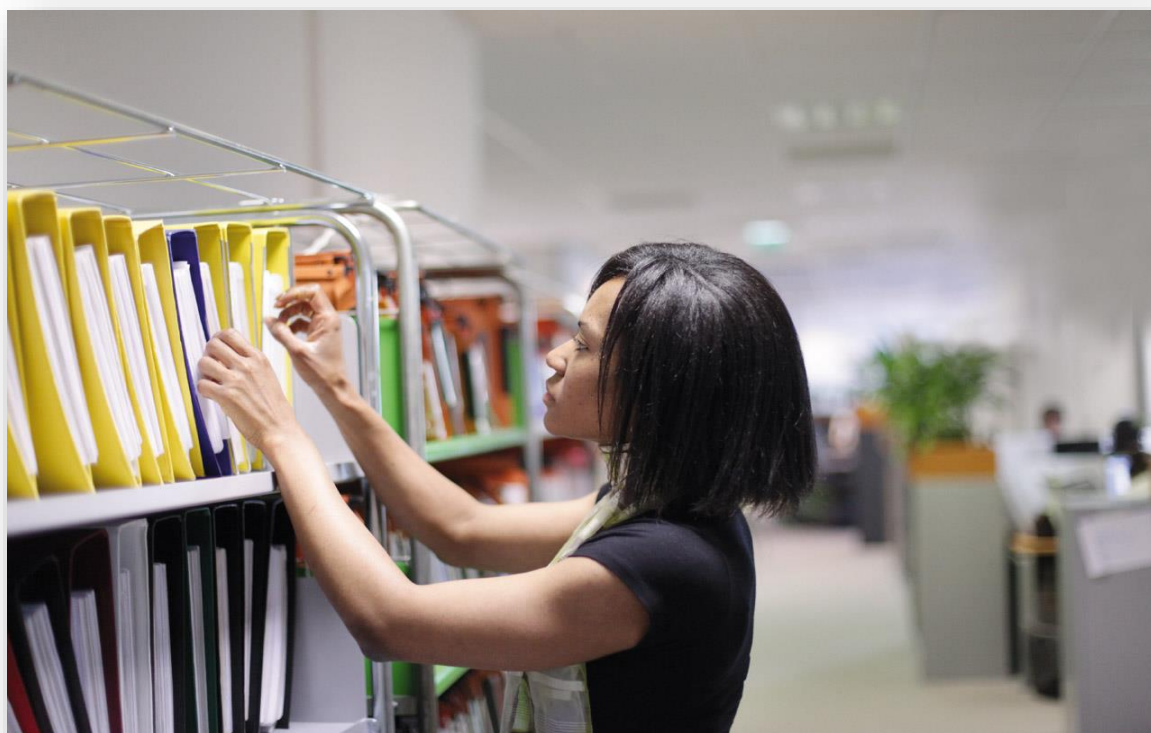


SBE

Version 11.40.500

Contrôle OCSP



Sommaire

DESCRIPTION	3
OCSP CONTROLE DES CERTIFICATS DE SIGNATURE DU TRANSPORT.....	4
Service de transfert de fichier	4
Paramétrage du dispositif de protocole EBICS	4
Paramétrage pour le service transferts de fichier	6
Paramétrage pour EBICS.....	7
Contrat demandeur	13
Validation effectuée pour un transfert demandeur EBICS	14
Validation effectuée pour un transfert serveur en EBICS.....	14
OCSP CONTROLE DES CERTIFICATS DE SIGNATURE DES SIGNATAIRES.....	15
Service de transaction	15
Clés de sécurité\ X509 (CryptoApi).....	15

Description

L'OCSP (Online Certificate Status Protocol) est un protocole qui permet de vérifier le statut d'un certificat X509, à savoir s'il est valide ou révoqué et la raison pour laquelle il a été révoqué.

Ce protocole est déjà utilisé pour vérifier le statut des certificats lors des connexions SSL et lors de la sécurisation des fichiers par enveloppe (PKCS, SMIME, ...) suivant les protocoles (FTP, http, ...), le paramétrage étant effectué au niveau du service Transfert de Fichiers, Clés de Sécurité X509.

Ce protocole est désormais disponible pour la validation des certificats de signataires utilisés sur le protocole EBICS et pour les certificats de signature de transport s'ils sont issus d'une AC.

Pour la validation des certificats utilisés par le Service de Transfert de fichiers avec le protocole EBICS, le paramétrage se fera au niveau des clés de sécurité EBICS.

Pour la validation des certificats utilisés par les signataires (via le WEB et le poste de signature) le paramétrage se fera au niveau du service de Transaction, clés de sécurité X509.

