le cas où le signataire ne dispose pas de biclé signature et de certificat, l'application peut effectuer une demande de génération de biclé de signature auprès du serveur de signature en renseignant les informations suivantes :

- l'identifiant du signataire;
- un identifiant de clé;
- un Secret d'Activation du conteneur de clé du signataire;
- un profil de clé de signature (ou son identifiant si celui-ci existe déjà sur le serveur);

Ainsi, le signataire possède une biclé protégée par son secret d'activation et la clé maître du serveur de signature.

Ensuite, l'application peut effectuer une demande de génération de certificat de signature auprès du serveur de signature en renseignant les informations suivantes :

- l'identifiant du signataire;
- un identifiant de clé;
- un Secret d'Activation du conteneur de clé du signataire;
- des paramètres inhérents au protocole utilisé (SCEP, A2M, CMP…).

Le serveur de signature peut alors répondre de deux facons :

1. le certificat est retourné (le certificat a pu être généré automatiquement au niveau de l'IGC) ;

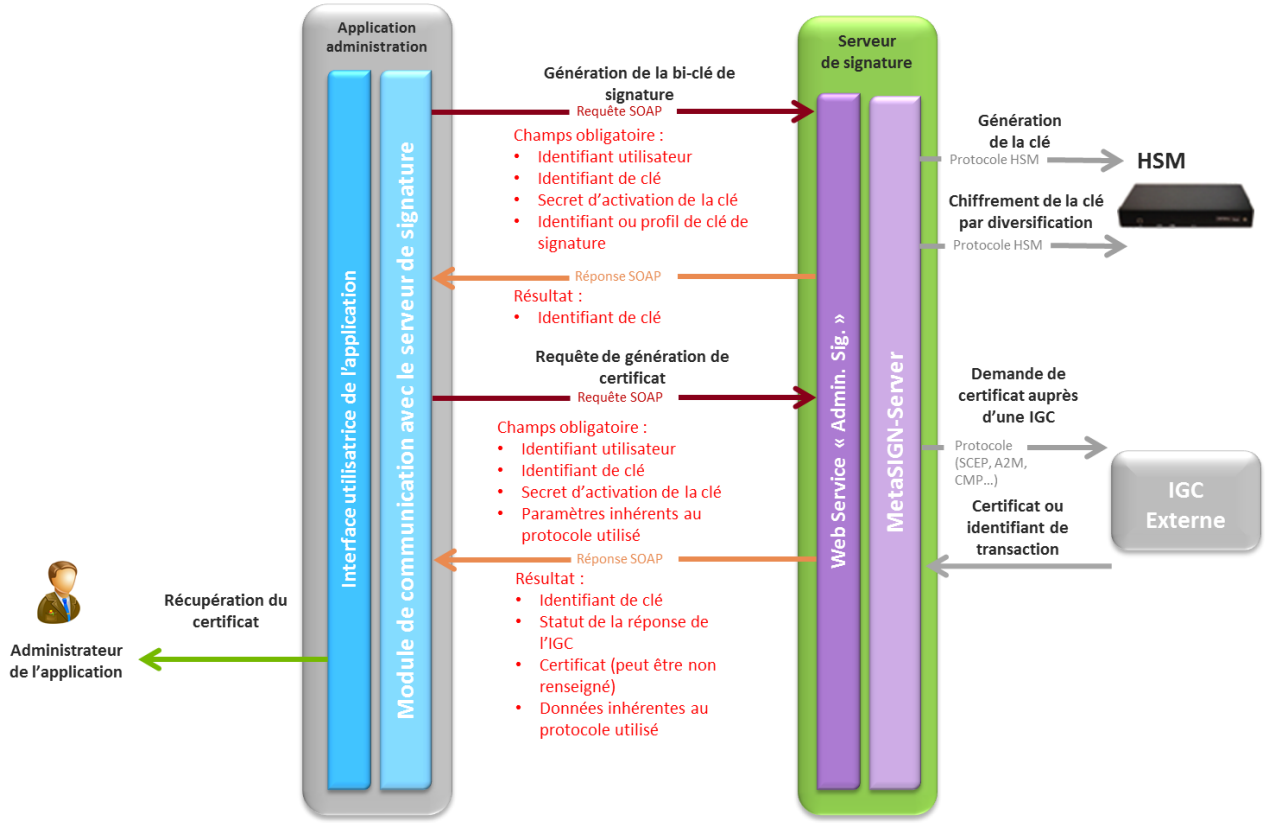

Figure 13 : Processus d'obtention d'une biclé et d'un certificat pour un signataire (1)

2. le certificat n'est pas retourné, mais un identifiant de transaction est renseigné (la génération du certificat nécessite une opération manuelle au niveau de l'IGC).

