



Sage XRT Business Exchange

Version 12.1.0

Données Personnelles



Sommaire

Objectif du document.....	4
Principales exigences européennes	5
Sécurité des données.....	6
Sécurité d'accès à la base de données	6
Affectation des permissions	6
Choix du niveau d'authentification	6
Définition d'une politique de sécurité via Sage XRT Common Services.....	7
Gestion des profils, rôles et utilisateurs.....	7
Fonctionnalités d'audit sur la gestion des identités et des accès	8
Reporting de sécurité	9
Conformité avec la loi Sarbanes Oxley	9
Données personnelles et traitements associés	12
Liste des données personnelles	12
Gestion des utilisateurs.....	14
Options de sécurité par entité	14
Paramétrage	14
Reporting	15

Signataires	15
Finalité des traitements.....	15
Gestion : création-modification-suppression.....	15
Reporting sur la base.....	16
Tiers : Clients-Fournisseurs-Salariés.....	16
Finalité des traitements.....	18
Gestion des tiers.....	21
Gestion des amendements.....	22
Export sur la base	23
Contacts des Agences Bancaires	23
Finalité des traitements.....	23
Gestion	23
Reporting sur la base.....	24
Droit de rectification et d'effacement des données - Durée de conservation des données personnelles	24
Mesures de sécurité complémentaires.....	25
Mesures générales	25
Utilisation de https	25
Mots de passe solides	25
Sécurisation des serveurs par droit d'accès	26
Protection des serveurs.....	26
Transparent Data Encryption TDE	27
Chiffrement des données en transit.....	27
Chiffrement des sauvegardes de la base de données.....	27
Sécurité du système de fichiers.....	27
Mesures applicatives.....	27
Signature de l'application et du site web	27
Autorisations	28
Protection contre les attaques	29
Périodicité d'accès au site web	30
Pour aller plus loin.....	30
Avertissement.....	31

Objectif du document

Le règlement général sur la protection des données (RGPD) est entré en application le 25 mai 2018 dans les 28 pays de l'Union Européenne.

Ce document est destiné à identifier les fonctionnalités existantes de **Sage XRT Business Exchange** qui peuvent faciliter la mise en conformité des entreprises avec ce règlement européen.

Principales exigences européennes

Principales Exigences sur la protection des données personnelles	Sage XRT Business Exchange
Garantir une sécurité appropriée	
Pour garantir la sécurité, l'entreprise devra déployer des mesures techniques et organisationnelles dans l'entreprise telles que : sécurisation des postes de travail, des serveurs, des espaces de stockage, ainsi que mettre en place des politiques ou clauses de confidentialité	
<p>Renforcement des mots de passe et de la protection de certaines données stockées ou échangées.</p> <p><u>cf. les fonctionnalités existantes en matière de sécurité</u></p>	✓
Gestion des droits de la personne (droit à la portabilité, droit à l'oubli / effacement, droit à l'opposition du traitement/consentement, droit à la rectification, etc.)	
Elle devra prévoir des fonctionnalités de rectification de données personnelles, d'import/export des données personnelles, et des fonctions de sélection des personnes concernées par les traitements.	
<p>Utilisation des fonctions de modification/suppression disponibles dans chaque Produit et accessibles selon les habilitations et les droits de l'utilisateur.</p> <p><u>cf. les fonctionnalités existantes sur les données personnelles</u></p>	✓
Contribution à la démonstration de la conformité	
L'entreprise devra référencer tous les documents qui démontrent les actions mises en place pour respecter ses obligations au regard de la réglementation européenne sur la protection des données personnelles– documents qu'elle pourra présenter en cas de contrôles tels que : les documents qui décrivent les mesures techniques et organisationnelles qu'elle a mises en place pour sécuriser l'exploitation des données personnelles, le registre de traitements.	
<p>Sage met à votre disposition une cartographie des données personnelles et des traitements associés pour Sage XRT Business Exchange.</p> <p><u>cf. la liste des données personnelles et des traitements associés</u></p>	✓

Sécurité des données

Sécurité d'accès à la base de données

Grâce à la console d'administration **Sage XRT Common Services**, vous définissez le mode de fonctionnement de la gestion des droits d'accès des utilisateurs aux applications **Sage XRT**.

Affectation des permissions

Les permissions peuvent être affectées selon deux modes distincts :

- Si vous souhaitez mettre en place une gestion simple des droits d'accès aux applications, qui ne fait intervenir qu'un seul administrateur de sécurité, sélectionnez **[Les droits d'accès sont accordés par un administrateur de sécurité]**.
- Si vous souhaitez mettre en place une gestion des droits d'accès aux applications dans laquelle toute opération effectuée par un administrateur de sécurité doit être validée par un deuxième administrateur de sécurité, sélectionnez **[Les droits d'accès sont accordés par un administrateur de sécurité de niveau 1 puis validés par un administrateur de sécurité de niveau 2]**.

Choix du niveau d'authentification

Rôles Sites

☐ ADMIN
☐ SIGNATAIRE

Authentification

☒ Authentification Windows
☐ Authentification LDAP
☐ Authentification standard
☐ Authentification Sage ID

Authentification de
☐ l'utilisateur via un Certificat X509
☐ Double authentification
☐ Mot de Passe par défaut

Mot de passe
Confirmation mot de passe

Type d'utilisateur

☐ Administrateur de sécurité de niveau 1
☒ Utilisateur standard

Informations diverses

Langue: Français

Description:

Email:

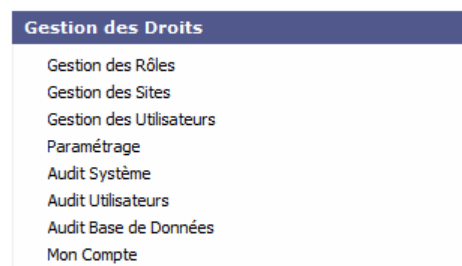
Période de Validité: 0 années (jusqu'à 4/17/2018)

Suivant le type d'authentification utilisé par l'administrateur de base de données (*DBA*) pour se connecter au serveur de bases de données, plusieurs options sont disponibles :

Sécurité des données

- **Utiliser la sécurité intégrée de Windows NT** : le *DBA* est authentifié grâce à son compte NT (ce niveau d'authentification est préconisé).
- **Utiliser un nom d'utilisateur et un mot de passe** : le *DBA* est authentifié grâce à un nom d'utilisateur et un mot de passe.
- **Authentification de l'utilisateur via un certificat X509** : pour le client web, l'authentification forte est un système d'authentification à deux phases.
 - Vérification du certificat sur l'**Active Directory** de l'entreprise
 - Challenge/Réponse entre le client et le composant d'authentification permettant de vérifier l'identité du client
- **Double authentification** : un deuxième facteur est utilisé pour l'authentification des utilisateurs pour générer un mot de passe à usage unique.
- **SageID**

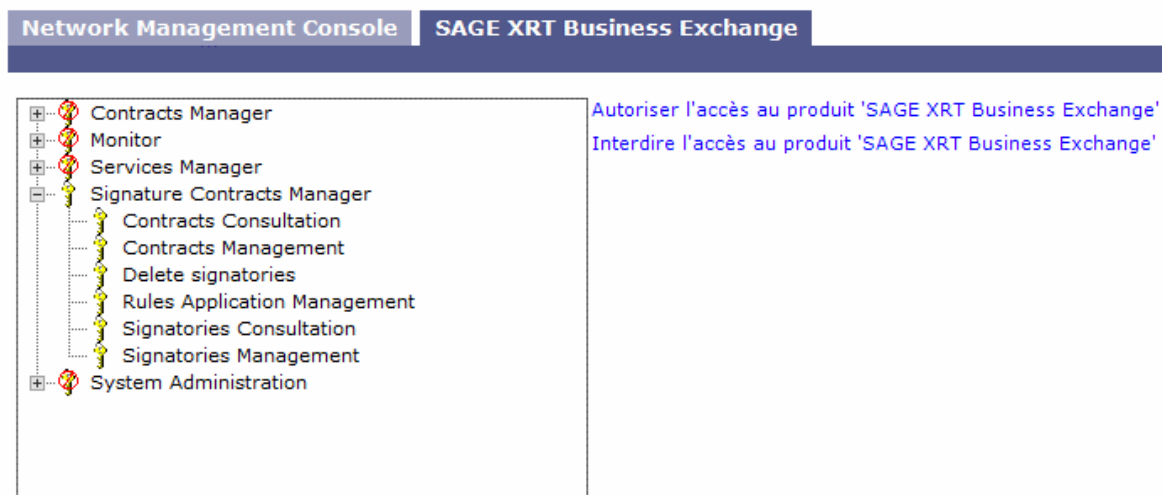
Définition d'une politique de sécurité via Sage XRT Common Services



Gestion des profils, rôles et utilisateurs

Les profils permettent de créer des rôles utilisateurs, administrateurs pour déterminer des autorisations d'accès aux applications.

