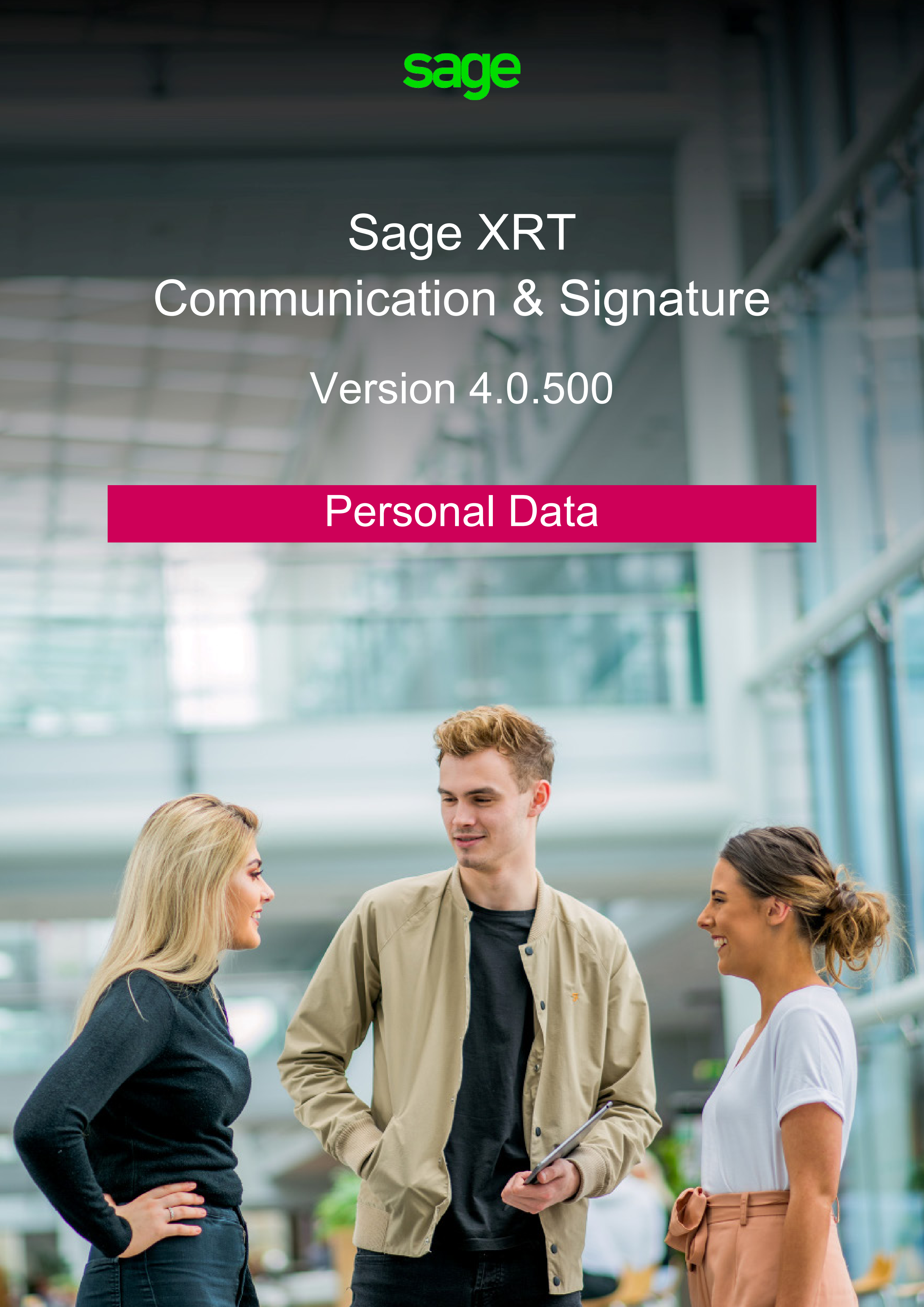
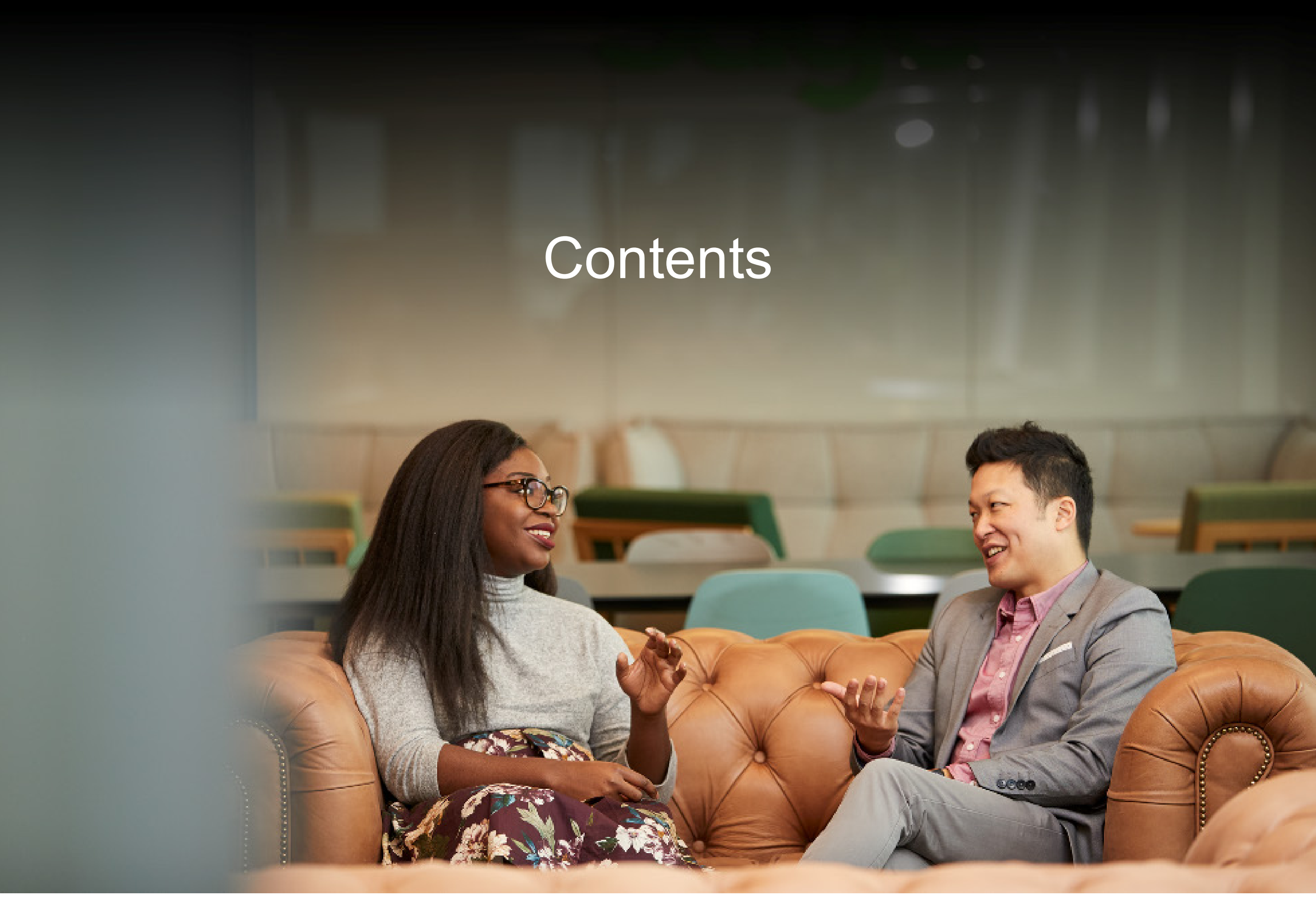
Sage XRT Communication & Signature