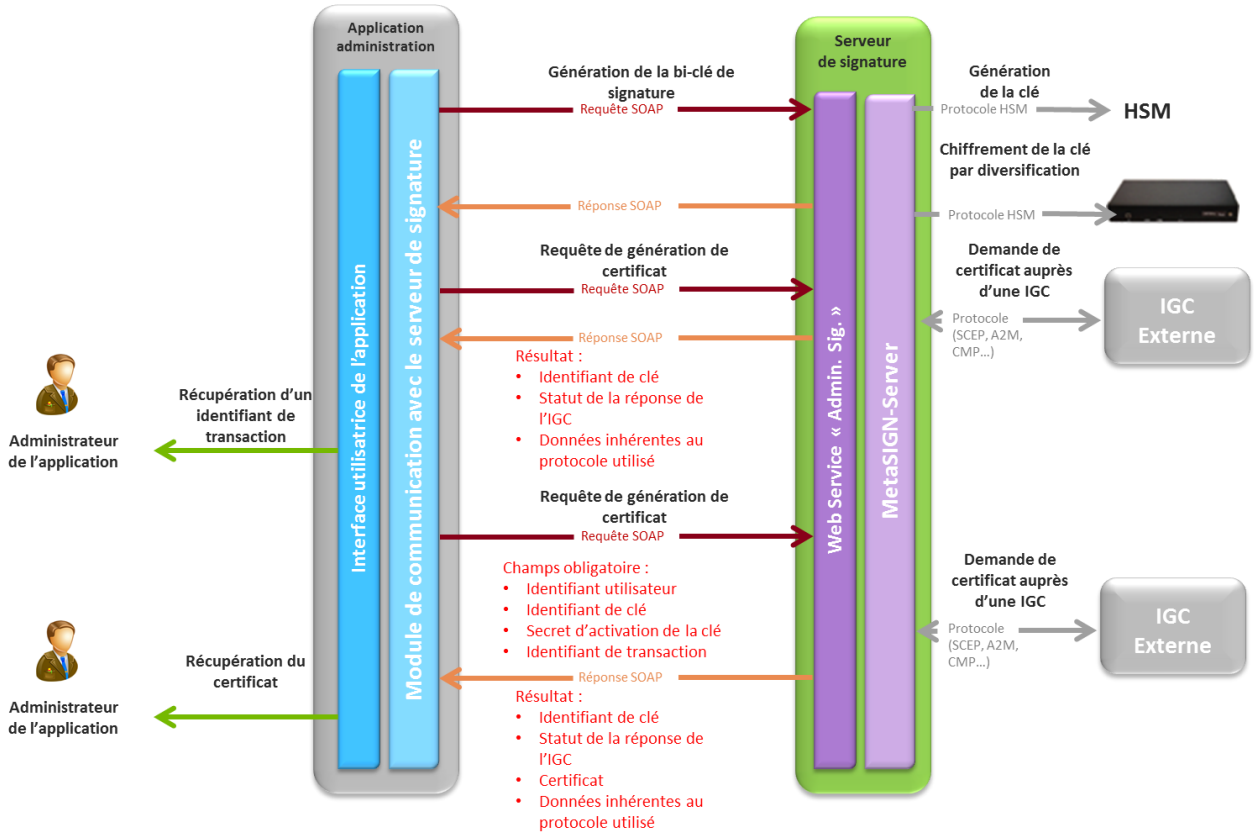

Figure 14 : Processus d'obtention d'une biclé et d'un certificat pour un signataire (2)

Dans le cas 2, l'application doit refaire une (ou plusieurs) demande(s) de génération de certificat en fournissant l'identifiant de transaction jusqu'à récupérer le certificat du signataire (dépendant de l'opération manuelle coté IGC).

Le dépôt du certificat est effectué automatiquement par le serveur de signature dès lors que le certificat est retourné dans la réponse.

4.4.5 Enrôlement d'un signataire FIDO

Si le signataire doit utiliser une clé de signature avec authentification auprès d'un token FIDO, il doit d'abord s'enrôler auprès du token FIDO.

