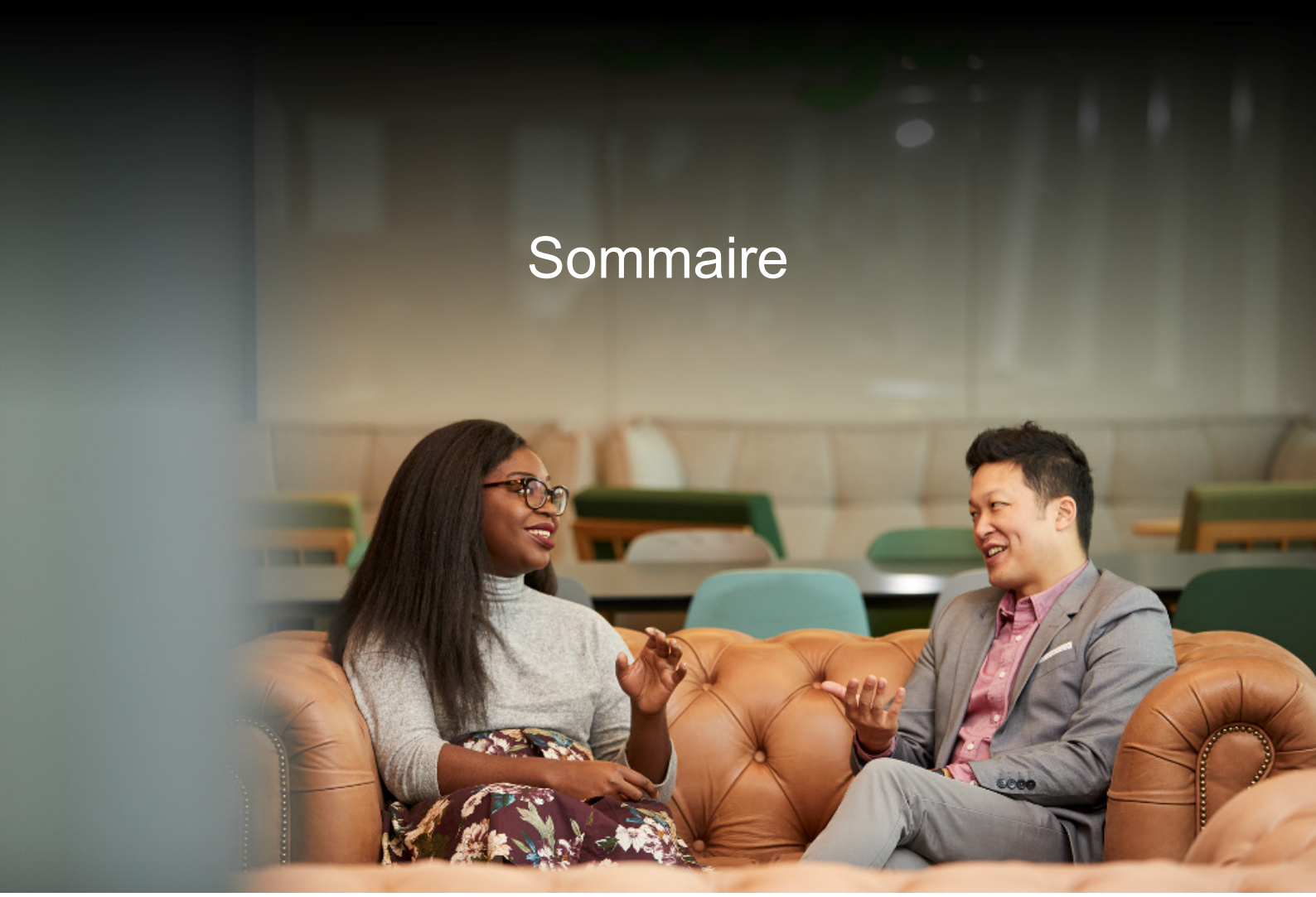
Sage XRT Communication & Signature

Version 4.0.500

Données Personnelles

Sommaire



Objectif du document **4**

Principales exigences européennes sur la protection des données personnelles **5**