Version 4.0.500

Personal Data





Contents

Purpose

The general data protection regulation (GDPR) applies in all EU Member States from 25 May 2018.

This document aims at identifying the existing functions from **Sage XRT Communication & Signature** that could help your company to comply with this European regulation.

European Basic Requirements

Basic Requirements for Personal Data Protection	**Sage XRT Communication & Signature**
Ensuring appropriate security	
The company must install appropriate technical and organizational safeguards that ensure the security of the personal data such as the securing of work stations and storage spaces, as well as confidentiality policies and clauses.	
Stronger Passwords and Protection of certain stored or exchanged data See the existing functions for security	✓
Managing individuals rights: data portability, right of erasure, right of objection to the processing/consent, right of rectification, etc.	
It must provide functions to correct and import/export personal data, as well as functions to select the individuals subject to processing of their data.	
Modification/Deletion functions available in every product, according to the user rights See the existing functions for personal data	✓
Helping demonstrate compliance	
The company must keep records of all the documents that demonstrate the actions set up to comply with the general data protection regulation - they could be presented in case of inspection, such as: documents describing the technical and organizational safeguards that it has installed to ensure the security of personal data use, the processing registry.	
Sage makes available records of all personal data and associated processing activities for **Sage XRT Communication & Signature**. See the list of personal data and associated processing activities	✓

Data Security

Database Access

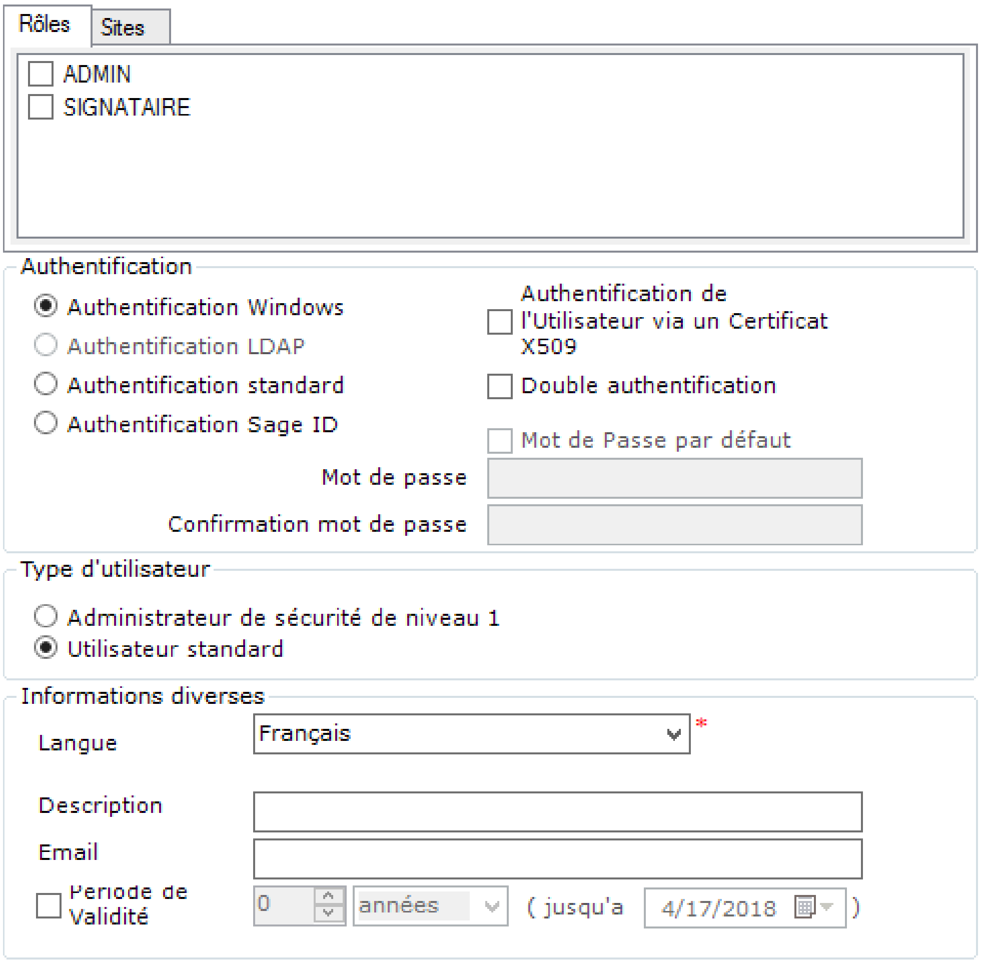
Sage XRT Common Services Administration Console enables you to define the management of user access rights for **Sage XRT** applications.