Il doit d'abord initialiser son enrôlement puis renvoyer les données récupérées à une application web gérant l'authentification FIDO. Les données renvoyées par le token FIDO doivent ensuite être déposées sur le serveur de signature afin de récupérer un identifiant de token FIDO.

Ensuite, la clé de signature peut être créée et elle devra être activée avant de pouvoir générer une CSR pour l'obtention d'un certificat.

4.4.6 Enrôlement de signataires Cachet

Un « Signataire Cachet » a pour rôle de signer des documents pour le compte d'une entité légale ou

d'une entreprise. Ce signataire est bien souvent une application.

Le clé de signature d'un « Signataire Cachet » doit être gérée en respectant des processus et règles garantissant que celle-ci a été produite dans un environnement sécurisé. C'est pour cela que ces clés sont généralement générées lors de cérémonie de clé dans le HSM. La biclé est alors connue sous un identifiant donné par le HSM et n'est jamais extraite du HSM.

De plus, l'authentification de l'application « Signataire Cachet » auprès du serveur de signature doit se faire par authentification certificat.

L'enrôlement d'un signataire « Cachet » ne peut être faite que par une application ayant différents rôles sur le serveur de signature.

En effet, l'enrôlement d'un signataire « Cachet » est réalisé en trois étapes :

- La génération de la biclé dans le HSM lors d'une cérémonie de clé;
- La déclaration de l'utilisateur (application) en tant que « Signataire » : l'application doit alors avoir un rôle d'administrateur sur le serveur de signature;
- l'affectation d'une clé de signature générée préalablement dans le HSM lors d'une cérémonie de clés et de son certificat associé : l'application doit alors avoir un rôle de gestionnaire sur le serveur de signature;

Pour déclarer un utilisateur (application) en tant que « Signataire Cachet », l'application réalise une demande de création d'utilisateur du serveur de signature en renseignant les informations suivantes :

- le nom de l'utilisateur;
- le rôle de l'utilisateur : Signer;
- Le certificat d'authentification de l'utilisateur;
- Le secret d'activation du conteneur de clé;
- optionnellement, les groupes auxquelles l'application doit appartenir.

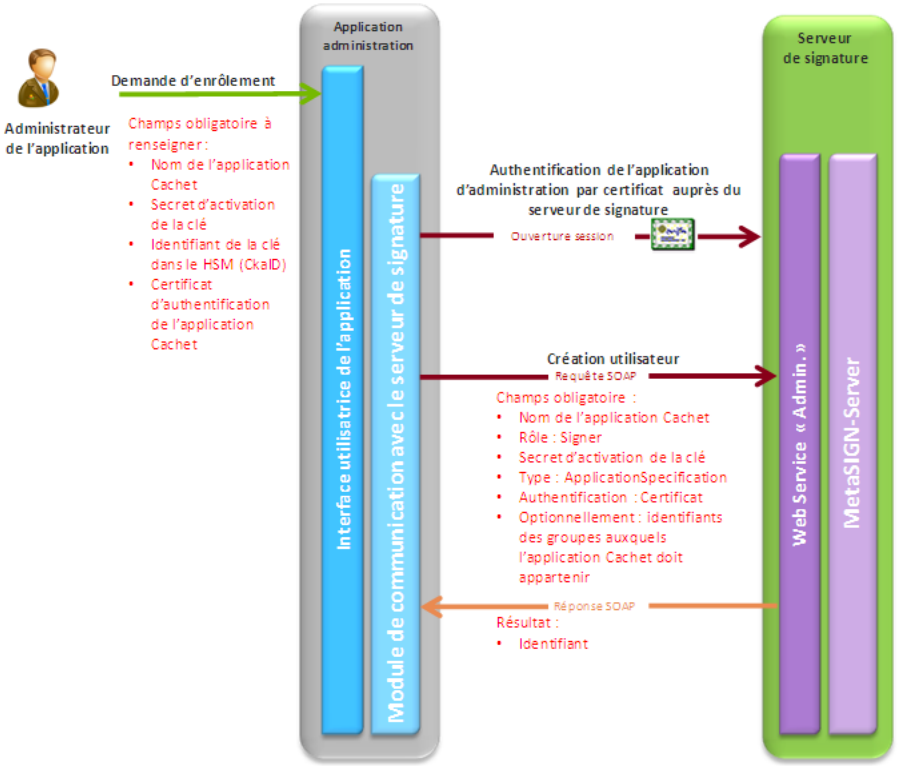

Figure 15 : Processus de déclaration d'un signataire cachet

L'application effectue ensuite :

1. soit une demande de certificat (sous forme de fichier CSR) pour le « Signataire Cachet » auprès du serveur de signature en renseignant les informations suivantes :
    - l'identifiant du signataire;
    - l'identifiant de clé CkaID dans le HSM
    - un identifiant de clé pour le serveur de signature;
    - un Secret d'activation du conteneur de clé du signataire;
    - le profil de clé.