OCSP Contrôle des certificats de signature du transport

Service de transfert de fichier

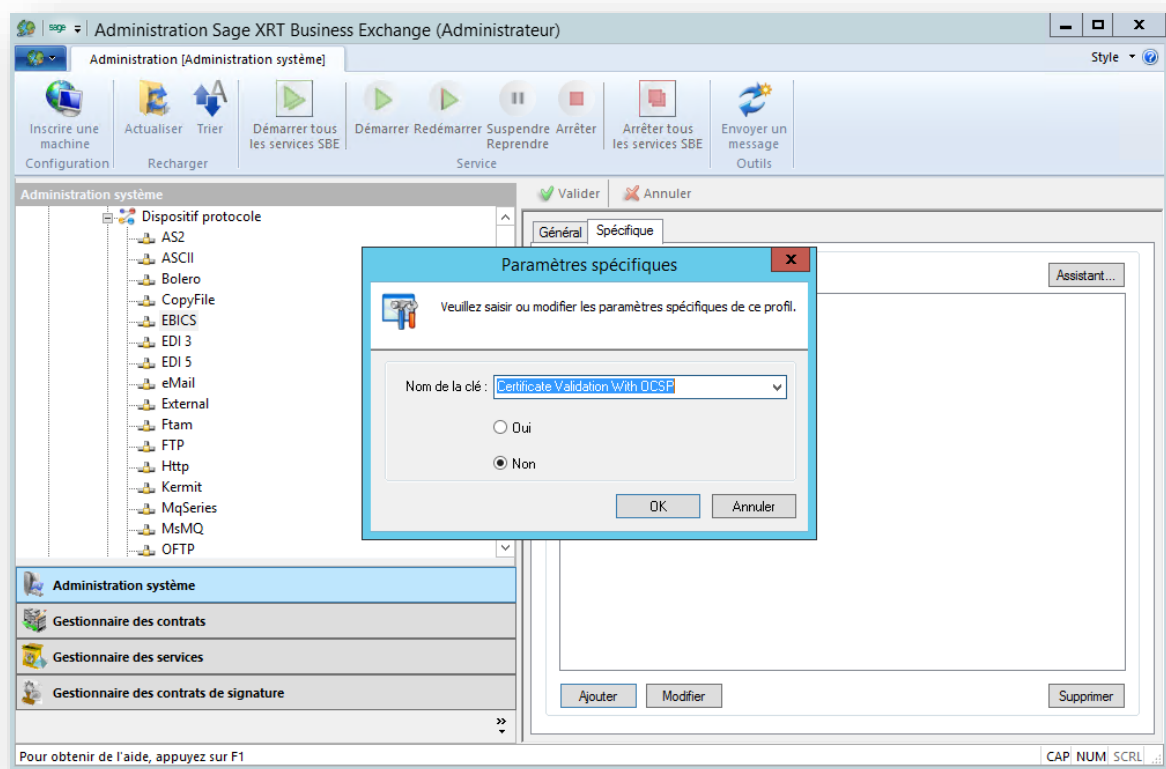
Pour la configuration du transport, le contrôle via OCSP est utilisé pour contrôler les certificats de signature et d'authentification du Partner.

Un premier niveau de paramétrage s'effectuant sur le dispositif protocolaire EBICS permet de valider ou dévaliser l'utilisation d'OCSP pour tous les partenaires utilisant ce dispositif.



Si OCSP n'est pas configuré le statut du certificat sera tout de même vérifié en recherchant celui-ci dans la liste de révocation (CRL) si elle est disponible.


Paramétrage du dispositif de protocole EBICS



Sur l'onglet spécifique, ajouter la clé **Certificat Validation With OCSP** à YES.

Ou via l'assistant, cocher **Validation des certificats via OCSP**

Assistant du paramétrage du dispositif protocole EBICS ✕

 Cet assistant vous permet facilement de saisir ou modifier les paramètres spécifiques de ce profil.

Général | Rapports | Timers | Réconciliation

Url :

Nom :