Modifier les Droits du Rôle SIGNATAIRE



Fonctionnalités d'audit sur la gestion des identités et des accès

Outre les diverses fonctionnalités qu'elle propose, la gestion des identités et des accès doit apporter la preuve de son bon fonctionnement.

Ces preuves doivent être fournies sur demande à un auditeur, sous forme de trace écrite afin d'être archivées.

Les preuves fournies doivent porter sur les domaines fréquemment couverts par les audits :

- Activité des administrateurs
 - création d'un utilisateur
 - suppression d'un utilisateur
 - changement du mot de passe d'un utilisateur
 - changement dans la stratégie de gestion des mots de passe
 - changement de la configuration de l'accès à l'annuaire LDAP
 - accès accordé à une fonction ou à un produit
 - accès refusé à une fonction ou à un produit
- Activité des utilisateurs finaux
 - connexion d'un utilisateur (login)
 - déconnexion d'un utilisateur (logout)
 - messages spécifiques de l'application
- Tests de conformité avec la politique de sécurité
 - compte utilisateur verrouillé après N tentatives infructueuses de connexion

Le tableau **Audit Utilisateurs** décrit les actions effectuées par les utilisateurs.

Date	Heure	Catégorie	Statut	Produit	Composant	Utilisateur	Compte de l'util...	Machine	Description
6/8/2018	10:16:40 AM	Application	Success	XBE	Administration	PARAPH	Paraph	SAGEPARA...	PARAPH a déverrouillé l'accès à la gestion d'intégrité
6/8/2018	10:16:30 AM	Application	Success	XBE	Administration	PARAPH	Paraph	SAGEPARA...	PARAPH demande à consulter les informations du site «Master» de la mach...
6/8/2018	10:16:29 AM	Application	Success	XBE	Administration	PARAPH	Paraph	SAGEPARA...	PARAPH demande à consulter les informations du domaine «SageParaphIn».
6/8/2018	10:16:23 AM	Login	Success	XBE	Administration	PARAPH	Paraph	SAGEPARA...	
6/8/2018	10:16:14 AM	Logout	Success	XBE	Administration	PARAPH	Paraph	SAGEPARA...	
6/8/2018	10:09:04 AM	Logout	Success	XBE	Moniteur	PARAPH	Paraph	SAGEPARA...	
6/8/2018	10:09:04 AM	Application	Success	XBE	Moniteur	PARAPH	Paraph	SAGEPARA...	PARAPH vient de se déloguer de l'application Moniteur.
6/8/2018	10:08:58 AM	Application	Success	XBE	Moniteur	PARAPH	Paraph	SAGEPARA...	PARAPH demande à consulter la log selon les critères suivant «Date >= 1/...
6/8/2018	10:08:30 AM	Application	Success	XBE	Moniteur	PARAPH	Paraph	SAGEPARA...	PARAPH demande à consulter la log selon les critères suivant «Source = P...
6/8/2018	10:08:30 AM	Application	Success	XBE	Moniteur	PARAPH	Paraph	SAGEPARA...	PARAPH demande à consulter la log selon les critères suivant «Ordinateur ...

Le tableau **Audit Système** décrit toutes les actions exécutées à un instant T pour chaque utilisateur.

Sécurité des données

Gestion des Droits							
Nombre de Rôles : 4				Nombre d'utilisateurs : 32			
Profils	Sites	Utilisateurs	Paramétrage	Audit Système	Audit Utilisateurs	Audit Base de Données	Mon Compte
Drag a column header here to group by that column							
Date	Heure	Statut	Utilisateur	Compte de l'utilisateur	Machine	Description	
6/8/2018	10:13:29 AM	Success	PARAPH	Paraph	SAGEPARAPHIN	Ajouter l'utilisateur 'UT12' au profil 'ADMINFONCTIONNEL -> isRole'	
6/8/2018	10:13:29 AM	Success	PARAPH	Paraph	SAGEPARAPHIN	Ajouter l'utilisateur 'UT11' au profil 'ADMINFONCTIONNEL -> isRole'	
6/8/2018	10:13:28 AM	Success	PARAPH	Paraph	SAGEPARAPHIN	Ajouter l'utilisateur 'SINISA' au profil 'ADMINFONCTIONNEL -> isRole'	
6/8/2018	10:13:28 AM	Success	PARAPH	Paraph	SAGEPARAPHIN	Ajouter l'utilisateur 'SIG8' au profil 'ADMINFONCTIONNEL -> isRole'	
6/8/2018	10:13:28 AM	Success	PARAPH	Paraph	SAGEPARAPHIN	Ajouter l'utilisateur 'SIG7' au profil 'ADMINFONCTIONNEL -> isRole'	
6/8/2018	10:13:28 AM	Success	PARAPH	Paraph	SAGEPARAPHIN	Créer un Rôle 'ADMINFONCTIONNEL' (isRole)	
6/8/2018	10:12:56 AM	Success	PARAPH	Paraph	SAGEPARAPHIN	Ajouter l'utilisateur 'UT12' au profil 'SIGNATAIRE -> isRole'	
6/8/2018	10:12:55 AM	Success	PARAPH	Paraph	SAGEPARAPHIN	Création d'un utilisateur 'UT12' (Utilisateur standard, umapiAuthenticationTypeS...	
6/8/2018	10:12:24 AM	Success	PARAPH	Paraph	SAGEPARAPHIN	Ajouter l'utilisateur 'UT11' au profil 'SIGNATAIRE -> isRole'	
6/8/2018	10:12:23 AM	Success	PARAPH	Paraph	SAGEPARAPHIN	Création d'un utilisateur 'UT11' (Utilisateur standard, umapiAuthenticationTypeS...	

Reporting de sécurité

La console d'administration **Sage XRT Common Services** vous permet d'éditer un rapport détaillant les fonctionnalités autorisées/interdites pour chaque profil, pour chacun des produits de la plate-forme.