Sécurité des données **6**

Sécurité d'accès à la base de données 6

Affectation des permissions 6

Choix du niveau d'authentification souhaitée 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 10

Données personnelles et traitements associés **12**

Liste des données personnelles 12

Gestion des utilisateurs 13

Options de sécurité par contrat bancaire 14

Paramétrage 14

Reporting 14

Signataires 14
Finalité des traitements 14
Gestion : création-modification-suppression 15
Reporting sur la base 15
Droit à la rectification et à l'effacement des données - Durée de conservation des données personnelles 15
Mesures de sécurité complémentaires ..... Erreur ! Signet non défini.
Mesures générales ..... **Erreur ! Signet non défini.**
Utilisation de https ..... **Erreur ! Signet non défini.**
Mots de passe solides ..... **Erreur ! Signet non défini.**
Sécurisation des serveurs par droit d'accès ..... **Erreur ! Signet non défini.**
Protection des serveurs ..... **Erreur ! Signet non défini.**
Chiffrement des données en transit 16
Sécurité du système de fichiers 18
Mesures applicatives 18
Signature de l'application 18
Authentifications 18
Autorisations 18
Pour aller plus loin ..... **Erreur ! Signet non défini.**
Avertissement 19

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 Communication & Signature** qui peuvent faciliter la mise en conformité des entreprises avec ce règlement européen.

©Sage 2018

Principales exigences européennes

Principales Exigences sur la protection des données personnelles	Sage XRT Communication & Signature
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	
Renforcement des mots de passe et de la protection de certaines données stockées ou échangées. cf. les fonctionnalités existantes en matière de sécurité	✔
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.	
Utilisation des fonctions de modification/suppression disponibles dans chaque Produit et accessibles selon les habilitations et les droits de l'utilisateur. cf. les fonctionnalités existantes sur les données personnelles	✔
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 règlementation 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.	
Sage met à votre disposition une cartographie des données personnelles et des traitements associés pour **Sage XRT Communication & Signature**. cf. la liste des données personnelles et des traitements associés	✔

©Sage 2018

Sécurité des données

Sécurité d’accès à la base de données

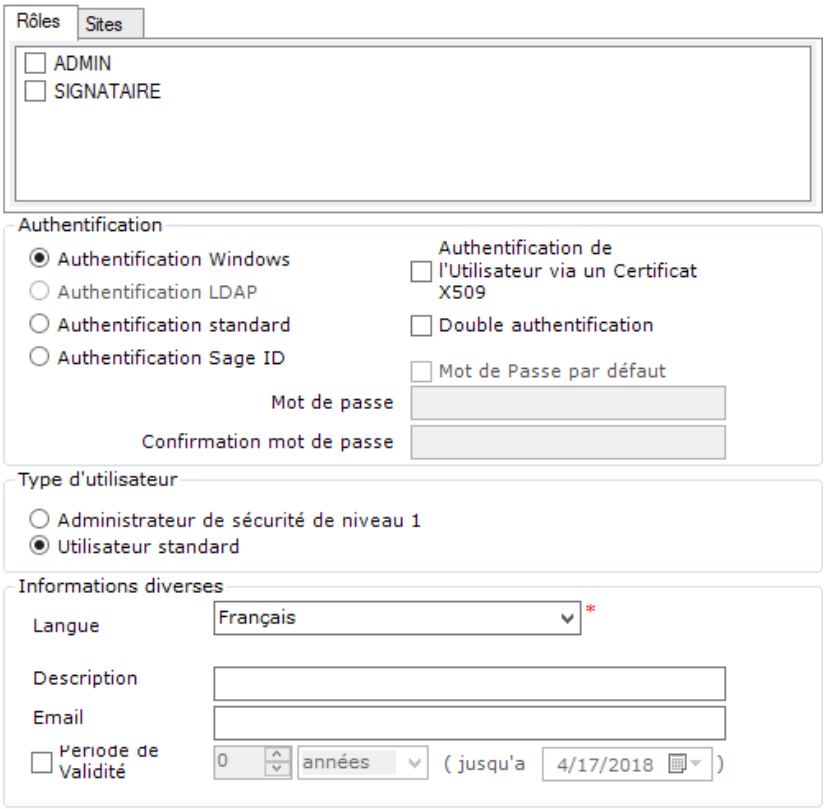
Grâce à la console d’administration **Sage XRT Common Services**, vous définissez le mode de fonctionnement de la gestion des droits d’accès des utilisateurs aux applications **Sage XRT**.