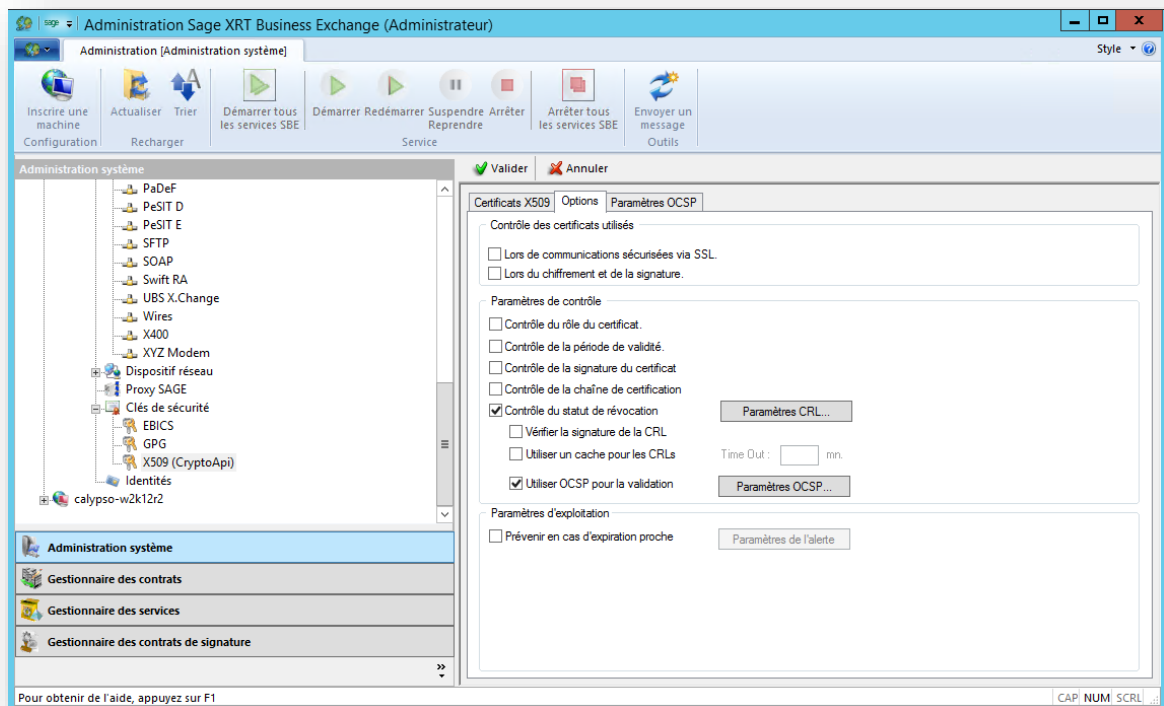
☒ Emission des clés au format X509
☒ Validation des certificats
 ☒ Validation des certificats via OCSP
☐ Validation des requêtes XML
☒ Auto activation des utilisateurs



La validation des certificats via OCSP n'est possible que si la Validation des certificats a été activé.

Paramétrage pour le service transferts de fichier

Ce paramétrage permet de vérifier le statut des certificats lors des connexions SSL et lors de la sécurisation des fichiers par enveloppe (PKCS7, SMIME, ...) suivant les protocoles (FTP, http, ...).



Onglet Options

Contrôle du statut de révocation est coché.

Utiliser OCSP pour la validation est coché.

Paramétrage pour EBICS

Un nouvel onglet Paramètre OCSP est disponible.

Il permet de définir les autorités pour lesquelles les certificats issus de cette autorité, seront validés via OCSP plutôt que CRL.

En ajoutant une autorité racine, ou une autorité intermédiaire, cela signifie que tous les certificats **directement** issus de ces autorités seront testés via OCSP.

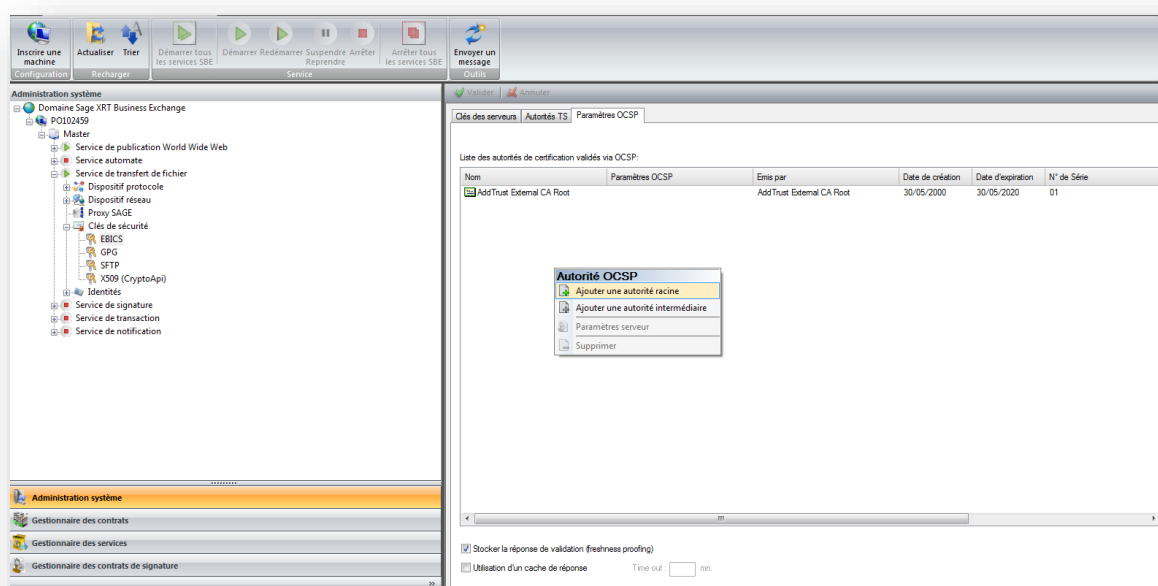
Cet onglet permet de définir ou sur définir les paramètres OCSP à utiliser lors de la validation, en principe le certificat contient l'information minimal permettant de vérifier son état.

