



Sage XRT Communication & Signature

Versión 4.2

Lista de novedades



Índice



Presentación	3
Gestión de la autenticación	4
API de explotación	6
Compatibilidad del sobre personalizado.....	10
Gestión de los protocolos criptográficos.....	11
Varios	13

Presentación

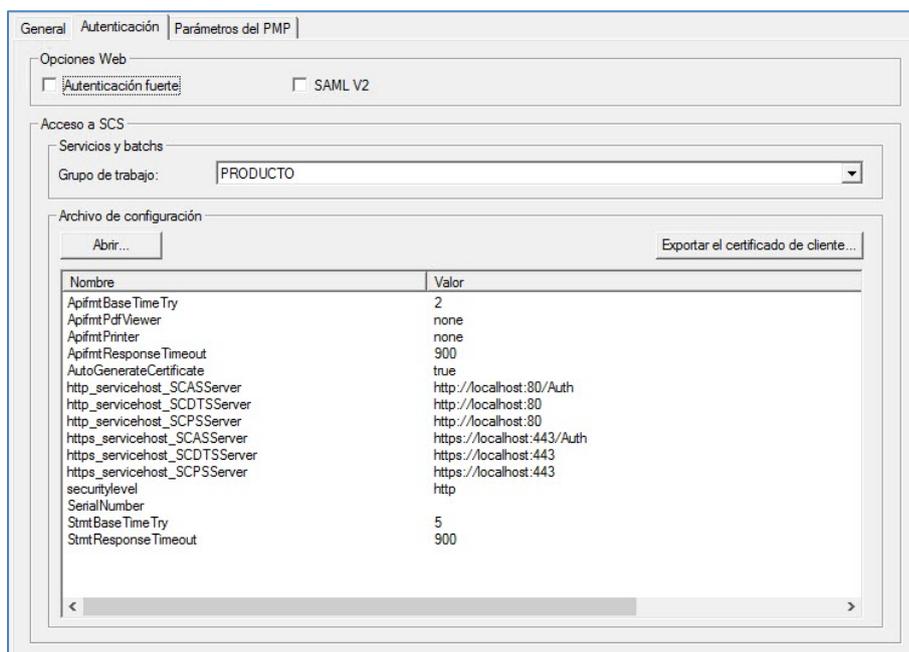
En este documento se describen las nuevas funcionalidades disponibles en la versión 4.2 de **Sage XRT Communication & Signature**.

El objetivo de esta versión es facilitar el intercambio de archivos entre las aplicaciones **Sage XRT Advanced** y **Sage XRT Communication & Signature**.

Importante: Esta versión no es compatible con la versión 4.1, ni las anteriores, de **Sage XRT Treasury**.

Gestión de la autenticación

Parámetros>Configuración>pestaña Autenticación



La pestaña **Autenticación** reúne:

- Las opciones de visualización de la página de conexión web (**Autenticación fuerte** o **SAML V2**).
- La información del archivo de configuración *wrapper*.

Sage.Fcs.Client se utiliza para consumir, de forma transparente, un conjunto de API **REST** alojado por los servicios de autenticación (**SCASServer**), de administración (**SCPSServer**) y de funcionalidades (**SCDTSServer**) de **Sage XRT Communication & Signature**.

La versión 4.2 de **Sage XRT Communication & Signature** integra esta biblioteca y llama algunos métodos.

El servidor de **Sage XRT Communication & Signature** se localiza mediante los parámetros del archivo de configuración *Sage.Fcs.Client.dll.config*.

Los parámetros que aparecen indicados son predeterminados. Desde esta interfaz, el usuario puede modificarlos según la configuración realizada.