Access Rights Management

Two modes to grant access rights are available:

- Select **Access permissions are granted by a security administrator**, if you want a simple access permissions management in which only one Security Administrator intervenes.
- Select **Access permissions are granted by a level 1 security administrator and validated by a level 2 security administrator**, if you want every action taken by Security Administrator to be validated by a second one.

Selection of Authentication Strategy



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

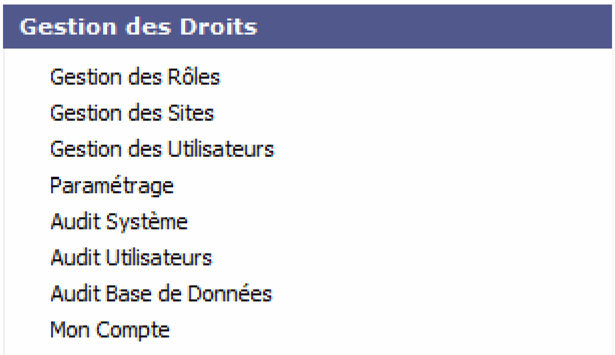
Informations diverses

Langue: Français *
Description:
Email:
☐ Période de Validité: 0 années (jusqu'à 4/17/2018)

According to the authentication type used by the Database Administrator (*DBA*) to connect to the database server, you can select:

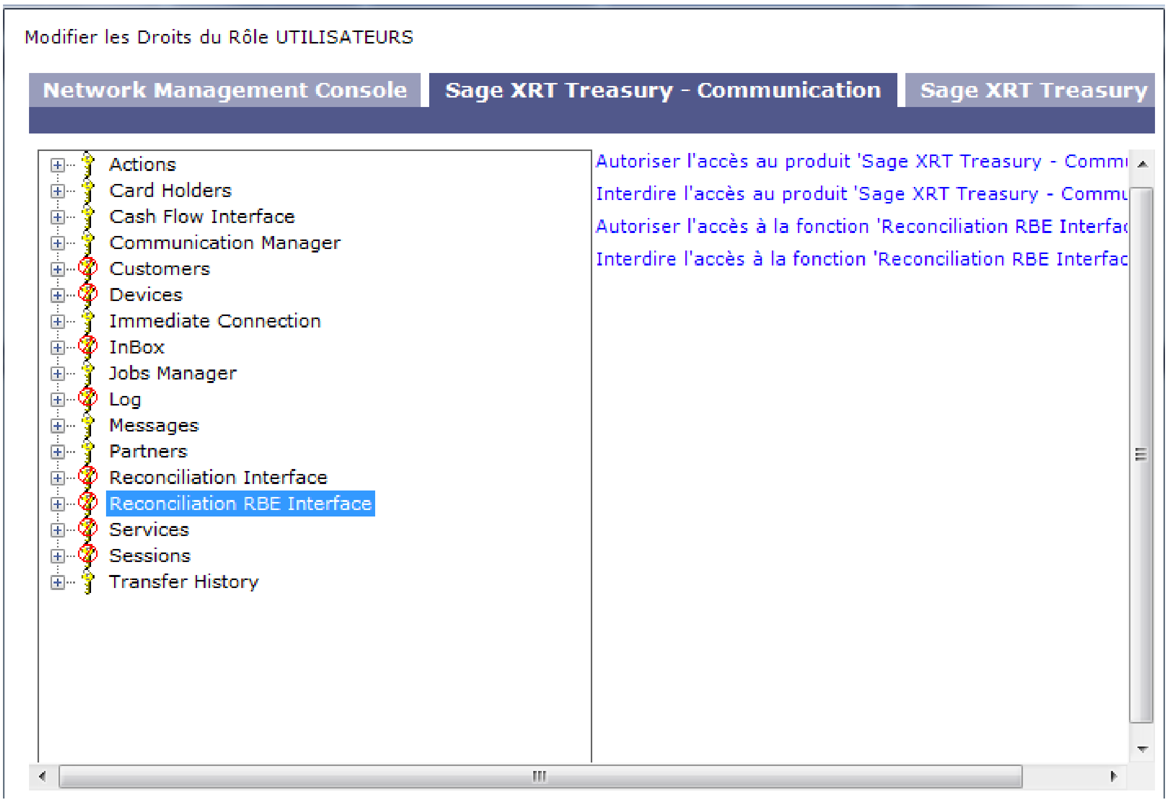
- **Use Windows NT integrated security**: the DBA is authenticated by its NT account, we recommend this authentication level.
- **Use a specific username and password**: the DBA is authenticated by a username and a password.
- **Authentication via X509 Certificate**: for the web client, the strong authentication consists of two phases.
  - Check of the certificate by searching the company's **Active Directory**
  - Challenge/Answer between the client and the authentication component to check client identity
- **Double Authentication**: a second factor is used for user authentication to generate a single-use password.