Il contient le point de distribution de la CRL et/ou l'adresse du Responder OCSP qui fournira l'état du certificat.

Dans le cas où ces informations seraient incorrectes et ou incomplètes, vous avez la possibilité de redéfinir certaines de ces informations via le clic droit paramétrages serveur.

Le serveur OCSP pour les autorités valides.

Sur le protocole EBICS :



Clique droit sur la fenêtre pour ajouter une autorité racine ou une autorité intermédiaire. Tous les certificats directement issus de ces autorités feront l'objet d'une validation via OCSP.

Stocker la réponse de validation (freshness pooling) : Cette option vous permettra de conserver la réponse de la validation OCSP.



Les réponses sont stockées et visualisable depuis le moniteur. Preuves de validités des certificats.

Traces Historique des transferts demandeurs EBICS : sur un transfert, sur l'onglet Info de sécurité \ Preuves de validité des certificats.

Dans le moniteur, détail d'un transfert

Information

Détail du transfert

Général Description Info. protocolaires Info. de sécurité Info. de signature

Protocole : TLS1.2

Authentification : NO

Certificat server : MOMO

Certificat client :

Algorithme de signature : SHA-384

Taille des clés : 0 bits

Algorithme de chiffrement : AES 256

Taille des clés : 256 bits

Algorithme d'échange de clés : ECDH Ephemeral

Taille des clés : 256 bits

Preuve : [Extraire la preuve...](#)

Preuves de validité de certificats :

Id	Certificat	Signataire
13444	OCSP-Ebics-Sig	momo-pc

Domaine Sage XRT Business Exchange Information Action

Accès à la liste des réponses OCSP archivés depuis le moniteur

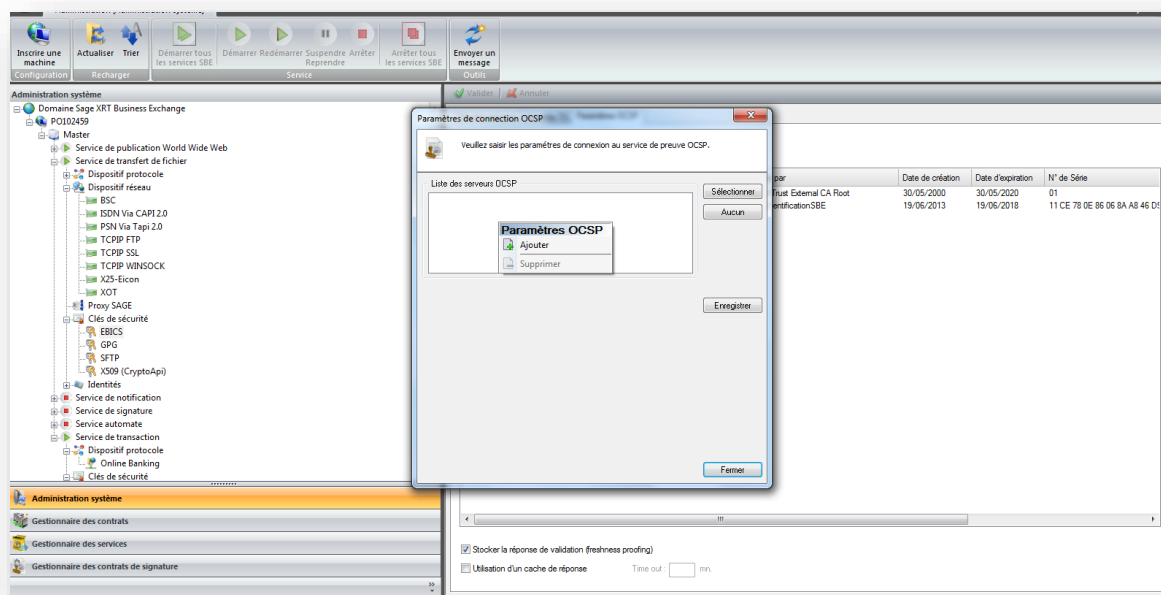
Utilisation d'un cache de réponse : Définir le délai de timeout de la réponse (en minute)

La première réponse sera stockée le temps indiqué afin de ne pas effectuer une nouvelle demande dans ce délai. Dans le cas où la réponse est encore valide **nextUpdate**.