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



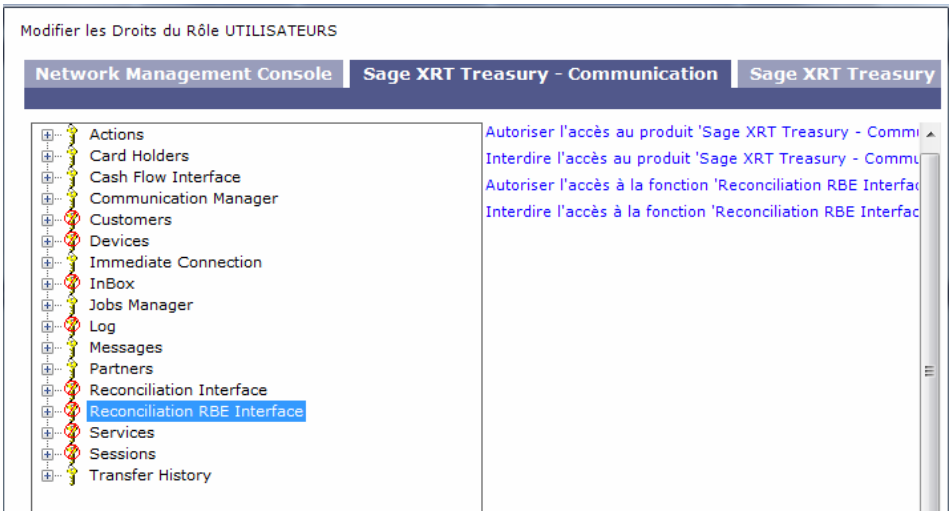
Suivant le type d'authentification utilisé par l'administrateur de base de données (*DBA*) pour se connecter au serveur de bases de données, plusieurs options sont disponibles :

- **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.

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.



©Sage 2018

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

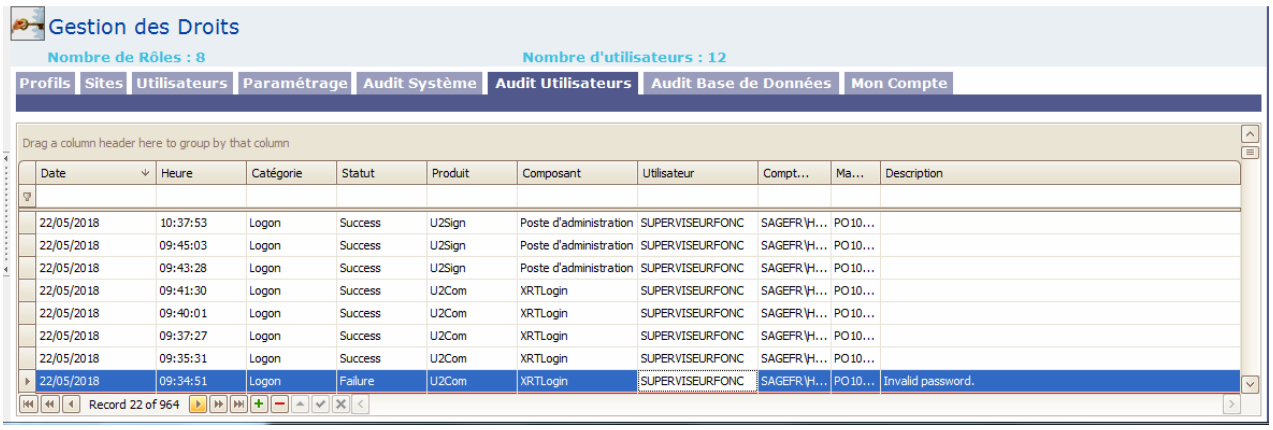
Outre les diverses fonctionnalités qu'elle propose, la gestion des identités et des accès doit apporter la preuve de son bon fonctionnement.