Definition of Security Policy through SXCS



Management of Profiles, Roles and Users

Profiles enable the creation of user and administrator roles to define access permissions.



Modifier les Droits du Rôle UTILISATEURS

Autoriser l'accès au produit 'Sage XRT Treasury - Commu
Interdire l'accès au produit 'Sage XRT Treasury - Commu
Autoriser l'accès à la fonction 'Reconciliation RBE Interfac
Interdire l'accès à la fonction 'Reconciliation RBE Interfac

Audit Functions for Access and Identities

On top of providing the obvious functions, the identity and access management must prove its efficiency.

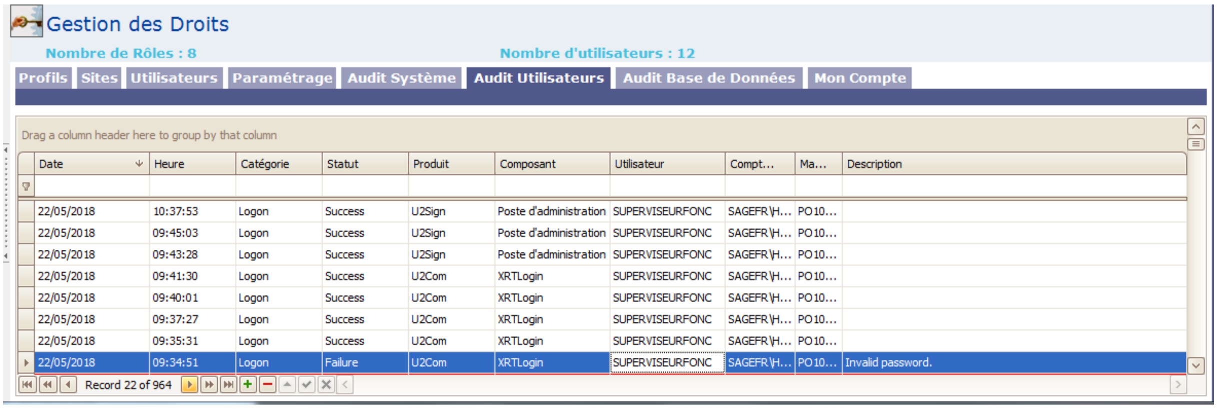
The evidence must be remitted to auditors upon request and in written to be archived.

The proof must cover the frequently audited areas, i.e.:

- Administrator Actions
  - Create User
  - Delete User
  - Change User Password
  - Change management strategy of passwords
  - Change access configuration to LDAP directory
  - Access granted
  - Access denied
- Final User Actions

  - Login
  - Logoff
  - Specific messages from the application
- Tests for compliance with security policy
  - User account locked after **n** failed tries log on

The **Users Audit** table describes all actions executed by the users.



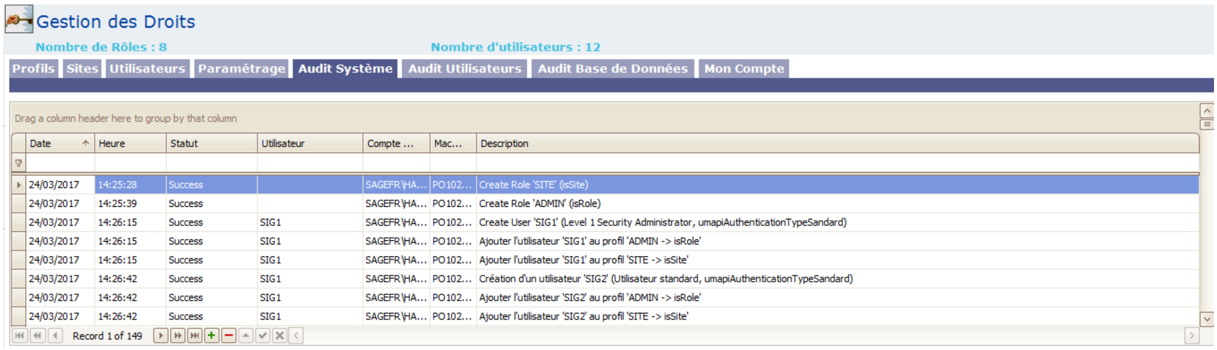
Gestion des Droits

Nombre de Rôles : 8 Nombre d'utilisateurs : 12

Date	Heure	Catégorie	Statut	Produit	Composant	Utilisateur	Compt...	Ma...	Description
22/05/2018	10:37:53	Logon	Success	U2Sign	Poste d'administration	SUPERVISEURFONC	SAGEFR\H...	PO10...	
22/05/2018	09:45:03	Logon	Success	U2Sign	Poste d'administration	SUPERVISEURFONC	SAGEFR\H...	PO10...	
22/05/2018	09:43:28	Logon	Success	U2Sign	Poste d'administration	SUPERVISEURFONC	SAGEFR\H...	PO10...	
22/05/2018	09:41:30	Logon	Success	U2Com	XRTLogin	SUPERVISEURFONC	SAGEFR\H...	PO10...	
22/05/2018	09:40:01	Logon	Success	U2Com	XRTLogin	SUPERVISEURFONC	SAGEFR\H...	PO10...	
22/05/2018	09:37:27	Logon	Success	U2Com	XRTLogin	SUPERVISEURFONC	SAGEFR\H...	PO10...	
22/05/2018	09:35:31	Logon	Success	U2Com	XRTLogin	SUPERVISEURFONC	SAGEFR\H...	PO10...	
22/05/2018	09:34:51	Logon	Failure	U2Com	XRTLogin	SUPERVISEURFONC	SAGEFR\H...	PO10...	Invalid password.

