



Sage XRT Communication & Signature

Version 4.2

Nouveautés

Sommaire

Présentation	3
Gestion de l'authentification	4
Api d'exploitation.....	6
Support de l'enveloppe personnalisée	10
Gestion des protocoles cryptographiques	11
Divers	13

Présentation

Ce document liste les nouvelles fonctionnalités disponibles dans la version 4.2 de **Sage XRT Communication & Signature**.

Cette version a été réalisée pour faciliter les échanges de fichiers entre l'application **Sage XRT Advanced** et l'application **Sage XRT communication & signature**.

Important ! Cette version n'est pas compatible avec les versions 4.1 et inférieures de **Sage XRT Treasury**.

Gestion de l'authentification

Paramètres/Configuration – onglet Authentification

Nom	Valeur
ApifmtPrinter	none
ApifmtResponseTimeout	900
AutoGenerateCertificate	true
http_servicehost_SCASServer	http://localhost:80/Auth
http_servicehost_SCDTSServer	http://localhost:80
http_servicehost_SCPSServer	http://localhost:80
https_servicehost_SCASServer	https://localhost:443/Auth
https_servicehost_SCDTSServer	https://localhost:443
https_servicehost_SCPSServer	https://localhost:443
securitylevel	http
SerialNumber	
StmtBaseTimeTry	5
StmtResponseTimeout	900

L'onglet **Authentification** regroupe :

- les options d'affichage de la page de connexion web (**Authentification forte** ou **SAML V2**)
- les informations du fichier de configuration *wrapper*

Sage.Fcs.Client permet de consommer de façon transparente un ensemble d'**API Rest** hébergé par les services d'authentification (**SCASServer**), d'administration (**SCPSServer**) et de fonctionnalités (**SCDTSServer**) de **Sage XRT Communication & Signature**.

Sage XRT Communication & Signature 4.2 intègre cette librairie et appelle des méthodes.

Le serveur **Sage XRT Communication & Signature** est localisé via le paramétrage du fichier de configuration *Sage.Fcs.Client.dll.config*.

Les paramètres indiqués sont prédéfinis. Vous pouvez les modifier en fonction de votre configuration, dans cette interface.

Gestion de l'authentification

Nom	Valeur	Commentaire
ApiFmtBaseTimeTry	2	Temporisation pour la partie <i>API</i> des formats
ApifmtPdfViewer	None	Outil d'affichage par défaut des Pdf.
ApifmtPrinter	None	Imprimante par défaut.
ApifmtResponseTimeout	900	Temps maximum de réponse de l' <i>Api</i> des formats.
AutoGenerateCertificate	true	Certificat autogénéré pour sécuriser les échanges
http_servicehost_SCASServer	http://localhost:80/Auth	Localisation du service d'authentification en http
http_servicehost_SCPSSServer	http://localhost:80	Localisation du service d'administration en http
http_servicehost_SCDTSServer	http://localhost:80	Localisation du service de fonctionnalité en http
https_servicehost_SCASServer	https://localhost:443/Auth	Localisation du service d'authentification en https
https_servicehost_SCPSSServer	https://localhost:443	Localisation du service d'administration en https
https_servicehost_SCDTSServer	https://localhost:443	Localisation du service de fonctionnalité en https
Securitylevel	http	Secure channel Http ou https
SerialNumber		Numéro de série du certificat si certificat autogénéré non utilisé
StmtBaseTimeTry	5	Non utilisé
StmtResponseTimeout	900	Non utilisé

Api d'exploitation

Le service **XRT ComSign Rest Api** vous permet d'échanger des données avec l'application **Sage XRT Communication & Signature** à l'aide de l'**Api Rest**.

Les **Api Rest** de production simple disponibles dans cette version permettent de suivre le parcours des flux bancaires en émission (ajout d'un fichier dans le poste de signature, envoi d'un fichier, suivi des statuts des fichiers).

Le service **XRT ComSign Rest Api** est installé avec l'application **Sage XRT Communication** et doit être démarré avec un compte de service.

Si elle est activée dans le fichier de configuration, la documentation des **Api Rest** est disponible sur [http\(s\)://Hostname:8888/comsign/swagger](http(s)://Hostname:8888/comsign/swagger). Vous pouvez consulter le détail des **Api** déjà disponibles dans cette version.