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 :

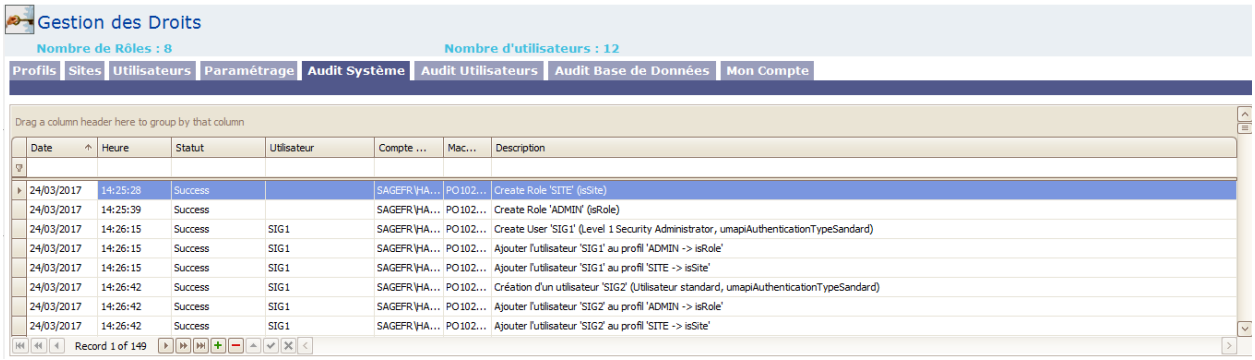
- Activité des administrateurs
  - création d'un utilisateur
  - suppression d'un utilisateur
  - changement du mot de passe d'un utilisateur
  - changement de la stratégie de gestion des mots de passe
  - changement de la configuration de l'accès à l'annuaire LDAP
  - accès accordé à une fonction ou 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 (logoff)
  - 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.