Record 22 of 964

The System Audit table describes all actions executed at time *t*.



Gestion des Droits

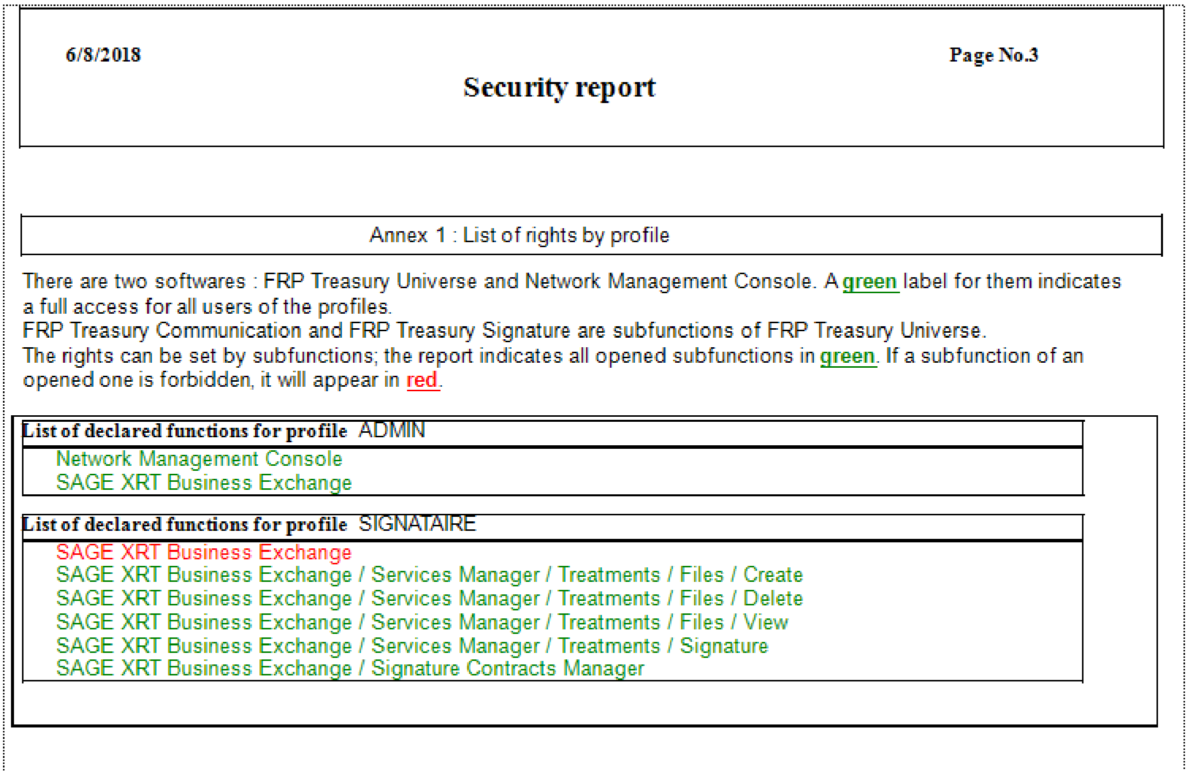
Nombre de Rôles : 8 Nombre d'utilisateurs : 12

Date	Heure	Statut	Utilisateur	Compte ...	Mac...	Description
24/03/2017	14:25:28	Success		SAGEFR\HA...	PO102...	Create Role 'SITE' (isSite)
24/03/2017	14:25:39	Success		SAGEFR\HA...	PO102...	Create Role 'ADMIN' (isRole)
24/03/2017	14:26:15	Success	SIG1	SAGEFR\HA...	PO102...	Create User 'SIG1' (Level 1 Security Administrator, umapiAuthenticationTypeSandard)
24/03/2017	14:26:15	Success	SIG1	SAGEFR\HA...	PO102...	Ajouter l'utilisateur 'SIG1' au profil 'ADMIN -> isRole'
24/03/2017	14:26:15	Success	SIG1	SAGEFR\HA...	PO102...	Ajouter l'utilisateur 'SIG1' au profil 'SITE -> isSite'
24/03/2017	14:26:42	Success	SIG1	SAGEFR\HA...	PO102...	Création d'un utilisateur 'SIG2' (Utilisateur standard, umapiAuthenticationTypeSandard)
24/03/2017	14:26:42	Success	SIG1	SAGEFR\HA...	PO102...	Ajouter l'utilisateur 'SIG2' au profil 'ADMIN -> isRole'
24/03/2017	14:26:42	Success	SIG1	SAGEFR\HA...	PO102...	Ajouter l'utilisateur 'SIG2' au profil 'SITE -> isSite'

Record 1 of 149

Security Reporting

Sage XRT Common Services Administration Console enables you to edit reports listing the authorized/denied functions for each profile and each product from the platform.



6/8/2018 **Security report** Page No.3

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

Compliance with Sarbanes Oxley Act

The *Sarbanes Oxley Act* imposes security rules to get access to operating systems and applications.

Here is the list of the Security Issues for access and use of **Sage XRT** applications and for a standard user.

Sage XRT password policy complies with the requirement of the *Sarbanes Oxley Act*.