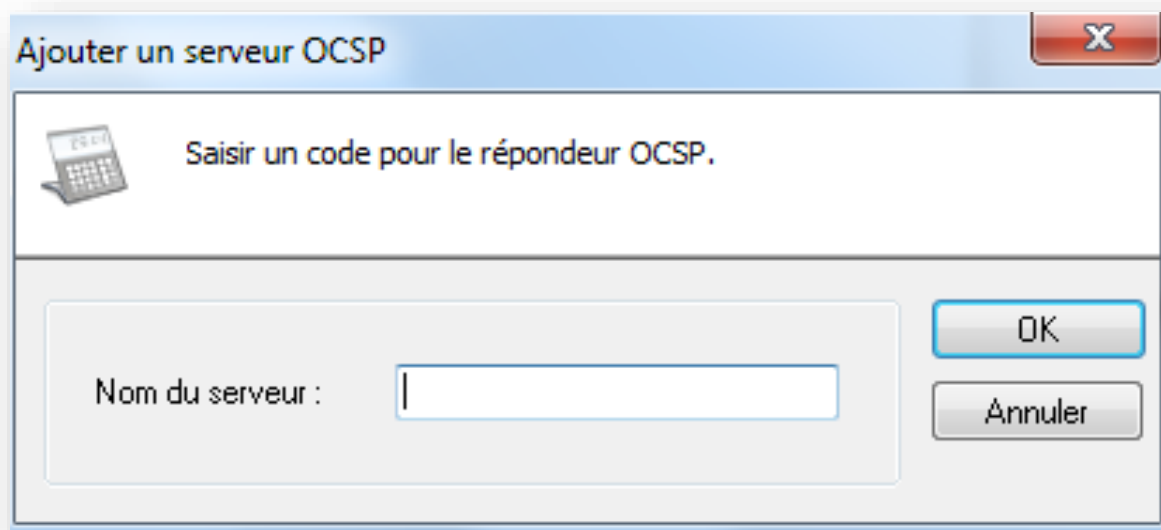
Lorsque vous avez ajouté les autorités concernées par le contrôle OCSP, et si vous devez modifier ou personnaliser les paramètres d'accès au Responder OCSP, cliquez droit sur une ou plusieurs autorités, sélectionnez **Paramètres serveur**.

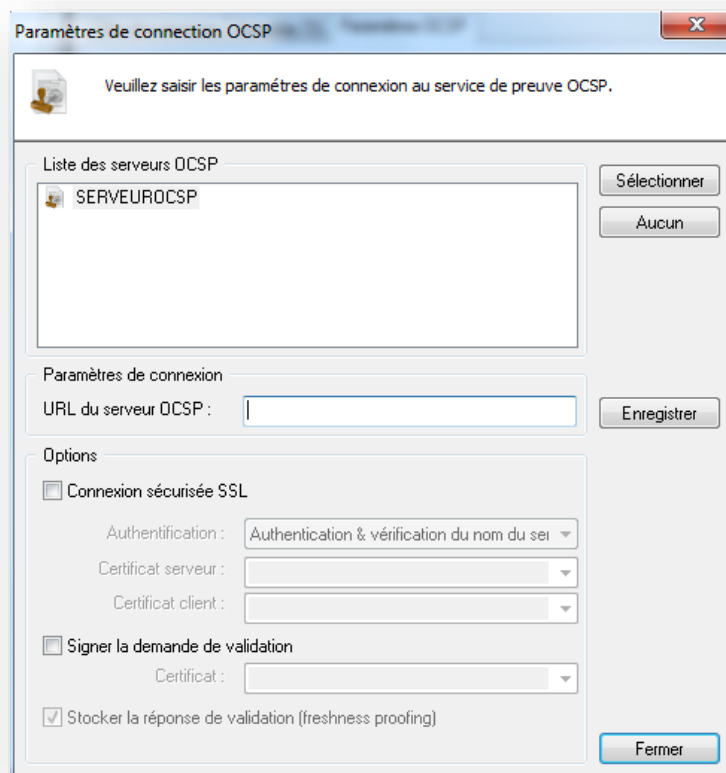


Clique droit, ajouter pour créer une configuration personnalisée du serveur OCSP, ce paramétrage est unique et peut être utilisé sur les autres services.



Ajouter le Nom du serveur OCSP (Code d'identification)





URL du serveur OCSP : Indiquer l'adresse url pour contacter le serveur OCSP, si vous ne voulez pas utiliser celle contenue dans le certificat.

Connexion sécurisée SSL : Indiquer les paramètres de connexion SSL (TLS1.2) au serveur OCSP et le type d'authentification à faire :

Authentification :

Authentification et vérification du serveur : La configuration du certificat serveur est nécessaire. Il indique que le certificat paramétré correspond à celui utilisé et que le common name correspond au nom du serveur.