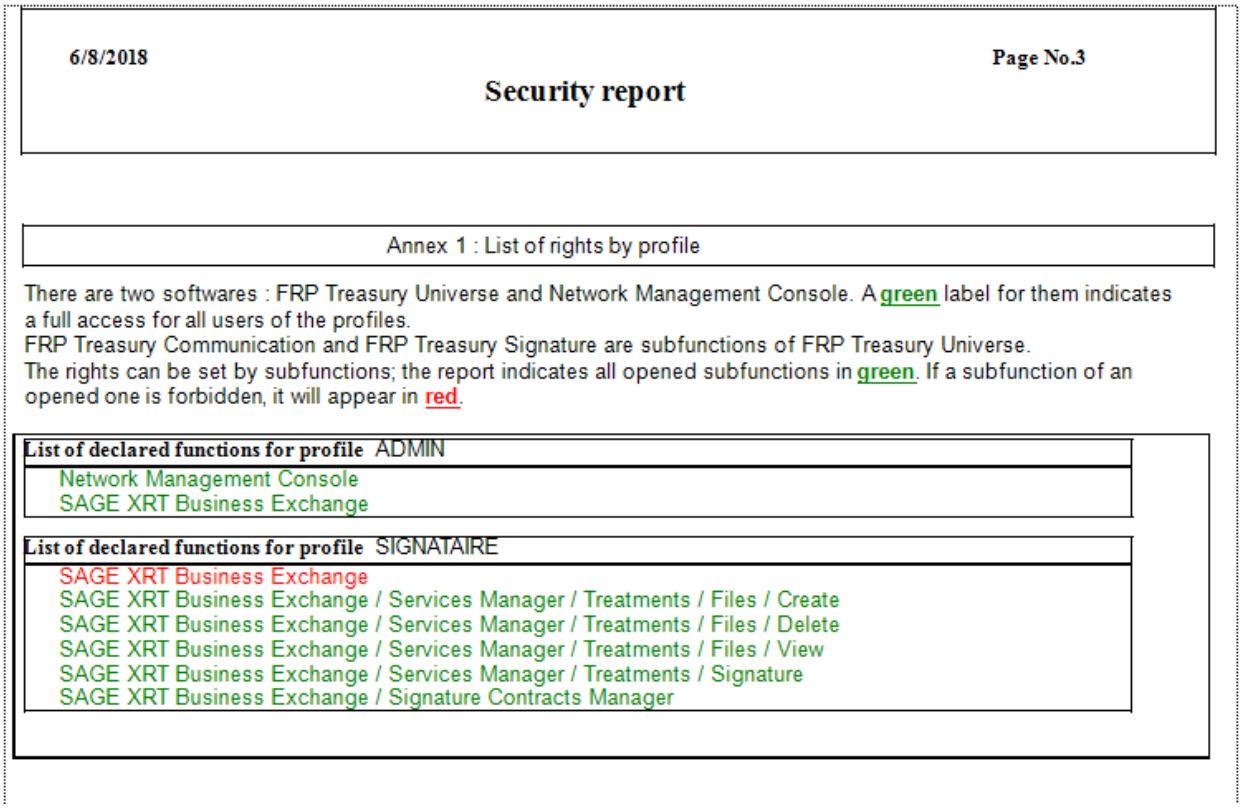
©Sage 2018

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



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 plateforme.



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.

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

©Sage 2018

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*.

Point de sécurité	Sage XRT Communication & Signature (poste lourd)	Sage XRT Communication & Signature (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	✔ Dans le cadre d'une sécurité NT totale, le mot de passe utilisé est celui de Windows paramétrable ✔ Dans le cadre de la sécurité standard XRT, le mot de passe applicatif n'est pas enregistré.	✔
Le mot de passe est verrouillé après 3 saisies de mot de passe incorrects. Il est réactivé au bout de 10 minutes	✔ paramétrable	✔ paramétrable

©Sage 2018

Sécurité des données

Point de sécurité	Sage XRT Communication & Signature (poste lourd)	Sage XRT Communication & Signature (module web)
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 modifiés depuis 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

©Sage 2018

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'utilisateur	Données client	Identification de l'utilisateur
Nom de l'utilisateur	Données client	Identification de l'utilisateur -signataire
Prénom de l'utilisateur	Données client	Identification de l'utilisateur -signataire
Email de l'utilisateur	Données client	Identification de l'utilisateur -signataire
Certificats de l'utilisateur	Données client	Identification du signataire
Nom contact partenaire financier	Données client	Contact banque
Nom du Tiers bénéficiaire	Données Etat Civil	Paiement fournisseurs, salaires
Prénom du Tiers bénéficiaire	Données Etat Civil	Paiement fournisseurs, salaires
Adresse du Tiers bénéficiaire	Données Etat Civil	Paiement fournisseurs, salaires
Code pays du Tiers bénéficiaire	Données client	Paiement fournisseurs, salaires
Téléphone du Tiers bénéficiaire	Données client	Paiement fournisseurs, salaires
Email du Tiers bénéficiaire	Données client	Paiement fournisseurs, salaires
Fax du Tiers bénéficiaire	Données client	Paiement fournisseurs, salaires
Nom banque du tiers bénéficiaire	Données bancaires	Paiement fournisseurs, salaires