Gestión de los protocolos criptográficos

Nombre	Valor	Comentario
ApiFmtBaseTimeTry	2	Temporización para el módulo de gestión de formatos (BFL)
ApifmtPdfViewer	None	Herramienta de visualización predeterminada de los archivos PDF
ApifmtPrinter	None	Impresora predeterminada
ApifmtResponseTimeout	900	Tiempo máximo de respuesta del módulo de gestión de formatos
AutoGenerateCertificate	True	Certificado autogenerado para garantizar la seguridad de los intercambios
http_servicehost_SCASServer	http://localhost:80/Auth	Ubicación del servicio de autenticación en HTTP
http_servicehost_SCPSSServer	http://localhost:80	Ubicación del servicio de administración en HTTP
http_servicehost_SCDTSServer	http://localhost:80	Ubicación del servicio de funcionalidades en HTTP
https_servicehost_SCASServer	https://localhost:443/Auth	Ubicación del servicio de autenticación en HTTPS
https_servicehost_SCPSSServer	https://localhost:443	Ubicación del servicio de administración en HTTPS
https_servicehost_SCDTSServer	https://localhost:443	Ubicación del servicio de funcionalidades en HTTPS
Securitylevel	HTTP	Secure channel HTTP o HTTPS
SerialNumber		Número de serie del certificado si no se utiliza el certificado autogenerado
StmtBaseTimeTry	5	No utilizado
StmtResponseTimeout	900	No utilizado

API de explotación

El servicio **XRT ComSign Rest Api** se utiliza para intercambiar datos con la aplicación **Sage XRT Communication & Signature** mediante la API **REST**.

Las API **REST** de producción simple que están disponibles en esta versión se utilizan para realizar el seguimiento de los flujos bancarios en emisión (adición de un archivo en el puesto de firma, envío de un archivo, seguimiento del estado de los archivos).

El servicio **XRT ComSign Rest Api** se instala junto con la aplicación **Sage XRT Communication** y debe iniciarse con una cuenta de servicio.

La documentación de las API **REST** figura en [http\(s\)://Hostname:8888/comsign/swagger](http(s)://Hostname:8888/comsign/swagger), siempre que se hay activado en el archivo de configuración. Puede consultar el detalle de las API que están disponibles para esta versión.

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)

Algunos datos necesarios para el funcionamiento del servicio se recuperan automáticamente al realizar la instalación.

A veces, es necesario definir algunos parámetros (modificación del DSN, de la dirección de la máquina, etc.) para la arquitectura deseada.

En la siguiente tabla se describe el archivo de configuración *Sage.Eb.ComSign.Api.exe.config*.

Gestión de los protocolos criptográficos

<appSettings>	Comentarios
<add key="UseSecureChannel" value="false" />	HTTPS o HTTPS (por defecto HTTP = false)
<add key="SecureChannelCertificateName" value="" />	Si no se indica, por defecto será True
<add key="DefaultAuthScheme" value="Ntlm" />	<p>Método de autenticación:</p> <ul style="list-style-type: none"> ▪ Por defecto, SageXRT (basada en el servicio SCAS) ▪ Negotiate (<i>Ntlm y/o Kerberos</i>) ▪ IntegratedWindowsAuthentication ▪ Basic ▪ Anonymous ▪ OAuth (Versión <i>OAuth2</i>) ▪ SAML (Versión <i>SAMLV2</i>) ▪ JWT (<i>JSON Web Token</i>) ▪ NTLM
<add key="Address" value="" />	Nombre del servidor, por defecto el nombre de la máquina.
<add key="AdditionnalPath" value="comsign" />	Ruta de acceso a la API REST, por defecto comsign
<add key="Port" value="8888" />	Puerto de acceso de la API REST, por defecto 8888
Parámetros de la autenticación SCS	
<add key="SCAS" value="http://localhost " />	Si método de autenticación = SageXRT
<add key="SCPS" value="http:// localhost" />	Si método de autenticación = SageXRT