Information version Api

Show/Hide | List Operations | Expand Operations

Simple Production Api

Show/Hide | List Operations | Expand Operations

POST	/v1/pdssa/addfile	Add a file payment's orders using SimpleApi
POST	/v1/pdssa/getstatus	Get Job status into the pds using SimpleApi
POST	/v1/pdssa/getticket	Get signature ticket using SimpleApi (NOT IMPLEMENTED)
POST	/v1/pdssa/geturlwkpage	Get interactive url Page using SimpleApi
POST	/v1/commsa/sendfile	Send a file payment's orders using SimpleApi
POST	/v1/commsa/recvfile	Receive a file using SimpleApi (NOT IMPLEMENTED)
POST	/v1/commsa/getstatus	Get Job status into the Comm using SimpleApi
POST	/v1/commsa/getfilelist	Get file list using SimpleApi (NOT IMPLEMENTED)
POST	/v1/commsa/getfiledata	Get file's data using SimpleApi (NOT IMPLEMENTED)
POST	/v1/commsa/delfile	Delete file using SimpleApi (NOT IMPLEMENTED)
POST	/v1/commsa/getremittanceslip	Get remittance slip using SimpleApi (NOT IMPLEMENTED)

Certaines informations nécessaires au fonctionnement du service sont automatiquement récupérées lors de son installation.

Parfois, l'architecture souhaitée nécessite de définir certains paramètres (modification du *DSN*, de l'adresse de la machine, etc.).

Le tableau ci-dessous décrit le fichier de configuration *Sage.Eb.ComSign.Api.exe.config*.

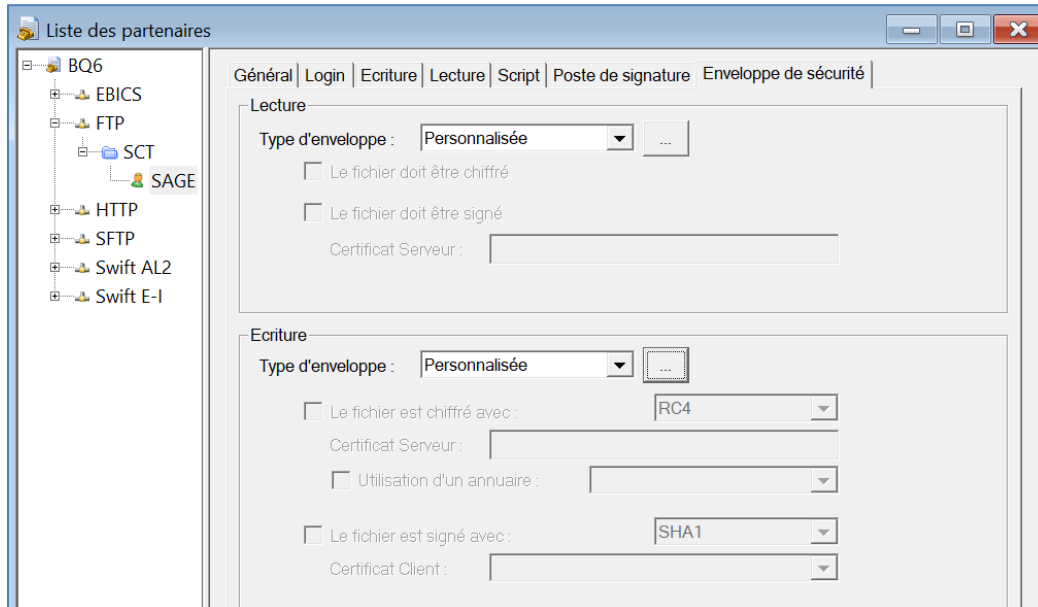
<appSettings>	Commentaires
<add key="UseSecureChannel" value="false" />	https ou http (par défaut http = false)
<add key="SecureChannelCertificateName" value="" />	Si non renseigné, par défaut True
<add key="DefaultAuthScheme" value="Ntlm" />	Méthode d'authentification : <ul style="list-style-type: none"> ▪ Par défaut, SageXrt (basée sur le service SCAS) ▪ Negotiate (<i>Ntlm</i> et/ou <i>Kerberos</i>) ▪ IntegratedWindowsAuthentication ▪ Basic ▪ Anonymous ▪ OAuth (Version <i>OAuth2</i>) ▪ Saml (Version <i>SamlV2</i>) ▪ Jwt (<i>Json Web Token</i>) ▪ Ntlm
<add key="Address" value="" />	Nom du serveur, par défaut nom de la machine
<add key="AdditionnalPath" value="comsign" />	Chemin d'accès à l' <i>Api Rest</i> par défaut comsign
<add key="Port" value="8888" />	Port d'accès de l' <i>Api Rest</i> par défaut 8888
Paramètres de l'authentification FCS	
<add key="SCAS" value="http://localhost " />	Si méthode d'authentification = SageXRT
<add key="SCPS" value="http:// localhost" />	Si méthode d'authentification = SageXRT