©Sage 2018

Données personnelles et traitements associés

Données à caractère personnel	Catégorie	Finalité
BIC banque du tiers bénéficiaire	Données bancaires	Paiement fournisseurs, salaires
IBAN – Identification du compte du Tiers bénéficiaire	Données bancaires	Paiement fournisseurs, salaires
IBAN – Identification du compte de frais du Tiers bénéficiaire	Données bancaires	Paiement fournisseurs, salaires
Nom du débiteur	Données Etat Civil	Prélèvements clients
Prénom du débiteur	Données Etat Civil	Prélèvements clients
IBAN du débiteur	Données bancaires	Prélèvements clients
Devise du compte du débiteur	Données bancaires	Prélèvements clients
BIC de la banque du débiteur	Données bancaires	Prélèvements clients
Référence unique du mandat	Données contrat	Prélèvements clients

Gestion des utilisateurs

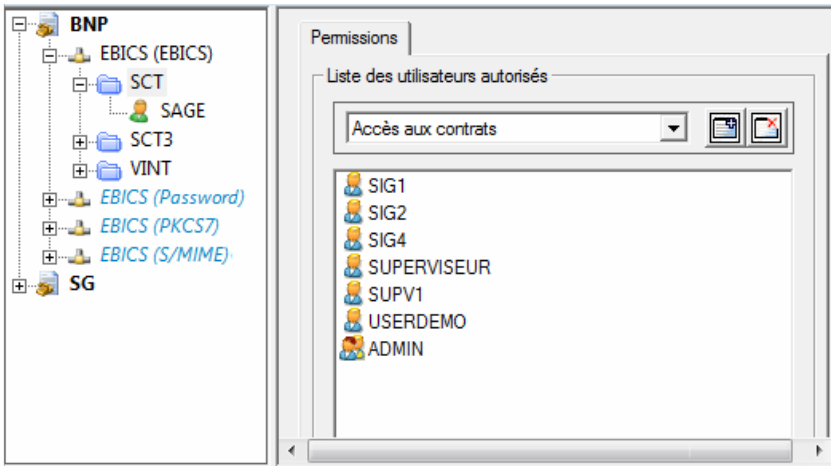
Les utilisateurs de l'application **Sage XRT Communication & Signature** sont créés par un administrateur habilité (cf. § *Définition d'une politique de sécurité via Sage XRT Common Services*).

©Sage 2018

Options de sécurité par contrat bancaire

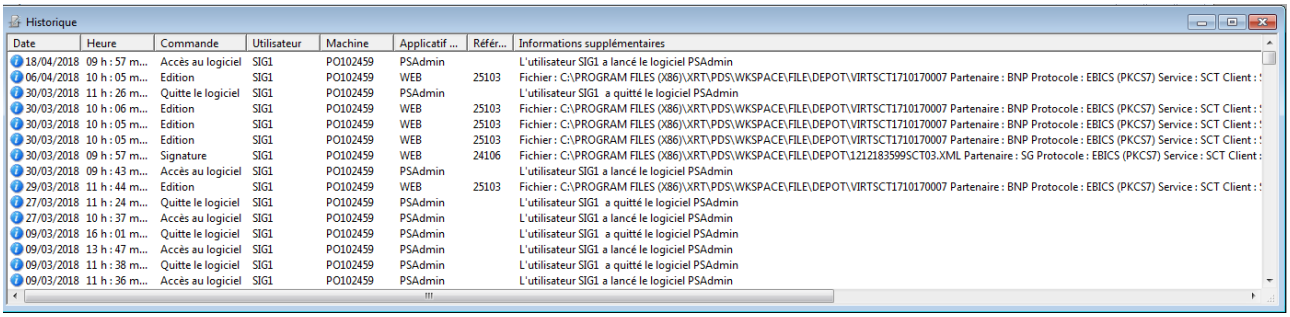
Paramétrage

Les droits d'accès, d'édition, d'extraction et de suppression des utilisateurs sont paramétrés au niveau des contrats de communication pour la signature.



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*).



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).