L'application obtient alors un fichier contenant une demande de certificat signée par la clé privée correspondant au CkaID afin qu'il puisse demander un certificat auprès d'une IGC.

Lorsque l'application a obtenu le certificat, elle réalise le dépôt de ce certificat pour le signataire sur le serveur de signature en renseignant les informations suivantes:

- l'identifiant du signataire;
- un identifiant de clé;
- un Secret d'Activation du conteneur de clé du signataire;
- le certificats de signature au format X509.

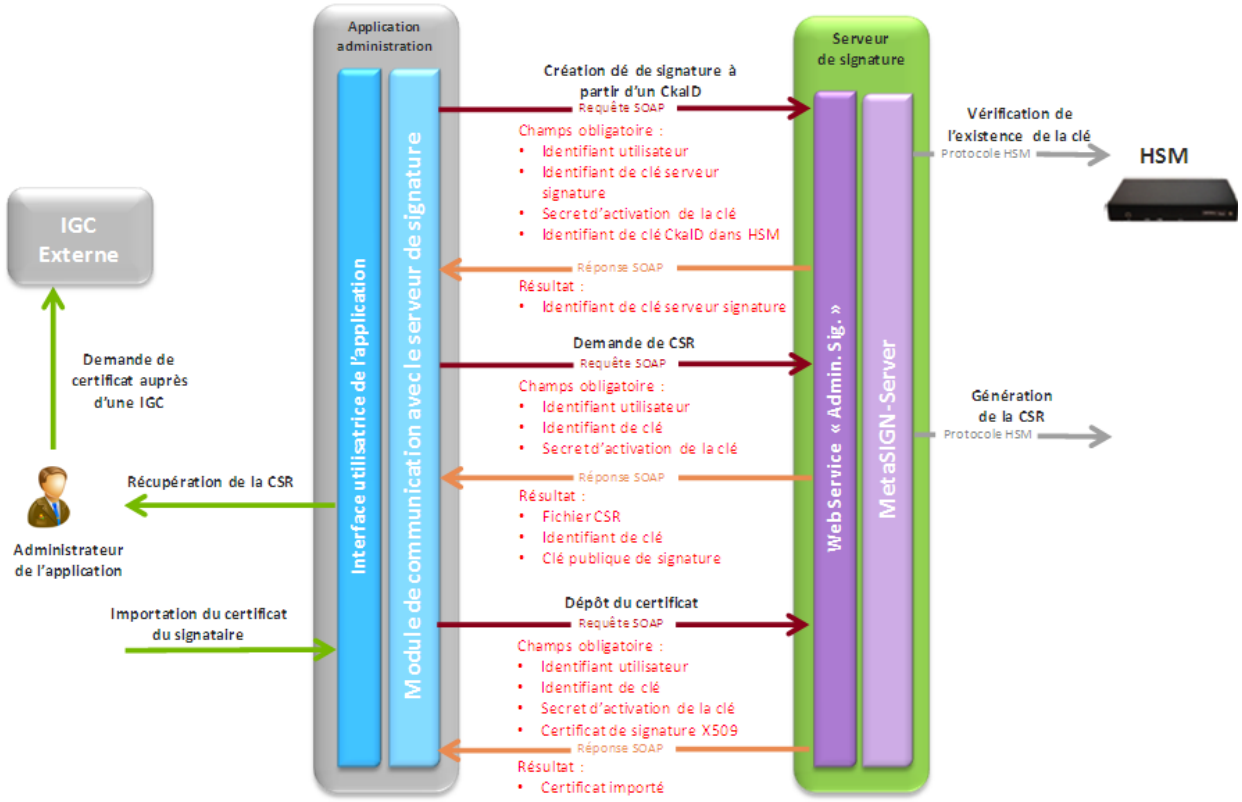

Figure 16 : Processus d'obtention d'un certificat pour un signataire cachet

2. soit une demande de génération de certificat pour le « Signataire Cachet » auprès du serveur de signature en renseignant les informations suivantes :
   - l'identifiant du signataire;
   - l'identifiant de clé CkaID dans le HSM
   - un Secret d'activation du conteneur de clé du signataire;
   - les paramètres inhérents au protocole utilisé.