6/8/2018	Page No.3																				
Security report																					
Annex 1 : List of rights by profile																					
There are two softwares : FRP Treasury Universe and Network Management Console. A green label for them indicates a full access for all users of the profiles. FRP Treasury Communication and FRP Treasury Signature are subfunctions of FRP Treasury Universe. The rights can be set by subfunctions; the report indicates all opened subfunctions in green . If a subfunction of an opened one is forbidden, it will appear in red .																					
<table><tr><td colspan="2">List of declared functions for profile ADMIN</td></tr><tr><td>Network Management Console</td><td></td></tr><tr><td>SAGE XRT Business Exchange</td><td></td></tr></table> <table><tr><td colspan="2">List of declared functions for profile SIGNATAIRE</td></tr><tr><td>SAGE XRT Business Exchange</td><td></td></tr><tr><td>SAGE XRT Business Exchange / Services Manager / Treatments / Files / Create</td><td></td></tr><tr><td>SAGE XRT Business Exchange / Services Manager / Treatments / Files / Delete</td><td></td></tr><tr><td>SAGE XRT Business Exchange / Services Manager / Treatments / Files / View</td><td></td></tr><tr><td>SAGE XRT Business Exchange / Services Manager / Treatments / Signature</td><td></td></tr><tr><td>SAGE XRT Business Exchange / Signature Contracts Manager</td><td></td></tr></table>		List of declared functions for profile ADMIN		Network Management Console		SAGE XRT Business Exchange		List of declared functions for profile SIGNATAIRE		SAGE XRT Business Exchange		SAGE XRT Business Exchange / Services Manager / Treatments / Files / Create		SAGE XRT Business Exchange / Services Manager / Treatments / Files / Delete		SAGE XRT Business Exchange / Services Manager / Treatments / Files / View		SAGE XRT Business Exchange / Services Manager / Treatments / Signature		SAGE XRT Business Exchange / Signature Contracts Manager	
List of declared functions for profile ADMIN																					
Network Management Console																					
SAGE XRT Business Exchange																					
List of declared functions for profile SIGNATAIRE																					
SAGE XRT Business Exchange																					
SAGE XRT Business Exchange / Services Manager / Treatments / Files / Create																					
SAGE XRT Business Exchange / Services Manager / Treatments / Files / Delete																					
SAGE XRT Business Exchange / Services Manager / Treatments / Files / View																					
SAGE XRT Business Exchange / Services Manager / Treatments / Signature																					
SAGE XRT Business Exchange / Signature Contracts Manager																					

Conformité avec la loi Sarbanes Oxley

La loi *Sarbanes Oxley* impose des règles de sécurité d'accès aux applications.

Ce paragraphe passe en revue plusieurs points sensibles liés à la sécurité d'accès et d'utilisation des produits **Sage XRT** pour un utilisateur commun.

La gestion des mots de passe au sein des applications **Sage XRT** est conforme aux exigences de la loi *Sarbanes Oxley*.

Sécurité des données

Point de sécurité	Sage XRT Business Exchange (poste lourd)	Sage XRT Business Exchange (module web)
Le système doit gérer des profils	✓	✓
Le mot de passe est obligatoire	✓	✓
Un mot de passe standard est donné à tous ou à un groupe à la création du compte	✓	✓
Le mot de passe doit être changé à la première connexion	✓ paramétrable	✓ paramétrable
Le mot de passe doit avoir 6 caractères minimum, dont 1 majuscule et 1 chiffre	✓ paramétrable	✓ paramétrable
Le mot de passe doit être changé tous les 42 jours	✓ paramétrable	✓ paramétrable
Le système historise les mots de passe. Les 4 derniers ne peuvent être réutilisés	✓ paramétrable	✓ paramétrable
Le mot de passe ne peut pas être enregistré pour qu'il ne soit plus demandé lors des connexions suivantes	<p>✓ Dans le cadre d'une sécurité NT totale, le mot de passe utilisé est celui de Windows</p> <p>paramétrable</p> <p>✓ Dans le cadre de la sécurité standard XRT, le mot de passe applicatif n'est pas enregistré.</p>	✓
Le mot de passe est verrouillé après 3 saisies de mot de passe incorrects. Il est réactivé au bout de 10 minutes	✓ paramétrable	✓ paramétrable
Le compte ne sera pas verrouillé s'il n'est pas utilisé pendant plusieurs jours	✓	✓
La session est verrouillée au bout de dix minutes d'inactivité	✗	✓ temps paramétrable
Les règles de sécurité ne peuvent être modifiées depuis	✓	✓

Sécurité des données

Point de sécurité	Sage XRT Business Exchange (poste lourd)	Sage XRT Business Exchange (module web)
la station de travail de l'utilisateur		
Les accès à l'application doivent être loggés	✓	✓
Pour les non CDI, obligation de saisir une date de fin de validité, qui sera en relation avec la date de fin de contrat	✓ paramétrable	✓ paramétrable

Données personnelles et traitements associés

Liste des données personnelles

Les données personnelles sont utilisées pour :

- identifier les utilisateurs, contrôler les accès et les autorisations sur l'application
- réaliser des contrôles, validations et signatures électroniques pour les échanges bancaires
- récupérer des fichiers de données bancaires

Les données financières des tiers permettent d'exécuter les ordres de paiement découlant d'un contrat entre les parties concernées.

Données à caractère personnel	Catégorie	Finalité
Alias de l'opérateur financier	Données client	Identification de l'utilisateur
Nom de l'opérateur financier	Données client	Identification de l'utilisateur -signataire
Prénom de l'opérateur financier	Données client	Identification de l'utilisateur -signataire
Fonction de l'opérateur financier	Données client	Identification de l'utilisateur -signataire
Téléphone de l'opérateur financier	Données client	Identification de l'utilisateur -signataire
Fax de l'opérateur financier	Données client	Identification de l'utilisateur -signataire
Email de l'opérateur financier	Données client	Identification de l'utilisateur -signataire
Certificats de l'opérateur financier	Données client	Identification du signataire
Nom contact agence bancaire	Données client	Contact banque
Téléphone contact agence bancaire	Données client	Contact banque
Fax contact agence bancaire	Données client	Contact banque
Email contact agence bancaire	Données client	Contact banque
Fonction contact agence bancaire	Données client	Contact banque
Service contact agence bancaire	Données client	Contact banque
Nom du Tiers bénéficiaire	Données Etat Civil	Paiement fournisseurs, salaires, contrôles Antifraude

Données personnelles et traitements associés


Données à caractère personnel	Catégorie	Finalité
Prénom du Tiers bénéficiaire	Données Etat Civil	Païement fournisseurs, salaires, contrôles Antifraude
Adresse du Tiers bénéficiaire	Données Etat Civil	Païement fournisseurs, salaires, contrôles Antifraude
Code pays du Tiers bénéficiaire	Données client	Païement fournisseurs, salaires, contrôles Antifraude
Téléphone du Tiers bénéficiaire	Données client	Païement fournisseurs, salaires, contrôles Antifraude
Email du Tiers bénéficiaire	Données client	Païement fournisseurs, salaires, contrôles Antifraude
Fax du Tiers bénéficiaire	Données client	Païement fournisseurs, salaires, contrôles Antifraude
Nom banque du tiers bénéficiaire	Données bancaires	Païement fournisseurs, salaires, contrôles Antifraude
BIC banque du tiers bénéficiaire	Données bancaires	Païement fournisseurs, salaires, contrôles Antifraude
IBAN – Identification du compte du Tiers bénéficiaire	Données bancaires	Païement fournisseurs, salaires, contrôles Antifraude
IBAN – Identification du compte de frais du Tiers bénéficiaire	Données bancaires	Païement fournisseurs, salaires, contrôles Antifraude
Nom du débiteur	Données Etat Civil	Prélèvements clients, contrôle Antifraude
Prénom du débiteur	Données Etat Civil	Prélèvements clients, contrôle Antifraude
IBAN du débiteur	Données bancaires	Prélèvements clients, contrôle Antifraude
Devise du compte du débiteur	Données bancaires	Prélèvements clients, contrôle Antifraude
BIC de la banque du débiteur	Données bancaires	Prélèvements clients
Référence unique du mandat	Données contrat	Prélèvements clients, contrôle Antifraude
Date de signature du mandat	Données contrat	Prélèvements clients, contrôle Antifraude
Lieu de signature du mandat	Données contrat	Prélèvements clients, contrôle Antifraude
Type de récurrence du mandat	Données contrat	Prélèvements clients, contrôle Antifraude

Gestion des utilisateurs

Les utilisateurs de l'application **Sage XRT Business Exchange** sont créés par un administrateur habilité sur chaque entité en se basant sur les utilisateurs créés dans la console d'administration (cf. § *Accès Sage XRT Common Services*, console d'Administration pour définir la politique de Sécurité).