©Sage 2018

Gestion : création-modification-suppression

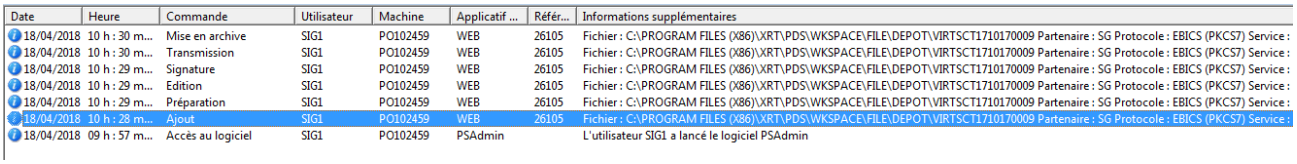
La création des signataires par un administrateur habilité est possible si :

- L'utilisateur est créé dans la console d'administration **Sage XRT Common Services** (cf. § *Fonctionnalités d'Audit sur la gestion des identités et des accès*).
- Le signataire est créé dans l'application **Sage XRT Communication & Signature**.

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

Reporting sur la base

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



Date	Heure	Commande	Utilisateur	Machine	Applicatif ...	Référ...	Informations supplémentaires
18/04/2018	10 h : 30 m...	Mise en archive	SIG1	PO102459	WEB	26105	Fichier : C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VIRTSCT1710170009 Partenaire : SG Protocole : EBICS (PKCS7) Service :
18/04/2018	10 h : 30 m...	Transmission	SIG1	PO102459	WEB	26105	Fichier : C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VIRTSCT1710170009 Partenaire : SG Protocole : EBICS (PKCS7) Service :
18/04/2018	10 h : 29 m...	Signature	SIG1	PO102459	WEB	26105	Fichier : C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VIRTSCT1710170009 Partenaire : SG Protocole : EBICS (PKCS7) Service :
18/04/2018	10 h : 29 m...	Edition	SIG1	PO102459	WEB	26105	Fichier : C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VIRTSCT1710170009 Partenaire : SG Protocole : EBICS (PKCS7) Service :
18/04/2018	10 h : 29 m...	Préparation	SIG1	PO102459	WEB	26105	Fichier : C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VIRTSCT1710170009 Partenaire : SG Protocole : EBICS (PKCS7) Service :
18/04/2018	10 h : 28 m...	Ajout	SIG1	PO102459	WEB	26105	Fichier : C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VIRTSCT1710170009 Partenaire : SG Protocole : EBICS (PKCS7) Service :
18/04/2018	09 h : 57 m...	Accès au logiciel	SIG1	PO102459	PSAdmin		L'utilisateur SIG1 a lancé le logiciel PSAdmin

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

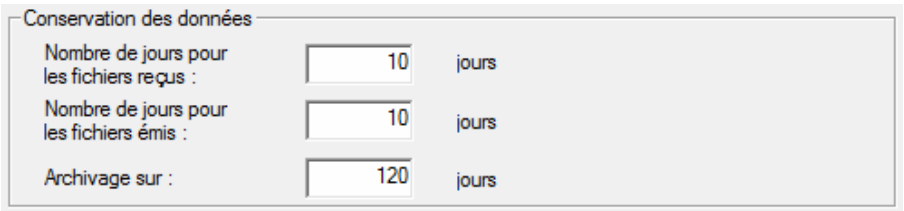
Vous avez la possibilité de modifier ou de supprimer toute donnée personnelle dans votre application pour répondre à la demande d'une personne physique.

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.

Paramétrage de conservation des fichiers contenant des données personnelles en signature :

Paramétrage de conservation des fichiers contenant des données personnelles en communication :



©Sage 2018

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

©Sage 2018

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.

©Sage 2018

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.

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'entrainent 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

Le code de votre application est signé. Cette signature certifie que le programme est légitime et conforme au développement initial.

Authentifications

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.

©Sage 2018

Autorisations

Un utilisateur à accès à un ou plusieurs contrats bancaires. Il est associé à un profil qui détermine ses droits d'accès aux fonctions de l'application et ses privilèges (accès, création, modification, suppression).

Il est possible sur chaque contrat bancaire de paramétrer des autorisations spécifiques pour 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.

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.

©Sage 2018

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 règlementation 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.

©Sage 2018