Le certificat du signataire est alors retourné et automatiquement déposé dans le serveur de signature pour le signataire.

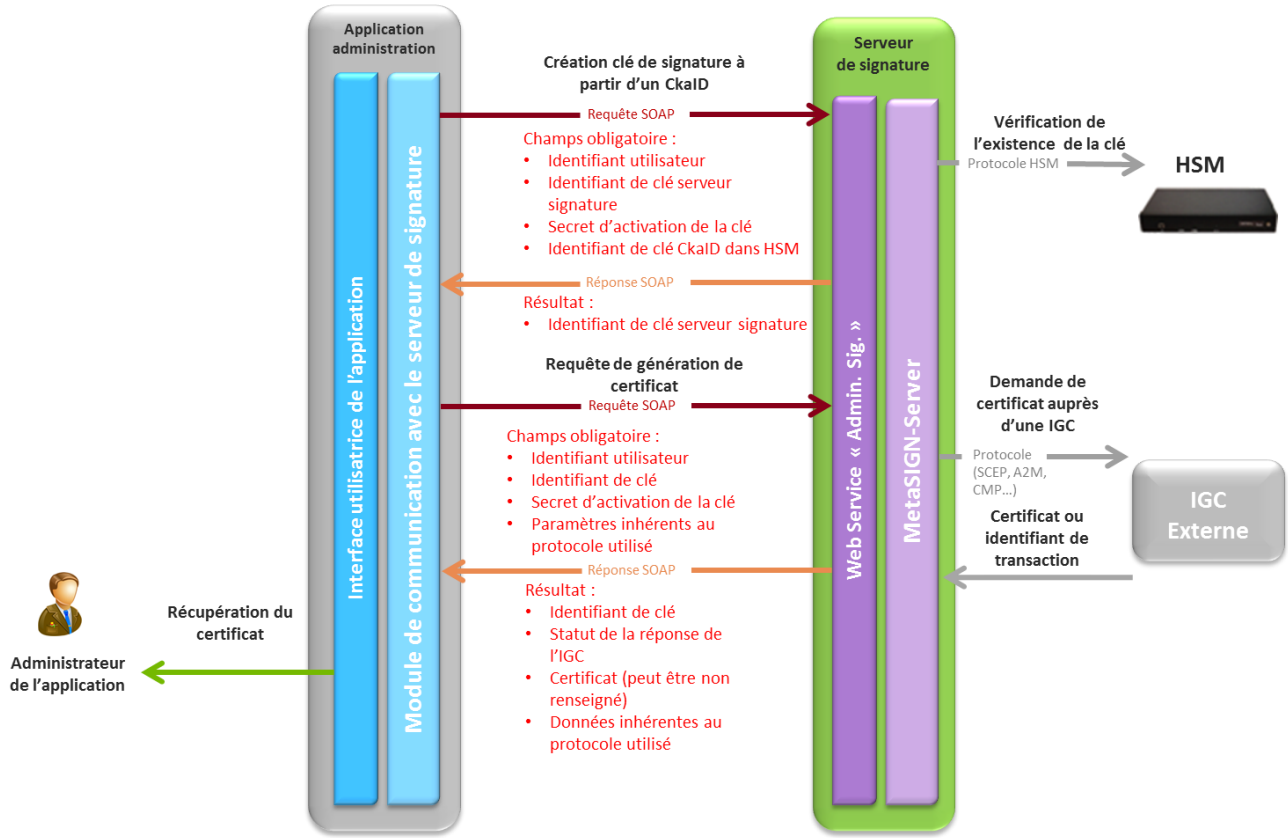

Figure 17 : Processus d'obtention d'un certificat pour un signataire cachet (2)

Il est possible que le certificat ne soit pas retourné par l'IGC (nécessite une opération manuelle coté IGC). Dans ce cas, un identifiant sera retourné par le serveur de signature afin de pouvoir ré-effectuer la demande du certificat (voir Figure 14).