<appSettings>	Commentaires
Paramètres de l'authentification OAuth2 / Bearer	
<add key="OAuthDecryption" value="Auto" />	Clé de décryptage autogénérée
<add key="OAuthValidationAlgorithm" value="HMACSHA256" />	Algorithme de validation autogénérée
<add key="OAuthValidationKey" value="AutoGenerate,IsolateApps" />	Clé de validation autogénérée
<add key="OAuthDecryptionKey" value="AutoGenerate,IsolateApps" />	Clé de déchiffrement autogénérée
<add key="OAuthAccessTokenExpire" value="30" />	Valeur en minute de la durée de vie du <i>token</i> d'accès
<add key="OAuthModeSupport" value="TokenEndpointServer" />	Quand la valeur TokenEndPoint est renseignée, le <i>SRA</i> devient serveur d'identité et de <i>tokens</i> d'accès. Pour récupérer un <i>token OAuth2</i> valide il faut appeler l'adresse du <i>SRA</i> + <i>/token</i> . Si cette valeur n'est pas renseignée, le <i>SRA</i> se limite à un serveur de ressources.
Paramètres de l'authentification JWT / Bearer	
<add key="JWTRealm" value="" />	Domaine du <i>JWT</i>
<add key="JWTIssuer" value="" />	Valeur de l'émetteur
<add key="JWTAudience" value="" />	Valeur de l'audience
<add key="JWTSecret" value="" />	Valeur du secret
<add key="JWTCertificateFindValue" value="" />	Nom du certificat
<add key="JWTCertificateFindType" value="FindBySubjectDistinguishedName" />	Mode de recherche du certificat, par défaut <i>DN</i> du nom de l'objet du certificat

<appSettings>	Commentaires
Paramètres de l'authentification SAMLV2 / Bearer	
<add key="SAMLAudience" value="" />	Valeur de l'audience
<add key="SAMLIssuerThumbPrint" value="" />	Valeur de l'empreinte de l'émetteur
<add key="SAMLIssuerName" value="" />	Valeur du nom de l'émetteur
Log activation parameter	
<add key="LogFile" value="" />	Chemin et nom du log de l'application. Non activé par défaut
Workgroup	
<add key="eBankingUrl" value="" />	Non utilisé
<add key="UmapiWorkGroup" value="WORKGROUP" />	Nom du <i>Workgroup UMAPI</i> Par défaut Workgroup

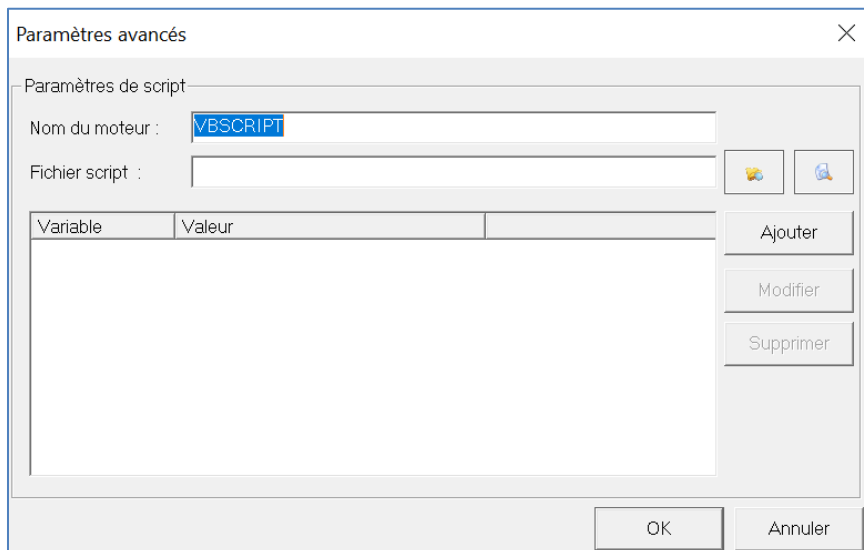
Support de l'enveloppe personnalisée


Sur les contrats bancaires, dans l'onglet **Enveloppe de Sécurité**, le type d'enveloppe **Personnalisée** a été ajouté.