Security Issues	Sage XRT Communication & Signature (rich client)	Sage XRT Communication & Signature (web module
The application manages profiles.	✓	✓
Passwords are mandatory.	✓	✓

Data Security

Security Issues	Sage XRT Communication & Signature (rich client)	Sage XRT Communication & Signature (web module
A standard password is given to everyone or to a group upon account creation.	✓	✓
The password must be changed upon first connection.	✓ Customizable	✓ Customizable
Passwords must contain at least 6 characters, among which 1 uppercase letter and 1 digit.	✓ Customizable	✓ Customizable
Passwords must be changed every 42 Days.	✓ Customizable	✓ Customizable
The application keeps the passwords history. The four last passwords cannot be used.	✓ Customizable	✓ Customizable
Passwords are not kept to avoid new entry in later connections.	✓ For a complete NT security, the passwords used are the Windows passwords. Customizable ✓ For XRT standard security, the application password is not stored.	✓
The password is locked after 3 unsuccessful entries. It is automatically reactivated after 10 minutes.	✓ Customizable	✓ Customizable
The account is not locked if not used for several days.	✓	✓
The session is locked after 10-minute inactivity.	✗	✓ Customizable
Security rules cannot be modified from user work station.	✓	✓
Every access to application must be logged.	✓	✓
For short-term contract users, the specification of an end	✓ Customizable	✓ Customizable

Security Issues	Sage XRT Communication & Signature (rich client)	Sage XRT Communication & Signature (web module
date of validity is mandatory corresponding to the end date of contract.		

Personal Data and Associated Processing

Personal Data List

Personal Data are used in order:

- To identify users, control access and authorizations in the application
- To check, validate and sign electronically during bank exchanges
- To retrieve bank data files

Financial data of third parties enable the execution of payment orders arising from the contract between the parties.

Personal Data	Category	Purpose
User Alias	Client Data	User ID
User Name	Client Data	User/Signatory ID
User First Name	Client Data	User/Signatory ID
User E-mail	Client Data	User/Signatory ID
User Certificates	Client Data	Signatory ID
Financial Partner Contact	Client Data	Bank Contact
Beneficiary Third Party Name	Marital Status	Salaries, Providers Payments
Beneficiary Third Party First Name	Marital Status	Salaries, Providers Payments
Beneficiary Third Party Address	Marital Status	Salaries, Providers Payments
Beneficiary Third Party Country Code	Client Data	Salaries, Providers Payments
Beneficiary Third Party Phone	Client Data	Salaries, Providers Payments
Beneficiary Third Party E-mail	Client Data	Salaries, Providers Payments
Beneficiary Third Party FAX	Client Data	Salaries, Providers Payments
Beneficiary Third Party Bank Name	Bank Data	Salaries, Providers Payments

Personal Data	Category	Purpose
Beneficiary Third Party BIC	Bank Data	Salaries, Providers Payments
Beneficiary Third Party IBAN - Account ID	Bank Data	Salaries, Providers Payments
IBAN - Disbursement Account of Beneficiary Third Party	Bank Data	Salaries, Providers Payments
Debtor Name	Marital Status	Client Drawings
Debtor First Name	Marital Status	Client Drawings
Debtor IBAN	Bank Data	Client Drawings
Debtor Account Currency	Bank Data	Client Drawings
Debtor Bank BIC	Bank Data	Client Drawings
Unique Mandate Reference	Contract Data	Client Drawings

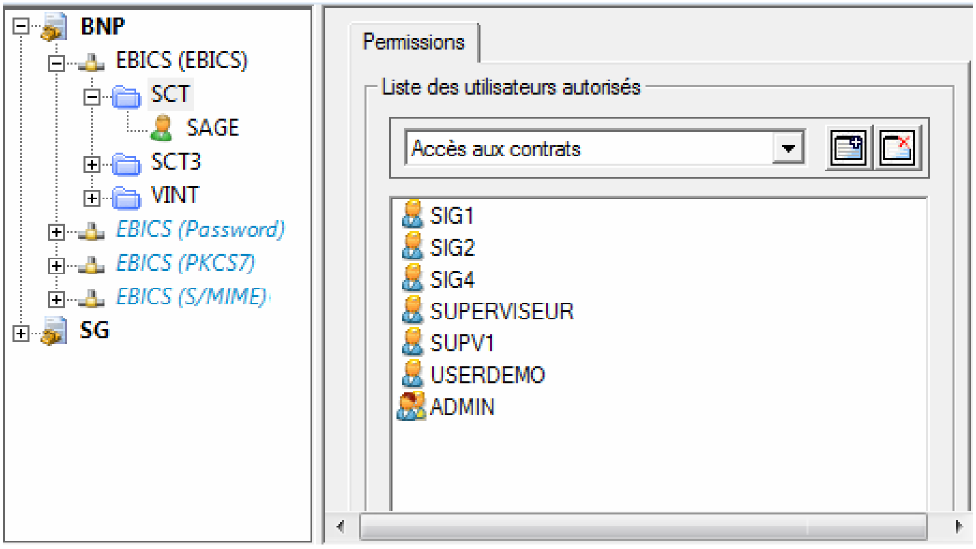
User Management

Sage XRT Communication & Signature users are created by an administrator with authorizations on each entity, based on the users created in the Administration Console (see § *Definition of Security Policy through SXCS*).

Security Options by Bank Contract

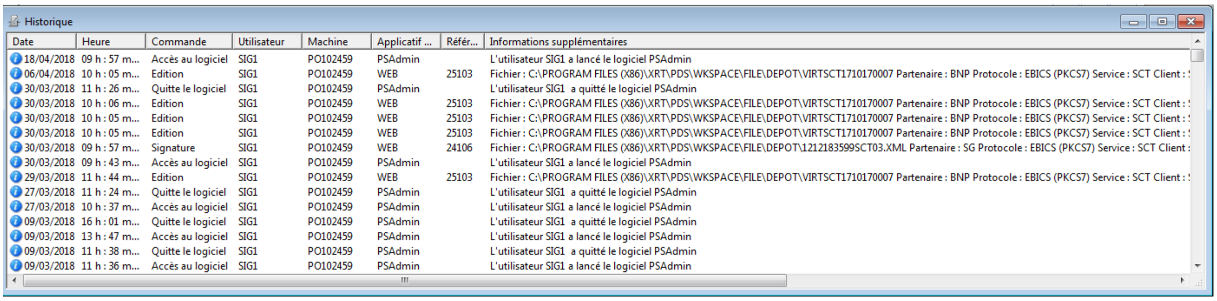
Setup

The access, edition, extraction and deletion rights are set up in the communication contracts for Signature.