Général Adresse Login Divers

Paramètres de connexion

Compte : SIG1 

☒ Faire un audit strict

☐ Contrôler les certificats de la liste

Options de sécurité par entité

Paramétrage

Les profils utilisateurs permettent de déterminer pour chaque entité :

- Les droits d'accès à chacune des fonctions du produit **Sage XRT Business Exchange**
- Les privilèges des utilisateurs

Opérateurs Financiers

Droits d'accès

Privileges

Liste des fonctions par service

Online Banking

ADMIFONFR - { Administration fonctionnelle }

Paramétrage

ADMTFR - { Administration }

Paramètres utilisateur

Notifications et alertes

AFRAUD - { Antifraude }

Anomalies

Liste autorisée

Liste d'exclusion

Procédure

Sécurité

BANKFEES - { Frais bancaires }

Flux d'information

Analyses

FILEFR - { Téléchargement }

UPLOAD - { Emission de fichiers }

DOWNLOAD - { Réception de fichiers }

HISTORY - { Historique des transferts }

MANDATFR - { Mandatèque }

Paramétrage

Création

Importation

Modification

Plate

Révoquer tous les droits

Accorder tous les droits

Reporting

Toutes les actions sur les utilisateurs sont consignées dans les journaux d'audit pour le site **Online Banking** (création-modification-suspension) ou dans l'audit de l'administration (cf. § *Fonctionnalités d'Audit sur la gestion des identités et des accès*).

Historique - Page 1/1

20 résultats par page

Date et Heure	Utilisateur	Entité	Action	Opérateur	Statut	Motif
11/04/2018 14:55:15	SIG2 Votre prénom {SIG2}	SOCIETE {SOCIETE}	Modifier	SIG1 Votre prénom {SIG1} - SOCIETE {SOCIETE}	Actif	
11/04/2018 14:55:11	SIG1 Votre prénom {SIG1}	SOCIETE {SOCIETE}	Modifier	SIG1 Votre prénom {SIG1} - SOCIETE {SOCIETE}	Actif	
11/04/2018 14:54:38	SIG1 Votre prénom {SIG1}	SOCIETE {SOCIETE}	Modifier	SIG1 Votre prénom {SIG1} - SOCIETE {SOCIETE}	Actif	
11/04/2018 14:54:21	SIG2 Votre prénom {SIG2}	SOCIETE {SOCIETE}	Activer	SIG1 Votre prénom {SIG1} - SOCIETE {SOCIETE}	Actif	
11/04/2018 14:54:14	SIG2 Votre prénom {SIG2}	SOCIETE {SOCIETE}	Modifier	SIG1 Votre prénom {SIG1} - SOCIETE {SOCIETE}	Non actif	
11/04/2018 14:54:00	SIG2 Votre prénom {SIG2}	SOCIETE {SOCIETE}	Suspendre	SIG1 Votre prénom {SIG1} - SOCIETE {SOCIETE}	Non actif	suspendre
11/04/2018 14:44:27	SIG2 Votre prénom {SIG2}	SOCIETE {SOCIETE}	Modifier	{SYSTEM\$} - {SYSTEM\$}	Actif	
11/04/2018 10:57:13	SIG1 Votre prénom {SIG1}	SOCIETE {SOCIETE}	Modifier	{SYSTEM\$} - {SYSTEM\$}	Actif	
29/12/2017 15:09:07	SIG1 Votre prénom {SIG1}	SOCIETE {SOCIETE}	Modifier	{SYSTEM\$} - {SYSTEM\$}	Actif	
13/12/2017 11:51:35	SIG2 Votre prénom {SIG2}	SOCIETE {SOCIETE}	Modifier	{SYSTEM\$} - {SYSTEM\$}	Supprimé	
12/12/2017 18:25:19	SIG1 Votre prénom {SIG1}	SOCIETE {SOCIETE}	Modifier	{SYSTEM\$} - {SYSTEM\$}	Supprimé	

Signataires

Finalité des traitements

Les signataires réalisent les contrôles, validations et signatures électroniques personnelles des échanges de données financières informatisées entre une société et son partenaire bancaire.

Les échanges de données informatisées consistent à exécuter les ordres de paiement découlant d'un contrat entre deux parties (règlement des salaires, factures fournisseurs, prélèvements bancaires).

Gestion : création-modification-suppression

La création des signataires par un administrateur habilité est possible si :

- L'utilisateur a été créé dans la console d'administration **Sage XRT Common Services** (cf. § *Fonctionnalités d'Audit sur la gestion des identités et des accès*).
- L'utilisateur a été créé dans l'application **Sage XRT Business Exchange**.
- Le privilège **Signataire** lui a été accordé.

La modification et suppression d'un signataire est accessible par un utilisateur habilité.

Données personnelles et traitements associés

Reporting sur la base

Toutes les actions des signataires sont consignées dans le journal des événements du service de transactions.

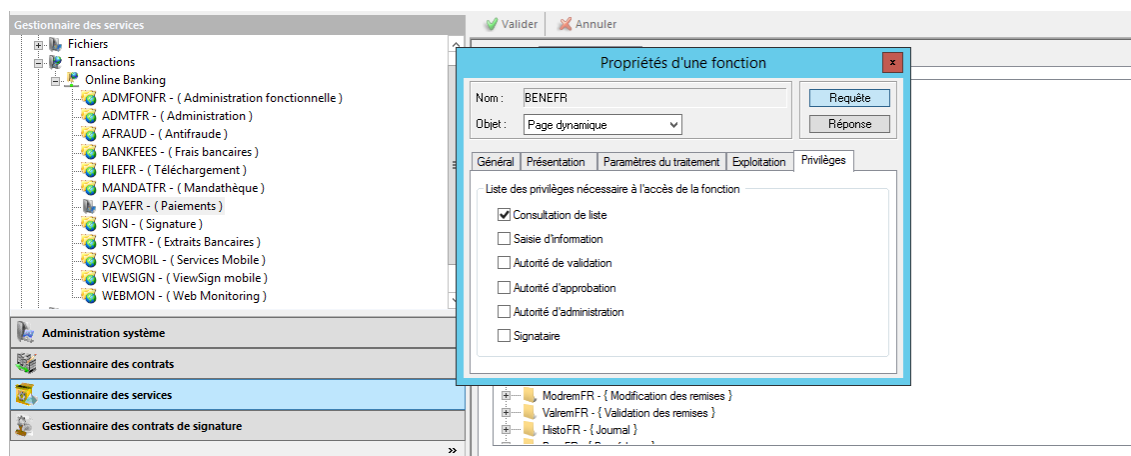
Date & Heure	Entité	Utilisateur	Transaction	Fonction	Description	Ordinateur	Protocole	Référence du moniteur
4/11/2018 11:34:57 AM	SOCIETE	SIG1	SIGN	SIGN	Paraphage du fichier (Validation) : 1521	SAGEPARA...	Online Banki...	T(17EF59CF-7CA9-4FE
4/11/2018 11:34:29 AM	SOCIETE	SIG1	SIGN	SIGN	Demande de signature de fichier(s) : 1524,1523...	SAGEPARA...	Online Banki...	T(04EEF072-5857-46E
4/11/2018 11:34:07 AM	SOCIETE	SIG1	SIGN	ADD	Demande d'ajout (avec préparation automatiqu...	SAGEPARA...	Online Banki...	T(3C719490-AEF4-449
4/6/2018 5:42:10 PM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T(232571D5-224C-42B
4/6/2018 5:42:07 PM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T(57FEE671-5957-424F
4/6/2018 5:42:04 PM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T(9F785A70-0804-4BF
4/6/2018 5:41:29 PM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T(0B7B9570-218C-415
4/6/2018 5:41:20 PM	SOCIETE	SIG1	SIGN	LOCKS	Demande de déverrouillage de fichier(s) : 1520	SAGEPARA...	Online Banki...	T(B5FCA2F7-1DA8-412
4/6/2018 5:39:56 PM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T(E8170413-17C8-4EE
4/6/2018 5:39:38 PM	SOCIETE	SIG1	SIGN	SIGN	Demande de signature de fichier(s) : 1520	SAGEPARA...	Online Banki...	T(15D05DB5-B965-43F
4/6/2018 5:39:19 PM	SOCIETE	SIG1	SIGN	ADD	Demande d'ajout (avec préparation automatiqu...	SAGEPARA...	Online Banki...	T(69EDD189-B66F-453
4/6/2018 5:35:07 PM	SOCIETE	SIG1	SIGN	ADD	Demande d'ajout (avec préparation automatiqu...	SAGEPARA...	Online Banki...	T(CED2F536-9D9B-42
4/6/2018 12:20:31 PM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T(3FF99B4A-B202-4A1
4/6/2018 11:50:56 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T(8DBDE346-78C0-4FE
4/6/2018 11:50:54 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T(0A86B3FD-7C9B-4FF
4/6/2018 11:50:51 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T(C26113C5-75BB-4D1
4/6/2018 11:50:22 AM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T(A44FC8CC-A049-400
4/6/2018 11:49:11 AM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T(4BFED8D8-2FC2-41
4/6/2018 11:45:58 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T(5E85A9AE-608A-4C0
4/6/2018 11:45:56 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T(E574D633-7455-49B
4/6/2018 11:45:54 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T(401EA4CD-DBDA-44
4/6/2018 11:45:50 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T(24DEFBE7-9614-402
4/6/2018 11:42:46 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T(663671D6-233B-45C
4/6/2018 11:40:37 AM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T(C1BC52D7-69A7-40E
4/6/2018 11:35:18 AM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T(9ED17AA6-D3C5-4E
4/6/2018 11:30:55 AM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T(6ECD3AC5-DAE5-4E
4/6/2018 11:17:59 AM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T(67F60B78-B5BA-484