Cliquez sur le bouton  pour accéder aux paramètres avancés.

Vous pouvez sélectionner ou créer un fichier script.



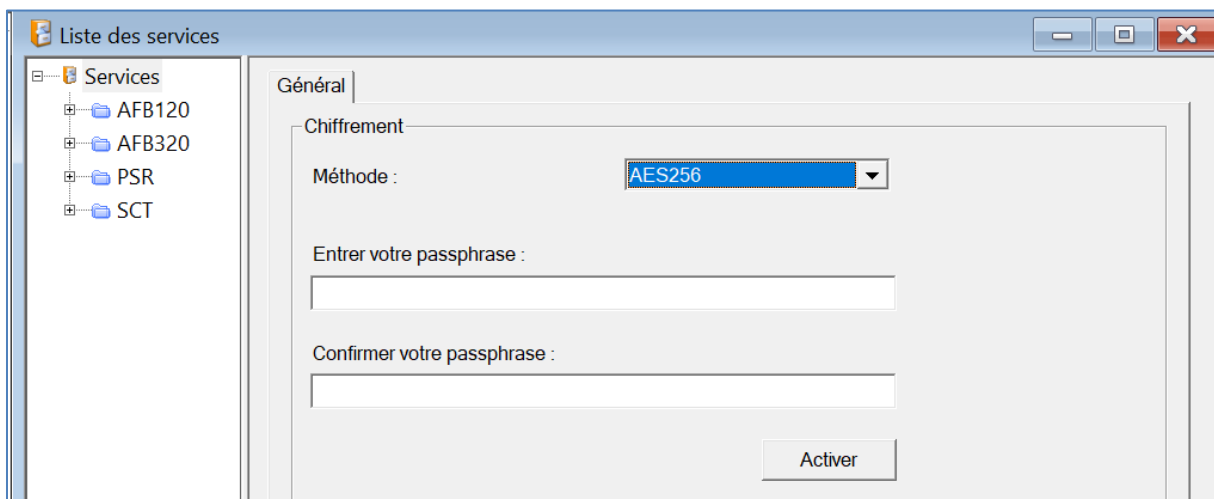
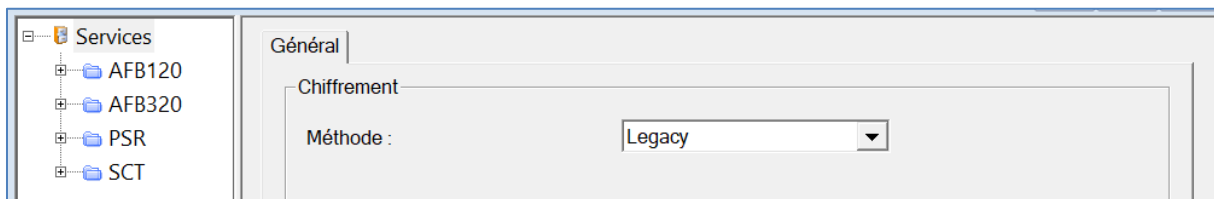
Si vous créez un fichier à partir du bouton , un *template* avec la fonction **décode** ou **encode** est disponible. Le fichier *template enveloppe.vbs* est livré dans le répertoire `\Workspace\Templates\`.

Gestion des protocoles cryptographiques

Dans le *WORKSPACE*, les fichiers peuvent désormais être cryptés selon la norme **AES256**.