Reporting

Every action is registered by user in the audit ledgers for **Online Banking** site (creation-modification-suspension) or in the administration audit (see § *Audit Functions for Access and Identities*).



Historique

Date	Heure	Commande	Utilisateur	Machine	Applicatif ...	Référ...	Informations supplémentaires
18/04/2018	09 h : 57 m...	Accès au logiciel	SIG1	PO102459	PSAdmin		L'utilisateur SIG1 a lancé le logiciel PSAdmin
06/04/2018	10 h : 05 m...	Edition	SIG1	PO102459	WEB	25103	Fichier : C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VIRTSCT1710170007 Partenaire : BNP Protocole : EBICS (PKCS7) Service : SCT Client :
30/03/2018	11 h : 26 m...	Quitte le logiciel	SIG1	PO102459	PSAdmin		L'utilisateur SIG1 a quitté le logiciel PSAdmin
30/03/2018	10 h : 06 m...	Edition	SIG1	PO102459	WEB	25103	Fichier : C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VIRTSCT1710170007 Partenaire : BNP Protocole : EBICS (PKCS7) Service : SCT Client :
30/03/2018	10 h : 05 m...	Edition	SIG1	PO102459	WEB	25103	Fichier : C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VIRTSCT1710170007 Partenaire : BNP Protocole : EBICS (PKCS7) Service : SCT Client :
30/03/2018	10 h : 05 m...	Edition	SIG1	PO102459	WEB	25103	Fichier : C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VIRTSCT1710170007 Partenaire : BNP Protocole : EBICS (PKCS7) Service : SCT Client :
30/03/2018	09 h : 57 m...	Signature	SIG1	PO102459	WEB	24106	Fichier : C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\1212183599SCT03.XML Partenaire : SG Protocole : EBICS (PKCS7) Service : SCT Client :
30/03/2018	09 h : 43 m...	Accès au logiciel	SIG1	PO102459	PSAdmin		L'utilisateur SIG1 a lancé le logiciel PSAdmin
29/03/2018	11 h : 44 m...	Edition	SIG1	PO102459	WEB	25103	Fichier : C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VIRTSCT1710170007 Partenaire : BNP Protocole : EBICS (PKCS7) Service : SCT Client :
27/03/2018	11 h : 24 m...	Quitte le logiciel	SIG1	PO102459	PSAdmin		L'utilisateur SIG1 a quitté le logiciel PSAdmin
27/03/2018	10 h : 37 m...	Accès au logiciel	SIG1	PO102459	PSAdmin		L'utilisateur SIG1 a lancé le logiciel PSAdmin
09/03/2018	16 h : 01 m...	Quitte le logiciel	SIG1	PO102459	PSAdmin		L'utilisateur SIG1 a quitté le logiciel PSAdmin
09/03/2018	13 h : 47 m...	Accès au logiciel	SIG1	PO102459	PSAdmin		L'utilisateur SIG1 a lancé le logiciel PSAdmin
09/03/2018	11 h : 38 m...	Quitte le logiciel	SIG1	PO102459	PSAdmin		L'utilisateur SIG1 a quitté le logiciel PSAdmin
09/03/2018	11 h : 36 m...	Accès au logiciel	SIG1	PO102459	PSAdmin		L'utilisateur SIG1 a lancé le logiciel PSAdmin

Signatories

Purpose of Data Processing

Signatories check, validate and sign electronically the financial data exchanges between a company and its banking partner.

These digital data flows consist of payment orders arising from the contract between two parties (salaries, providers invoices, bank direct debits).

Management: creation-modification-deletion

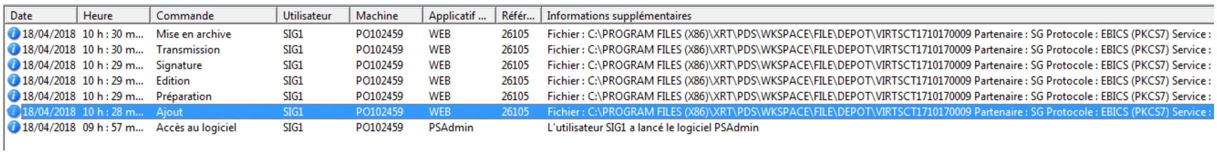
An authorized administrator can create signatories only if:

- The signatory is a user created in **Sage XRT Common Services** Administration Console (see § *Audit Functions for Access and Identities*).
- The signatory is a user created in **Sage XRT Communication & Signature**.

Authorized users can modify and delete signatories.

Database Report

Every signatories' action is registered in the event log for the transaction service.



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

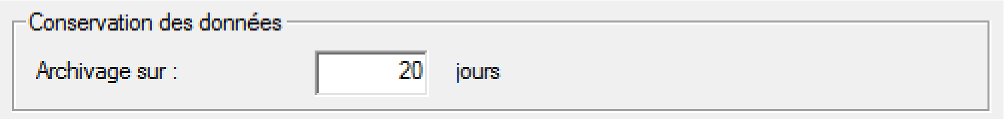
Rights of Rectification and Erasure - Retention Period

You can modify and delete any personal data from your application to deal with an individual's request.

However, the applications process must be respected to complete modifications and erasures.

Important! All the local rules specify data retention periods.