Tiers : Clients-Fournisseurs-Salariés

La liste des tiers est alimentée soit manuellement, soit automatiquement par l'importation d'un fichier de tiers ou de transactions.

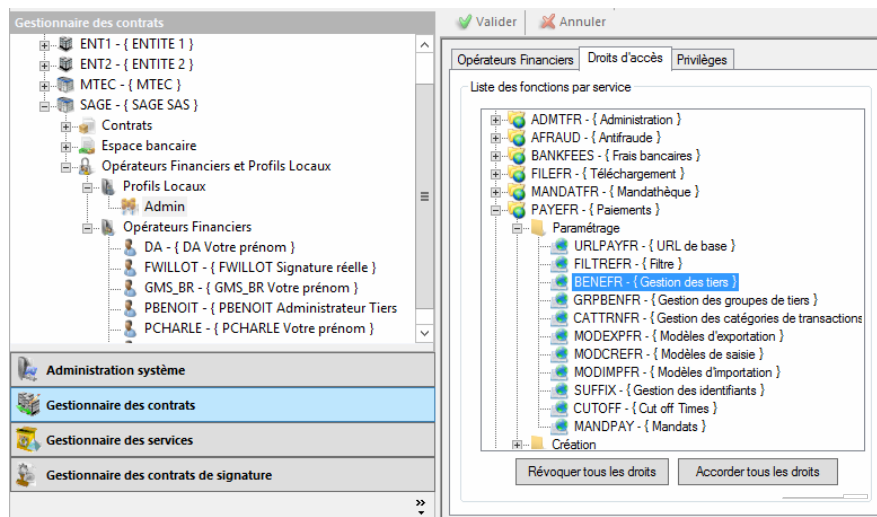
Cette liste est disponible dans l'application à titre consultatif. Elle peut être modifiée et supprimée.

La déclaration d'accès aux fonctions définit les personnes habilitées à gérer les tiers.

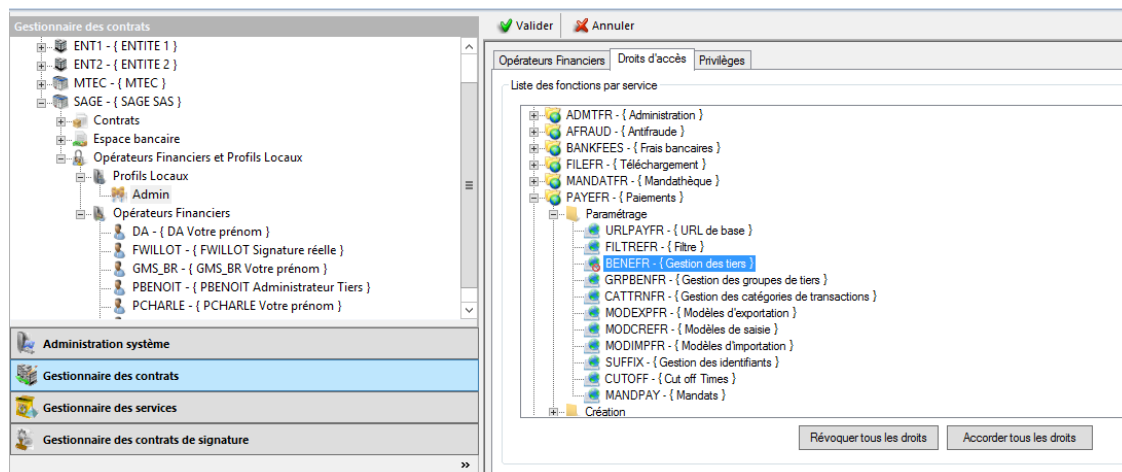


Déclaration du niveau de privilège minimum pour accéder à la fonction de gestion des tiers

Données personnelles et traitements associés



Déclaration d'autorisation d'accès à la fonction de gestion des tiers



Déclaration d'interdiction d'accès à la fonction de gestion des tiers

Accueil Paramétrage Création Importation Modification Validation Autorisation Modification des remises Validation des remises Journal Procédures Gestion des incidents Automatismes Répartition bancaire Sécurité Exportation

URL de base Filtre **Tiers** Groupes de tiers Catégories de transactions Modèles d'exportation Modèles de saisie Modèles d'importation Identifiants Cut off Times Mandats

Les tiers ainsi que leurs banques et/ou comptes doivent être créés préalablement à la saisie des transactions de paiement. Lors de la création d'une transaction, vous sélectionnez un tiers existant.

Recherche

Filtre appliqué :

Entité d'origine :

Code : Nom :

☐ Mis à jour suite au traitement des corrections de domiciliation reçues

Liste des tiers - Page 1/1

20 résultats par page

	Tiers	Identifiant bancaire	Banque	Pays	Source	Statut	Tm	Correction Domiciliation
<input type="checkbox"/>	MOB1 - MOB1	FR111112222333333333344		FR	Manuel	Actif		
<input type="checkbox"/>	MOB2 - MOB2	FR12345678901234567890123		FR	Manuel	Actif		
<input type="checkbox"/>	T001 - name001	FR6004100001000000000135555555	LCL	FR	Manuel	Actif		
<input type="checkbox"/>	T002 - name002	FR2004100001000000000166	LCL	FR	Manuel	Actif		

Liste des tiers présentée à un utilisateur bénéficiant d'un niveau de privilège au-delà de Consultation

Données personnelles et traitements associés

Les données personnelles sont listées ci-dessous :

Accueil Paramétrage Création Importation Modification Validation Autorisation Modification des remises Validation des remises Journal Procédures Gestion des incidents

URL de base Filtre **Tiers** Groupes de tiers Catégories de transactions Modèles d'exportation Modèles de saisie Modèles d'importation Identifiants

Pour ajouter un nouveau tiers, saisissez l'ensemble des champs du formulaire puis cliquez sur le bouton 'Enregistrer'.

Tiers

Type de tiers : Créditeur/Debiteur

Code d'identification :

Nom :

Identifiant national :

Type autre identifiant :

Autre identifiant :

Adresse :

Code Postal :

Code Province :

Ville :

Etat :

Pays :

☐ Non résident

Interlocuteur :

Service :

Téléphone :

Fax :

Email :

☒ Propriétaire du compte

Nom du propriétaire du compte :

Adresse :

Code Postal :

Ville :

Numéro d'autorisation :

Banque

Nom :

Type autre identifiant :

Autre Identifiant :

Adresse :

Code Postal :

Code Province :

Ville :

Etat :

Pays :

Code BIC :

Code BIC1 (non connecté) :

Compte postal :

Vérifier Rechercher Déduire à partir de l'IBAN...