Gestión de los protocolos criptográficos

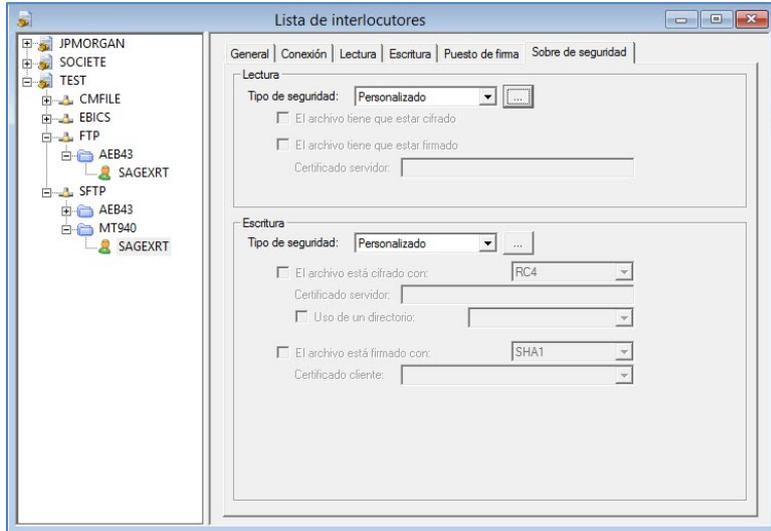
<appSettings>	Comentarios
Parámetros de la autenticación OAuth2 / Bearer	
<add key="OAuthDecryption" value="Auto" />	Clave de descifrado autogenerada
<add key="OAuthValidationAlgorithm" value="HMACSHA256" />	Algoritmo de validación autogenerada
<add key="OAuthValidationKey" value="AutoGenerate,IsolateApps" />	Clave de validación autogenerada
<add key="OAuthDecryptionKey" value="AutoGenerate,IsolateApps" />	Clave de descifrado autogenerada
<add key="OAuthAccessTokenExpire" value="30" />	Valor en minutos de la duración del <i>token</i> de acceso
<add key="OAuthModeSupport" value="TokenEndpointServer" />	Si se indica el valor TokenEndPoint , el SRA pasa a ser servidor de identidad y de <i>tokens</i> de acceso. Para recuperar un <i>token</i> OAuth2 válido, hay que llamar a la dirección del SRA + <i>/token</i> . Si dicho valor no se indica, el SRA se limita a ser un servidor de recursos.
Parámetros de la autenticación JWT / Bearer	
<add key="JWTRealm" value="" />	Dominio del JWT
<add key="JWTIssuer" value="" />	Valor del emisor
<add key="JWTAudience" value="" />	Valor de la audiencia (destinatarios)
<add key="JWTSecret" value="" />	Valor del secreto
<add key="JWTCertificateFindValue" value="" />	Nombre del certificado
<add key="JWTCertificateFindType" value="FindBySubjectDistinguishedName" />	Modo de búsqueda del certificado, por defecto el DN del nombre del objeto del certificado

Gestión de los protocolos criptográficos

<appSettings>	Comentarios
Parámetros de la autenticación SAMLV2 / Bearer	
<add key="SAMLAudience" value="" />	Valor de la audiencia (destinatarios)
<add key="SAMLIssuerThumbPrint" value="" />	Valor de la huella digital del emisor
<add key="SAMLIssuerName" value="" />	Valor del nombre del emisor
Log activation parameter	
<add key="LogFile" value="" />	Ruta y nombre del log de la aplicación. Por defecto no está activado
Grupo de trabajo (Workgroup)	
<add key="eBankingUrl" value="" />	No utilizado
<add key="UmapiWorkGroup" value="WORKGROUP" />	Nombre del <i>Workgroup</i> <i>UMAPI</i> . Por defecto Workgroup

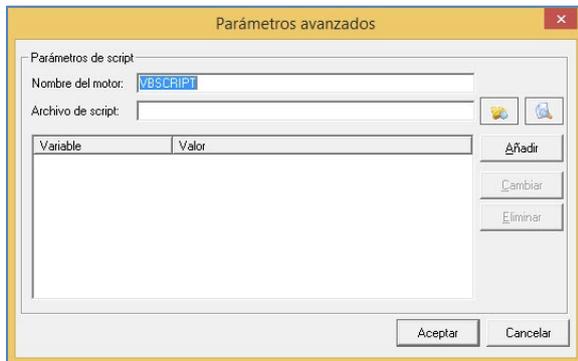
Compatibilidad del sobre personalizado

En la pestaña **Sobre de seguridad** de los contratos bancarios, se ha añadido el tipo de seguridad **Personalizado**.