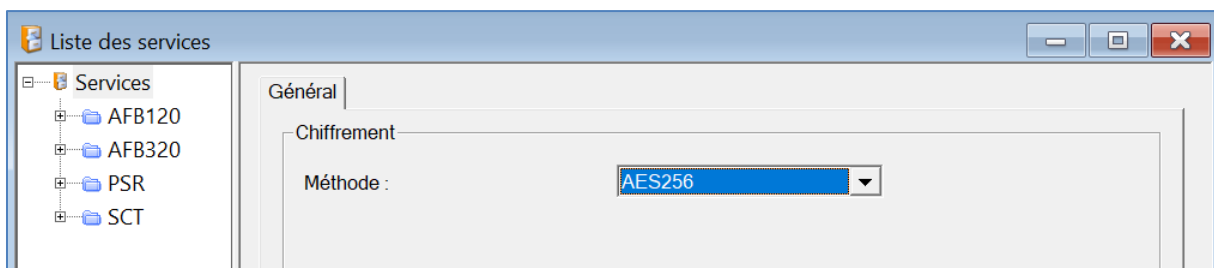
Pour les calculs de sceaux et la vérification des doublons, la fonction **SHA2-256** est utilisée.

Pour paramétrer le chiffrement **AES256**, la méthode **AES256** doit être sélectionnée au niveau du paramétrage des services.



Vous devez définir un *passphrase*, puis cliquer sur **Activer**.

Important ! Ce *passphrase* doit être conservé de manière sécurisée.



A partir de cette activation, tous les fichiers sont désormais chiffrés en **AES256**.

Note : Pour activer le chiffrement au niveau de chaque service concerné, sélectionnez les options de sécurité **Chiffrement des fichiers** et **Chiffrement des archives** dans l'onglet **Propriétés** du paramétrage.

The screenshot shows the 'Paramétrage' window with the 'Propriétés' tab selected. On the left, a tree view shows the 'Services' folder expanded, with 'SCT' selected. The main area contains the following configuration:

- Edition**
 - Projet : SCT
 - Libellé : Format SCT SEPA
 - Visualisation : SCT_VISU_DET
 - Libellé : Edition detaille du SCT SEPA
- Conservation des données**
 - Nombre de jours pour les fichiers reçus : 10 jours
 - Nombre de jours pour les fichiers émis : 10 jours
 - Archivage sur : 120 jours
- Sécurité**
 - ☒ Chiffrement des fichiers
 - ☒ Chiffrement des archives

Vous pouvez rétablir le chiffrement *Legacy* en modifiant la méthode de chiffrement.

La modification ne s'appliquera qu'aux fichiers à venir.

L'utilitaire *sigcrypt* utilisé pour déchiffrer les fichiers a été modifié pour prendre en compte cette nouvelle fonctionnalité.

Divers

Pour l'application **Sage XRT Treasury – Communication** la gestion des droits a été améliorée :

- Droits **Session/Create** appliqués aux connexions
- Droits **Fonction COM** appliqués aux paramètres d'Identification EBICS (gestion des droits du contrats gérés dans l'application **Sage XRT Common Services**)
- Pour toutes les interfaces (**Trésorerie, Rapprochement, Rapprochement LCR, flux5, sepamail**), ajout du droit **Delete** (géré dans l'application **Sage XRT Common Services**)

Sage XRT Treasury - Signature	<input checked="" type="checkbox"/> Services
	<input checked="" type="checkbox"/> Clients
	<input checked="" type="checkbox"/> Dispositifs
	<input checked="" type="checkbox"/> Actions
	<input checked="" type="checkbox"/> Messages
	<input checked="" type="checkbox"/> Sessions
	<input checked="" type="checkbox"/> Interface trésorerie
	<input checked="" type="checkbox"/> Interface rappro
	<input checked="" type="checkbox"/> Interface rappro LCR
	<input checked="" type="checkbox"/> Historique des transferts
	<input checked="" type="checkbox"/> Log
	<input checked="" type="checkbox"/> Porteurs
	<input checked="" type="checkbox"/> Boîte de réception
	<input checked="" type="checkbox"/> Gestionnaire des traitements
	<input checked="" type="checkbox"/> SepaMail Interface
	<input checked="" type="checkbox"/> Generate
	<input checked="" type="checkbox"/> Report
	<input checked="" type="checkbox"/> Delete
	<input checked="" type="checkbox"/> Flux5 Interface
	<input checked="" type="checkbox"/> Generate
	<input checked="" type="checkbox"/> Report
	<input checked="" type="checkbox"/> Delete
Sage XRT Treasury - Communication	
Sage XRT Functional Service	