Vérifier Rechercher

Compte

Type de RIB :

Compte :

Devise :

Domiciliation :

☒ Local ☐ IBAN ☐ BBAN

Pays Clé IBAN N° compte

Finalité des traitements

Les traitements utilisant les tiers permettent de procéder à des règlements ou à des encaissements en fonction de la nature du transfert utilisé et de la catégorie du tiers concerné.

Gestion des paiements

Les différents types de paiements gérés dans **Sage XRT Business Exchange** s'appuient sur les zones du tiers utiles pour la constitution des remises.

Données personnelles et traitements associés

Par exemple, pour un virement domestique, les coordonnées d'un tiers sont incluses dans la transaction dès lors qu'il participe à la remise.

Accueil Paramétrage **Création** Importation Modification Validation Autorisation Modification des remises Validation des remises Journal Procédures Gestion des incidents

Vir. compte à compte **Vir. domestique** Vir. international Vir. commercial Chèque Prélèvement Ordre de paiement

Identification

Catégorie de transaction : SCT VDOM 001.001.03
Banque émettrice : BNP - (FR)

Intervenants

Donneur d'ordre : SAGE SAS
Payeur : SAGE SAS
Compte à débiter : 30004000010000000000039 - (FR763000400001000
Bénéficiaire : T001 - name001
Payé : T001 - name001

Transfert

Référence :
Montant : 1200 EUR
Type de virement : Différé
Date d'exécution : 18/04/2018 Format JJ/MM/AAAA
Date de valeur : 18/04/2018 Format JJ/MM/AAAA
Finalité : Salaire
Motif :
Type de récurrence : Unique
Date de début : Format JJ/MM/AAAA
Date de fin : Format JJ/MM/AAAA

Saisie manuelle d'un virement domestique

Accueil Paramétrage **Création** Importation Modification Validation Autorisation Modification des remises Validation des remises Journal Procédures Gestion des incidents Automatismes Répartition bancaire Sécurité Exportation

Vir. compte à compte **Vir. domestique** Vir. international Vir. commercial Chèque Prélèvement Ordre de paiement

Veillez relire et confirmer l'ordre de virement ci-dessous :

Identification

Catégorie de transaction : SCT VDOM 001.001.03
Banque émettrice : BNP

Intervenants

Donneur d'ordre : SAGE SAS
Payeur : SAGE SAS
Compte à débiter : 30004000010000000000039 - (FR7630004000010000000000039 EUR)
Bénéficiaire : T001 - name001
Payé : T001 - name001
Compte à créditer : FR50600410000100000000001355555555

Transfert

Référence : REFERENCE
Montant : 1 200.00 EUR
Date d'exécution : 18/04/2018
Date d'exécution initiale : 18/04/2018
Date de valeur : 18/04/2018

Confirmation d'enregistrement d'un virement domestique

Données personnelles et traitements associés

Gestion des encaissements

Les différents types d'encaissement gérés dans **Sage XRT Business Exchange** s'appuient sur les zones du tiers utiles pour la constitution des remises.

Par exemple, pour un prélèvement domestique, les coordonnées d'un tiers sont incluses dans la transaction dès lors qu'il participe à la remise.

Accueil Paramétrage **Création** Importation Modification Validation Autorisation Modification des remises Validation des remises Journal Procédures Gestion des incidents

Vir. compte à compte Vir. domestique Vir. international Vir. commercial Chèque **Prélèvement** Ordre de paiement

A partir d'un modèle

Liste des modèles :

Identification

Catégorie de transaction : SDD 008.002.02
Banque émettrice : BNP - (FR)
Mandat :

Intervenants

Payé : SAGE SAS
Compte à créditer : 3000400001000000000039 - (FR763000400001000
Payeur : T001 - name001 [Créer](#)

Transfert

Référence :
Montant : 1200 EUR
Date d'échéance : 18/04/2018 Format JJ/mm/aaaa
Date de valeur : 18/04/2018 Format JJ/mm/aaaa
Motif :

Type de récurrence : Unique
Intervalle :
Date de début : Format JJ/mm/aaaa

Saisie manuelle d'un prélèvement

Données personnelles et traitements associés

Gestion des tiers

La gestion du ou des tiers s'effectue via le filtre standard des tiers. Un filtre peut être privé, à usage ponctuel ou répétitif, appliqué par défaut ou non.

Accueil Paramétrage Création Importation Modification Validation Autorisation Modification des remises Validation des remises Journal Procédures Gestion des incidents Automatismes Répartition bancaire Sécurité Exportation

URL de base **Filtre** Tiers Groupes de tiers Catégories de transactions Modèles d'exportation Modèles de saisie Modèles d'importation Identifiants Cut off Times Mandats

Identification

Libellé :

Type de filtre : Tiers

Définition du filtre

Le filtre s'applique sur la liste des tiers présentée avant visualisation, création, importation, modification, suppression d'un tiers, ainsi que sur l'aide à la recherche d'un tiers.

☐ Type de tiers :

☐ Groupe(s) de tiers

☐ Code d'identification

☐ Pays : AD

☐ Devise(s) RIB : AED

☐ Source :

☐ Statut(s) :

☐ Nom(s)

Application

☒ Filtre par défaut

Utilisation du filtre :

☒ Uniquement par celui qui l'a créé

☐ Toute personne habilitée

Enregistrer Retour Réinitialiser

Création d'un filtre sur la liste des tiers

Filtre **Tiers** Groupes de tiers Catégories de transactions Modèles d'exportation Modèles de saisie Modèles d'importation Identifiants Cut off Times Mandats

Recherche

Filtre appliqué : FILTRE TIERS Modifier

Entité d'origine :

Code : Nom :

☐ Mis à jour suite au traitement des corrections de domiciliation reçues

Liste des tiers - Page 1/1

20 résultats par page

	Tiers	Identifiant bancaire	Banque	Pays	Source	Statut	Tm	Correction Domiciliation
<input type="checkbox"/>	MOB1 - MOB1	FR111112222333333333344		FR	Manuel	Actif		
<input type="checkbox"/>	MOB2 - MOB2	FR12345678901234567890123		FR	Manuel	Actif		
<input type="checkbox"/>	T001 - name001	FR60041000010000000000135555555	LCL	FR	Manuel	Actif		
<input type="checkbox"/>	T002 - name002	FR20041000010000000000166	LCL	FR	Manuel	Actif		

Liste filtrée de tiers

Un tiers a la possibilité de faire modifier, par une personne habilitée, le contenu de ses données personnelles. La modification de son numéro de compte peut être notifiée au tiers considéré, via le paramétrage de l'alerte sur le type de données des tiers.

Droit à l'oubli des données personnelles des tiers

Un tiers a la possibilité de faire supprimer, par une personne habilitée le contenu de ses données personnelles.

Données personnelles et traitements associés

Export sur la base

Le reporting des tiers s'effectue via l'utilisation d'un filtre, d'un modèle (permettant de définir quelles données exporter) et d'un format.

The screenshot shows the 'Tiers' tab selected in a navigation bar. Below the bar, a message states: 'Pour sélectionner les tiers que vous voulez exporter, sélectionner un filtre, un modèle d'export et un format.' The main area contains a 'Définition' section with the following fields:

- Type d'exportation : Libre (dropdown)
- Filtre appliqué : FILTRE TIERS (dropdown) with a 'Modifier' button next to it.
- Modèle d'exportation : (empty dropdown)
- Format : A dropdown menu is open, showing options: XML, ASCII, EXCEL, and WORD.

A blue 'Exporter' button is located at the bottom left of the form.

Déclenchement de l'export

The screenshot shows the 'Modèles d'exportation' tab selected in a navigation bar. The main area is divided into two sections: 'Identification' and 'Caractéristiques'.