Authentification simple : Il n'y a pas de contrôle du nom du serveur.

Le certificat client sera utilisé pour s'authentifier lors de la connexion SSL si nécessaire

Signer la demande de validation : Dans le cas où le reponder OCSP demande une signature de la requête, indiquer le certificat à utiliser pour signer la demande de validation OCSP

Cliquer sur **Sélectionner** pour affecter la configuration OCSP à l'autorité. Ces paramètres seront utilisés lors de la validation des certificats issu de cette autorité.

Contrat demandeur

Vous devez paramétrer le contrat demandeur de la façon suivante.

Ajouter la politique de sécurité : **X509 EBICS OCSP**



Utiliser une liaison avec un dispositif protocolaire EBICS pour lequel OCSP a été activé.

Validier Annuler

Général Connexion Ecriture Lecture Poste de signature

Informations

Libellé : Propriétés avancées :

Politique de sécurité

X509 Ebics OCSP

Période de validité

Date début : 12/30/2016 Date fin : 12/30/2026

Statut

☐ Service en opposition

Liaison

HOLDISF ▶

Validation effectuée pour un transfert demandeur EBICS

Le certificat de signature sera vérifié avant le transfert :

[X.509 EBICS VERIFY CERTIFICATE TO USE]

Certificate =OCSP-Ebics-Sig2

PKI Used =X509 OCSP

[X.509 CHECK KEY LEN]

Key Length =2048

[X.509 CHECK KEY USAGE]

INFO =Cert Non-Repudiation Key usage found

Certificate Issuer =MoMoAc Intermediate CA

[CHECK REVOCATION WITH OCSP]

CHECK ISSUER WITH OCSP=YES

[X.509 VERIFY ALL CERT In CHAIN BY OCSP]

[PROOF SAVING]

INFO=FRESHNESS PROOF SAVED

Proof Id =13448

Validate OCSP Result =CERTIFICATE VALID

Validation effectuée pour un transfert serveur en EBICS

Le certificat d'authentification et de signature reçus, seront vérifiés lors de l'initialisation du transfert.

[VERIFY EBICS AUTHENTICATE SIGNATURE]

[CHECK CERTIFICATE TS]

Common Name =OCSP-Ebics-Aut

Time Validity =OK

Certificate Issuer =MoMoAc Intermediate CA

[OCSP CERTIFICATE VALIDATION]

[PROOF SAVING]

INFO=FRESHNESS PROOF SAVED

Proof Id =13449

Validate OCSP Result =CERTIFICATE VALID

[CHECK CERTIFICATE TS]

Common Name =OCSP-Ebics-Sig2

Time Validity =OK

Certificate Issuer =MoMoAc Intermediate CA

[OCSP CERTIFICATE VALIDATION]

Proof Id (from cache) =13448

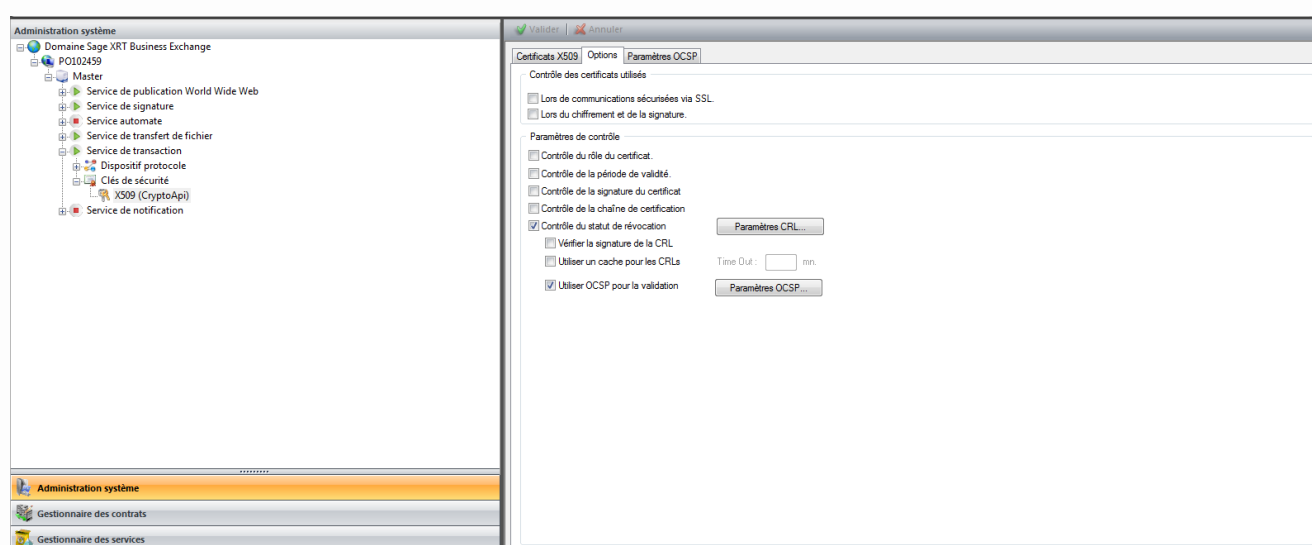
OCSP Contrôle des certificats de signature des signataires

Pour le poste de signature, le contrôle OCSP est réalisé lors de la signature d'un fichier.