Haga clic en el botón  para acceder a los parámetros avanzados.

Puede seleccionar o crear un archivo SCRIPT.



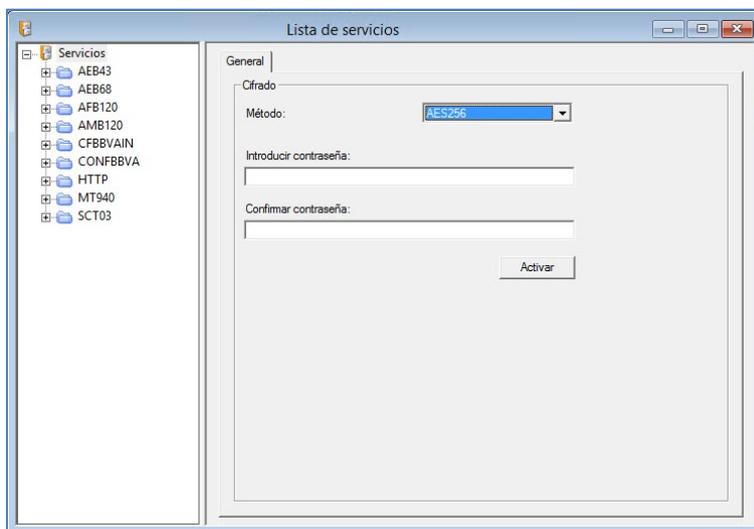
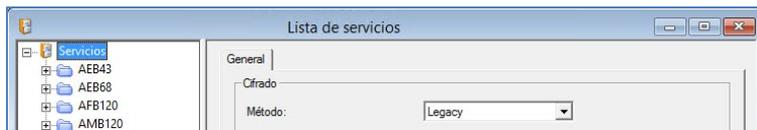
Si crea un archivo con el botón , habrá disponible un modelo (*template*) con la función **descodificación** o **codificación**. Desde el directorio `\\Wkspace\Templates\` se accede al archivo *template envelope.vbs*.

Gestión de los protocolos criptográficos

En el *WORKSPACE*, ahora los archivos pueden cifrarse según la norma **AES256**.

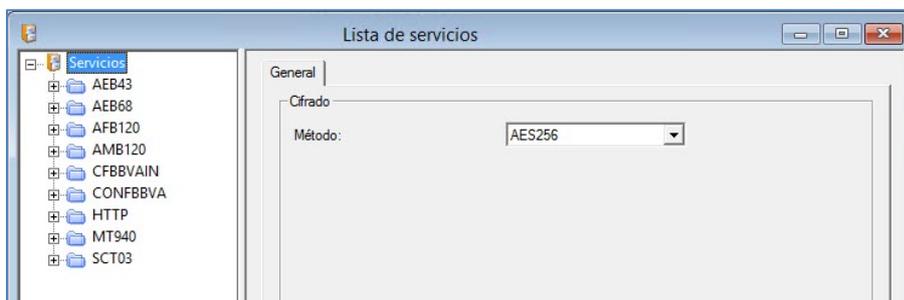
La función **SHA2-256** se utiliza para calcular los sellos y comprobar si hay duplicados.

Para configurar el cifrado **AES256**, hay que haber seleccionado el método **AES256** en la configuración de los servicios.



Debe definir una contraseña (*passphrase*), y hacer clic en **Activar**.