Identification section:

- Libellé : MODELE EXPORT
- Type de données : Tiers

Caractéristiques section:

- Liste des champs disponibles :** A list box containing 'Adresse de la banque', 'Adresse du propriétaire du compte', 'Autre identifiant', 'Autre identifiant de la banque', and 'Code BIC de la banque'.
- Exporter les champs dans cet ordre :** A list box containing 'Nom', 'Adresse', 'Ville', 'Pays', and 'Email'.
- Between the two list boxes are '>>>' and '<<<' buttons.
- Below the 'Exporter les champs dans cet ordre' list box are 'Déplacer vers le haut' and 'Déplacer vers le bas' buttons.

At the bottom, there are three buttons: 'Modifier' (blue), 'Supprimer' (orange), and 'Réinitialiser' (orange).

Paramétrage d'un modèle d'export

Contacts des Agences Bancaires

Finalité des traitements

Les données personnelles de la partie **Contact** de l'agence peuvent être utilisées lors :

- des communications relatives aux contrats d'échange de données informatisées
- d'un évènement empêchant la réalisation des échanges bancaires

Gestion

La création, modification ou suppression des données du contact bancaire est accessible par l'administrateur de l'application.

Reporting sur la base

Les actions de consultation des agences bancaires sont consignées dans l'audit de l'administration (cf. § *Fonctionnalités d'Audit sur la gestion des identités et des accès*).

Droit de rectification et d'effacement des données - Durée de conservation des données personnelles

Vous avez la possibilité de modifier ou de supprimer toute donnée personnelle dans votre application pour répondre à la demande d'une personne physique.

Les applications proposent cependant un certain nombre de contrôles techniques qu'il conviendra de respecter pour finaliser la modification ou la suppression.

Important ! Toutes les lois locales imposent des règles minimales de conservation des données.

Délai de conservation des fichiers :

Mode serveur émetteur :	
Nombre de relectures permises :	<input type="text" value="-1"/> <input type="button" value="↑"/> <input type="button" value="↓"/>
Nombre de jours de mise à disposition :	<input type="text" value="-1"/> <input type="button" value="↑"/> <input type="button" value="↓"/>
Mode demandeur/serveur récepteur :	
Nombre de jours pour les fichiers reçus :	<input type="text" value="-1"/> <input type="button" value="↑"/> <input type="button" value="↓"/>
Mode demandeur émetteur :	
Nombre de jours pour les fichiers émis :	<input type="text" value="-1"/> <input type="button" value="↑"/> <input type="button" value="↓"/>
Archivage :	
Nombre de jours pour les fichiers archivés :	<input type="text" value="-1"/> <input type="button" value="↑"/> <input type="button" value="↓"/>
Signature :	
Nombre de jours pour les fichiers archivés :	<input type="text" value="-1"/> <input type="button" value="↑"/> <input type="button" value="↓"/>

Paramétrage de conservation des fichiers contenant des données personnelles en communication

Dans l'administration **Sage XRT Business Exchange**, vous pouvez également paramétrer des purges automatiques pour :

- Les fichiers reçus
- Les archives

Mesures de sécurité complémentaires

Afin de minimiser le risque de violation de données et de pénalité, certains principes élémentaires de sécurité sont recommandés.

Même si la sécurisation du système et du réseau reste sous votre responsabilité, la plateforme de la solution vous fournit quelques outils :

- Les navigateurs web standard et les protocoles *http* ou *https* sont utilisés. La technologie web assure une isolation de premier niveau entre le serveur web et le poste de travail.
- Les mots de passe ne sont pas transférés sur le réseau. Le système d'authentification est basé sur des normes. Il peut s'agir d'une connexion *Windows* contrôlée dans un annuaire *LDAP* ou d'une authentification par certificat. Par souci de simplicité, une solution basée sur les utilisateurs et les mots de passe cryptés stockés dans le serveur web de la solution est disponible. Vous pouvez ajouter une double authentification.
- La gestion des droits est effectuée au niveau des entités. Elle est basée sur les profils de fonctions associés à l'utilisateur. Il est également possible de gérer les permissions d'accès aux contrats au niveau des services pour chaque entité.

Mesures générales

Utilisation de https

La solution est une application web accessible via une connexion *http* ou *https*. Bien que *http* soit disponible, nous vous recommandons de toujours utiliser *https* pour les instances de production, en particulier si votre solution est accessible à partir de l'internet public.

Mots de passe solides

Si vous utilisez ce mode d'authentification, n'oubliez pas d'établir une politique de gestion des mots de passe, afin que les utilisateurs définissent un mot de passe fort.

Pour optimiser la sécurité, un mot de passe fort doit :

- contenir 6 caractères minimum (plus il y a de caractères, plus le mot de passe est solide)
- utiliser une combinaison de chiffres, de majuscules et minuscules et de symboles (tels que @ # \$ % ! ? &, etc.)
- ne pas contenir un motif de clavier tel que *azerty*
- ne pas contenir la date de naissance de l'utilisateur
- Ne pas être utilisé sur plusieurs applications

Sécurisation des serveurs par droit d'accès

Les serveurs hébergeant les composants de la solution contiennent des fichiers de configuration et d'autres données vulnérables aux menaces internes.

Les administrateurs doivent être les seules personnes autorisées à se connecter aux serveurs.

Veillez à octroyer à ces utilisateurs les droits destinés à l'administration de la solution sur les répertoires appropriés.

Important ! Les administrateurs de serveur doivent être différents des administrateurs de la solution.

Protection des serveurs

Les serveurs de solution doivent être construits en utilisant les normes de l'industrie.

Utilisation de pare-feux locaux

Utilisez des pare-feux locaux sur vos serveurs pour verrouiller tout port IP qui n'est pas nécessaire au fonctionnement de la solution ou à l'accès des utilisateurs.

Généralement, si tous les composants de la solution sont installés sur un même serveur, la solution n'a besoin que des ports *http* ou *https* pour fonctionner.

Pour les installations à plusieurs serveurs, vous devez ouvrir les ports (ou plages de ports) nécessaires à la communication entre les différents composants.

Sécurisation de l'architecture internet

L'architecture que vous implémentez est la clé de votre sécurité, tout particulièrement si votre système est accessible à partir de l'internet public.

Pour connecter vos systèmes et les rendre disponibles sur internet, vous devez décider :

- quels serveurs et ports doivent être vus du monde extérieur
- comment les requêtes extérieures sont interceptées, traduites et dirigées vers ces serveurs et ports, le cas échéant.

Cela implique des équipements tels que :

- un pare-feu, situé entre votre réseau interne et internet pour intercepter les requêtes entrantes et les transférer vers les serveurs appropriés de votre réseau
- une *DMZ* ou "zone démilitarisée", c'est-à-dire une zone de réseau physique ou logique qui isole votre réseau local d'internet.

Le pare-feu est le gardien des *points de contrôle* de votre *DMZ*.

Note : Ces recommandations ne s'appliquent que si votre solution est visible sur internet. Vous n'avez pas besoin de configurer de **DMZ** ni de pare-feu externe si vous utilisez votre propre réseau local.

Transparent Data Encryption TDE

Pour mieux sécuriser votre base de données, vous pouvez utiliser le chiffrement *TDE (Transparent Data Encryption)*.

Le chiffrement *TDE* vous permet de crypter la base de données.

Sage XRT Business Exchange 12.1 a été validé avec les environnements suivants :

- SQL Server 2016 TDE
- Oracle 12c TDE

Chiffrement des données en transit

La communication entre votre couche applicative et votre base de données peut se faire à travers la norme *TLS (Transparent Layer Security)*.

L'option **ForceEncryption** de **SQL Server** force le chiffrement du protocole et vous permet de préserver la confidentialité des informations en cryptant les données.

Chiffrement des sauvegardes de la base de données

Afin de protéger les données, il est recommandé de chiffrer les sauvegardes de la base de données.

Le chiffrement *TDE* protège de fait les sauvegardes car il est impossible de restaurer ou d'attacher des fichiers sans le certificat.