Le certificat sera vérifié via OCSP lors de la signature.

Service de transaction

Clés de sécurité\ X509 (CryptoApi)



Onglet Options

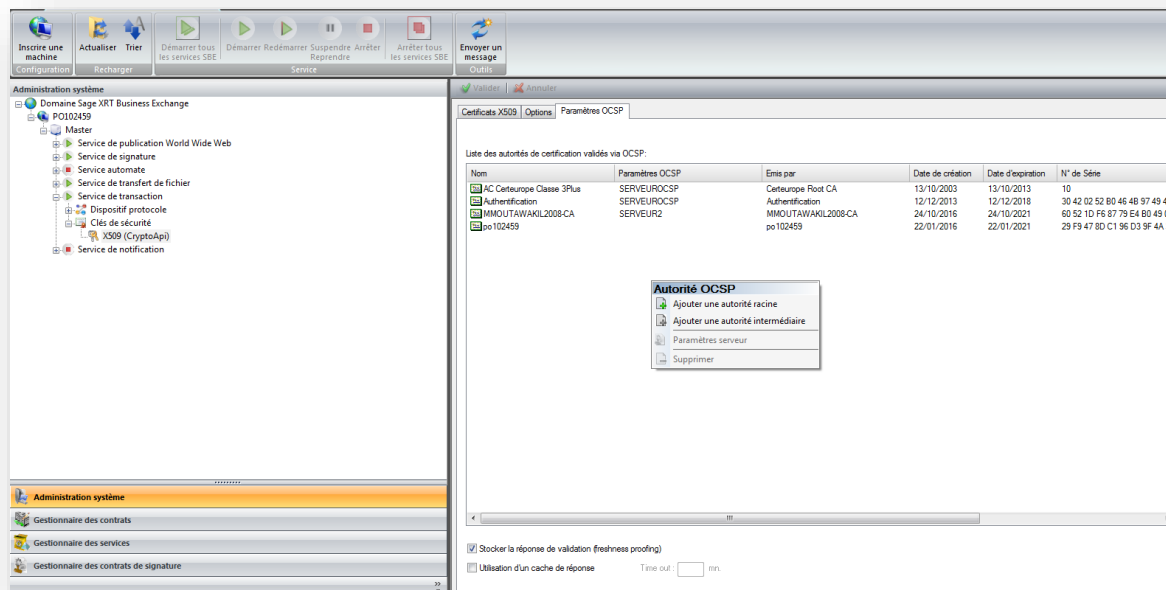
Contrôle du statut de révocation est coché.

Utiliser OCSP pour la validation est coché.

Un nouvel onglet Paramètre OCSP est disponible. Il permet pour le poste de signature de définir le serveur OCSP pour les autorités valides.



Les serveurs OCSP paramétrés sur le service de transfert de fichier sont automatiquement proposés.



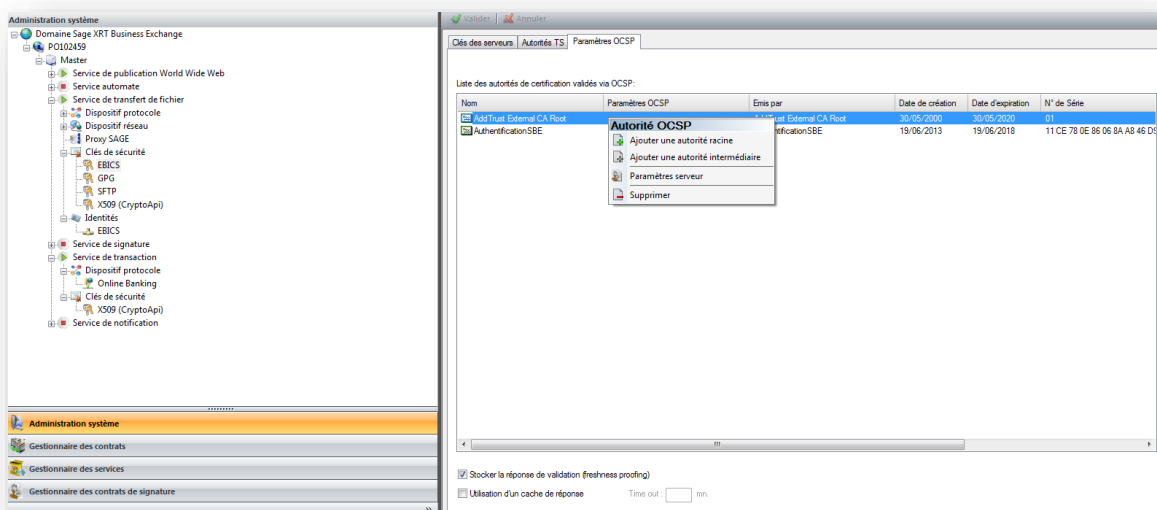
Clique droit sur la fenêtre pour ajouter une autorité racine ou une autorité intermédiaire valide qui fera l'objet de vérification.