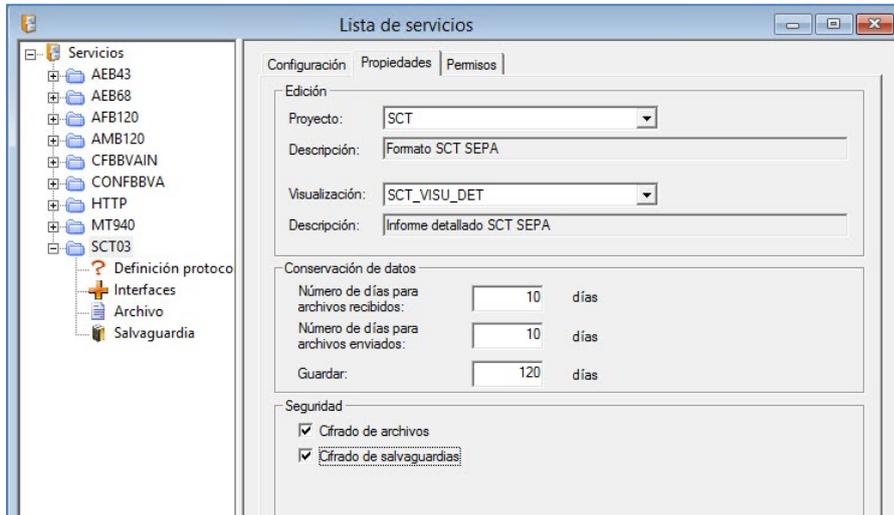
Importante: Hay que garantizar la seguridad de dicha contraseña.



Al realizar la activación, todos los archivos se cifran en **AES256**.

Gestión de los protocolos criptográficos

Nota: Para activar el cifrado en cada servicio correspondiente, seleccione las opciones de seguridad **Cifrado de archivos** y **Cifrado de salvaguardias** en la pestaña **Propiedades** de la configuración.



Puede restablecer el cifrado *Legacy* modificando el método de cifrado.

La modificación solo se aplicará a los próximos archivos.

La utilidad *sigcrypt* utilizada para descifrar los archivos se ha modificado para tener en cuenta esta nueva funcionalidad.

Varios

Se ha mejorado la gestión de los permisos para la aplicación **Sage XRT Treasury Communication**:

- Permisos **Sesiones/Crear** aplicados a las conexiones.
- Permisos **Función COM** aplicados a los parámetros de identificación EBICS (gestión de los permisos de los contratos gestionados en la aplicación **Sage XRT Common Services**).
- Para todas las interfaces (**Tesorería, Conciliación, Conciliación de efectos, Flux5, SepaMail**), se ha añadido el permiso **Eliminar** (gestionado en la aplicación **Sage XRT Common Services**).

Modificación de los derechos de acceso a las funciones del perfil "ADMIN"✕

Sage XRT Administration Service	<input type="checkbox"/> Conexión inmediata
	<input type="checkbox"/> Administrador de comunicaciones
	<input type="checkbox"/> Interlocutores
	<input type="checkbox"/> Servicios
Sage XRT Treasury - Signature	<input type="checkbox"/> Clientes
	<input type="checkbox"/> Dispositivos
	<input type="checkbox"/> Acciones
	<input type="checkbox"/> Mensajes
Sage XRT Treasury - Communication	<input type="checkbox"/> Sesiones
	<input type="checkbox"/> Interfaz Tesorería
	<input type="checkbox"/> Interfaz Conciliación
	<input type="checkbox"/> Interfaz Conciliación de efectos
	<input type="checkbox"/> Histórico de transferencias
Sage XRT Functional Service	<input type="checkbox"/> Log
	<input type="checkbox"/> Portadores
	<input type="checkbox"/> Bandeja de entrada
	<input type="checkbox"/> Administrador de tratamientos
	<input type="checkbox"/> Interfaz SepaMail
	<input type="checkbox"/> Generar
	<input type="checkbox"/> Comunicar
	<input type="checkbox"/> Eliminar
	<input type="checkbox"/> Interfaz Flux5
	<input type="checkbox"/> Generar
	<input type="checkbox"/> Comunicar
	<input type="checkbox"/> Eliminar