Important ! Il est fondamental de sauvegarder le certificat en lieu sûr, et de ne pas stocker au même endroit les sauvegardes des bases et celle du certificat. Pour *Oracle*, vous pouvez utiliser le cryptage du réseau natif.

Sécurité du système de fichiers

La sécurité du système de fichiers des différents serveurs doit être implémentée avec les outils appropriés (antivirus, sécurité d'accès au réseau, etc.).

Assurez-vous que ces outils n'entraînent aucun problème de performance.

Par exemple, évitez d'exécuter une analyse antivirus continue sur un serveur de base de données.

Mesures applicatives

Signature de l'application et du site web

Le code de votre application est signé. Cette signature certifie que le programme est légitime et conforme au développement initial et que l'intégrité des fichiers binaires de votre application est assurée.

Pour assurer l'intégrité du site web **Online Banking**, vous pouvez calculer une signature.

Mesures de sécurité complémentaires

Un administrateur habilité gère le calcul et le contrôle de la signature sur le site *master* de **Sage XRT Business Exchange**.

Important ! Pour activer l'intégrité du site web, vous devez définir un passphrase. Ce passphrase doit être stocké en lieu sûr.

La solution prend en charge plusieurs modes d'authentification :

- **Sécurité intégrée de Windows NT** : l'utilisateur est authentifié grâce à son compte NT. Ce niveau d'authentification est recommandé.
- **Nom d'utilisateur et un mot de passe** : l'utilisateur est authentifié grâce à un nom d'utilisateur et un mot de passe.
- **Authentification de l'utilisateur via un certificat X509** : pour le client web, l'authentification forte est un système d'authentification à deux phases :
 - Vérification du certificat sur le répertoire *Active Directory* de l'entreprise
 - Challenge/Réponse entre le client et le composant d'authentification, permettant de vérifier l'identité du client
- **Double authentification** : un deuxième facteur est utilisé pour l'authentification des utilisateurs afin de générer un mot de passe à usage unique.
- **SageID**

Autorisations

Un utilisateur a accès à une ou plusieurs entités. Il est associé à un profil qui détermine ses droits d'accès aux fonctions de l'application et ses privilèges : consultation de liste, saisie d'information, autorité de validation, autorité d'approbation, autorité d'administration et signataire.

Les privilèges sont déterminés par les packages d'import.

Mesures de sécurité complémentaires

Il est possible sur chaque contrat bancaire de paramétrer des autorisations spécifiques pour les utilisateurs et les signataires (accès aux contrats, accès aux éditions, droits d'archivage et droits d'extraction).

Grâce à ces fonctionnalités, vous pouvez définir différemment l'accès aux données critiques sur chaque entité pour un utilisateur donné.

Important ! Assurez-vous de conserver ces règles au fil du temps. Simplifiez-les au maximum, sans compromettre votre politique de sécurité.

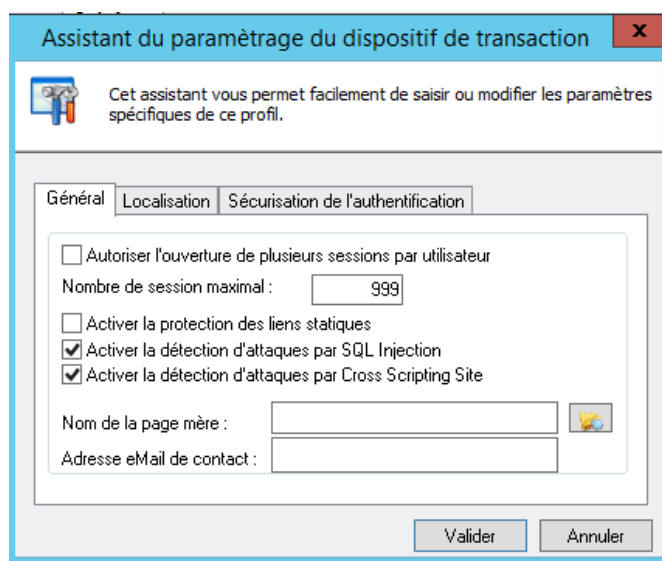
Protection contre les attaques

Certaines attaques peuvent compromettre la sécurité de vos données et de votre domaine.

Les requêtes *SQL injection* permettent d'injecter dans une requête SQL en cours un morceau de requête non prévu par le système et pouvant compromettre la sécurité du site web.

Le *Cross-Site Scripting* est un type de faille de sécurité des sites web qui injecte du contenu dans une page, permettant ainsi des actions sur les navigateurs web visitant la page.

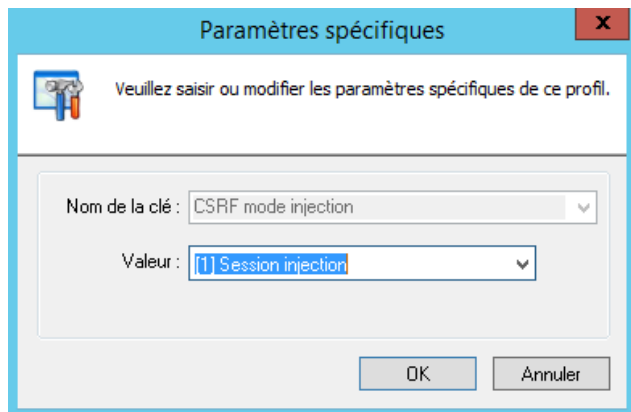
Vous pouvez activer les options de détection d'attaque au niveau du service de transaction.



L'objectif d'une attaque *CSRF (Cross-Site Request Forgery)* est de transmettre à un utilisateur authentifié une requête *http* falsifiée qui pointe sur une action interne au site, afin qu'il l'exécute sans en avoir conscience et en utilisant ses propres droits.

Mesures de sécurité complémentaires

Activez l'option dans les paramètres spécifiques du service.



Les attaques *DTD* sont des failles de sécurité sur les parseurs *XML*.

Ces failles ont déjà été utilisées pour réaliser des attaques par déni de service. Elles permettent également d'obtenir le contenu d'un fichier en intégrant une entité externe.

Le code de l'application utilise le compilateur *XSL.NET* de dernière génération.

Périodicité d'accès au site web

Vous pouvez définir une périodicité d'accès au site web, afin de contrôler la légitimité des connexions.

Un calendrier d'accès aux données peut être défini.

Exemple : Accès des utilisateurs au site web **Online Banking** non autorisé le week-end.

Pour aller plus loin

La mise en œuvre de ces mesures de sécurité complémentaires nécessite des compétences ainsi que des retours d'expérience que nos équipes de consulting sont en mesure de vous apporter.

Nous vous engageons à les contacter si vous souhaitez appliquer ces recommandations.

Avertissement

Les informations relatives au Règlement Général de Protection des Données (ci-après RGPD) fournies par Sage sont de nature générale et communiquées à titre informatif. Elles ne constituent pas un avis professionnel ou juridique. Sage ne saurait garantir qu'une information communiquée reproduise exactement une réglementation ou un texte législatif adopté officiellement. En cas de désaccord, le texte du journal officiel prévaut.

Bien que nous ayons fait notre possible pour nous assurer que les informations fournies soient exactes et à jour, les informations sont données telles quelles sans aucune garantie, explicite ou implicite. Sage n'assume aucune responsabilité pour toute erreur ou omission et n'est pas tenue responsable des dommages (y compris, entre autres, les dommages relatifs à la perte de clients ou de bénéfices) découlant de l'utilisation de ces informations ou de toute mesure ou décision prise en conséquence de l'utilisation de ces informations.

Nos produits intègrent des fonctions facilitatrices visant à accompagner l'utilisateur dans sa démarche de mise en conformité au RGPD. Toutefois, nous attirons l'attention des utilisateurs quant au fait que la seule utilisation des produits n'est pas de nature à garantir leur conformité au RGPD.

Nous rappelons que les informations communiquées ne dispensent pas l'utilisateur des produits Sage de consulter un conseil juridique afin d'obtenir toutes informations utiles relatives au RGPD et de s'y conformer.