Stocker la réponse de validation (freshness pooling) : Cette option vous permettra de conserver la réponse de la validation OCSP.

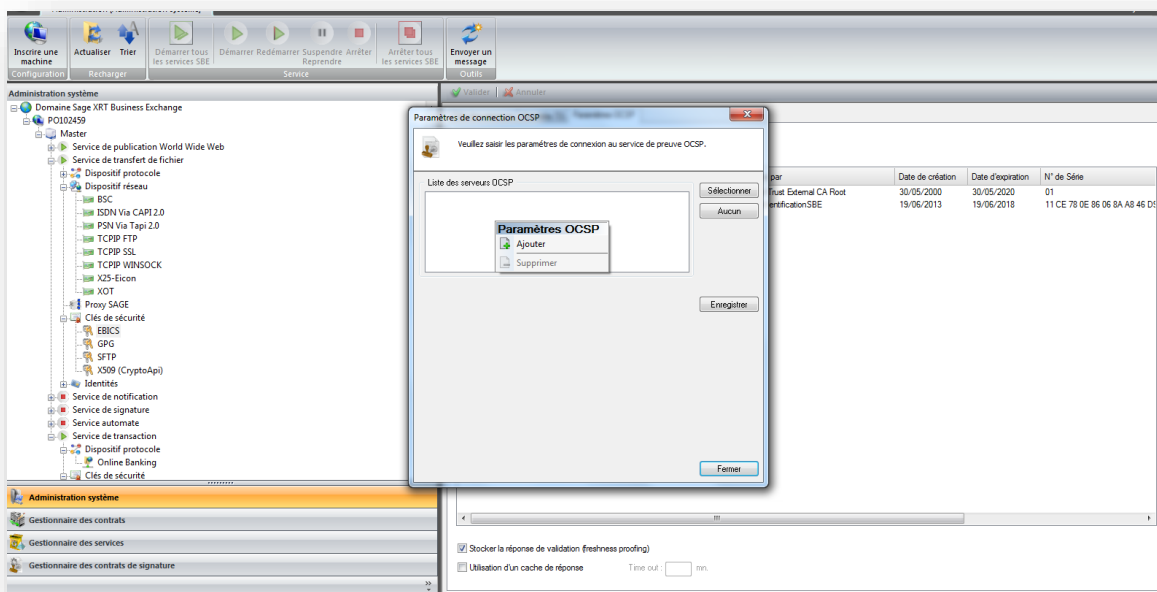


Les réponses sont stockées dans le moniteur.

Sur chaque autorités valides, il est possible de définir des paramètres OCSP différents des paramètres par défaut en se positionnant sur l'autorité, et en cliquant sur Propriétés Avancées.



Clique droit, ajouté pour renseigner les paramètres du serveur OSCP



Ajouter le Nom du serveur OCSP

Ajouter un serveur OCSP

Saisir un code pour le répondeur OCSP.

Nom du serveur :

OK

Annuler



URL du serveur OCSP : Indiquer l'adresse url pour contacter le serveur OCSP, si vous ne voulez pas utiliser celle contenue dans le certificat.

Connexion sécurisée SSL : Indiquer les paramètres de connexion SSL (TLS1.2) au serveur OCSP et le type d'authentification à faire :

Authentification :

Authentification et vérification du serveur : La configuration du certificat serveur est nécessaire. Il indique que le certificat paramétré correspond à celui utilisé et que le common name correspond au nom du serveur.

Authentification simple : Il n'y a pas de contrôle du nom du serveur.

Le certificat client sera utilisé pour s'authentifier lors de la connexion SSL si nécessaire

Signer la demande de validation : Dans le cas où le repondre OCSP demande une signature de la requête, indiquer le certificat à utiliser pour signer la demande de validation OCSP

Cliquer sur **Sélectionner** pour affecter la configuration OCSP à l'autorité. Ces paramètres seront utilisés lors de la validation des certificats issu de cette autorité.