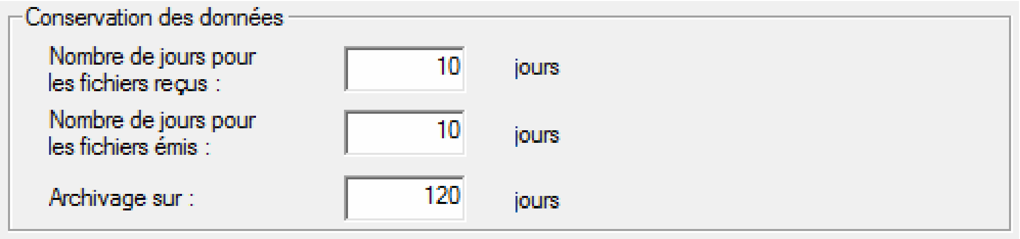
Setup of file retention periods for Signature personal data



Conservation des données

Archivage sur : 20 jours

Setup of file retention periods for Communication personal data



Conservation des données

Nombre de jours pour les fichiers reçus : 10 jours

Nombre de jours pour les fichiers émis : 10 jours

Archivage sur : 120 jours

Additional Security Measures

To minimize regulation infringement and potential sanctions, some basic principles should be applied.

Even though the system and network security remains your responsibility, the solution platform offers you some tools:

- Standard web browsers and *http* or https protocol are used. Web technology guarantees a first layer of isolation between the web server and the workstation.
- Passwords are not transferred onto the network. Authentication system is based on standards. It may be a *Windows* connection checked through the LDAP (Lightweight Directory Access Protocol) or an authentication through certificate.
  For simplicity reasons, you can use a method based on users and encrypted passwords stored on the application web server. You may also double the authentication.
- Rights are managed at Entities‘ level. They depend on the profile associated with the user.
  Access to contracts can also be granted or restricted from the services of each entity.

General Measures

Using https

The application is a web application accessible through an *http* or *https* connection. Although *http* is available, we recommend you use *https* for production instances, especially if your application is available from the internet.

Strengthening Passwords

If you use this authentication mode, do not forget to adopt a Password Management Policy that imposes strong passwords.

Strong passwords must:

- have at least six characters (the more characters, the stronger the password).
- use a combination of lowercase letters, uppercase letters, numbers, and symbols such as @ # $%!? &, etc.
- cannot contain the keyboard's own letter combinations such as *qwerty*.
- cannot contain the DBO.
- must not be used for other applications.

Securing Servers through Access Rights

The servers that host the application components contain sensitive setup files and data which remain vulnerable to internal threats.

Additional Security Measures

The administrators must be the only users authorized to connect to the servers.

Make sure you granted them with the rights specific to the application administration on the relevant directories.

Important! The server administrators must be different from the application administrators.

Protecting Servers

The application servers must be based on the industry best practices.

Using Local Firewalls

Use local firewalls on your servers to lock all IP ports that are not required for the application operation nor for the user access.

Usually, when all the application components are installed on the same server, the application requires only *http* or *https* ports for its operation.

For multi-server installations, you must open the ports (or range of ports) required for the communication between components.

Securing Internet Architecture

Your architecture is the key to your security, especially if your application is available from the internet.

To connect your systems and make them available on the internet, you must answer the following questions:

- Which servers and ports must be seen from the outside?
- How the external requests are blocked, translated and redirected to these servers and ports?

This involves equipments such as:

- A firewall between your private network and the internet to block and redirect external requests to the relevant servers of your network.
- A demilitarized zone which is a physical or logical subnetwork that isolates your private network form the internet.

The firewall is the guardian of your **DMZ** *checkpoints*.

Note: These recommendations are relevant only if your application is visible on the internet. You do not need to set up any **DMZ**, , nor firewall if you use your own private network.

Encrypting Data in Transit

You can use the **Transparent Layer Security** standard for the communication between your application layer and your database.

Additional Security Measures

The **ForceEncryption** option in **SQL Server** forces the protocol encryption which guarantees the data privacy.

File System Security

The security of the file system for the servers must be implemented with the corresponding tools (antivirus, network access security, etc.).

Make sure these tools do not cause performance issues.

For example, avoid running a continuous antivirus scan on a database server.

Application Measures

Application Signature

The code of your application has been signed. This signature certify that the program is legit and corresponds to the initial development.

Authentication

The application provides several authentication modes:

- **Use Windows NT integrated security**: the user is authenticated by its NT account, we recommend this mode.
- **Use a specific username and password**: the user is authenticated by a username and a password.
- **Authentication via X509 Certificate**: for the web client, the strong authentication consists of two phases.
  - Check of the certificate by searching the company's **Active Directory**
  - Challenge/Answer between the client and the authentication component to check client identity
- **Double authentication**: a second factor is used for user authentication to generate a single-use password.

Authorizations

A single user has access to one or more Bank Contracts. Each user is associated with a profile that defines their access rights and privileges (access, creation, modification, deletion).

Specific authorizations can be set up for signatories on each bank contract (contract access, report access, archiving and exporting rights).

This enables you to differentiate access rights to sensitive data for each entity and user.

Important! Make sure you continue applying these rules in the future. Keep them as simple as possible while enforcing your security policy.

For Further Information

Setting up all additional Security Measures requires technical skills and feedbacks which our consulting teams can provide you with.
Do not hesitate to contact them if you want to apply these recommendations.

Disclaimer

The information on GDPR provided hereby is intended as advice of a general nature for information purposes and is not to be construed as professional nor legal advice. *Sage* cannot guarantee the provided information exactly reproduces an officially adopted text. In case of dispute, the Official Journal of the European Union prevails.

While we have made every effort to ensure that the information provided is correct and up to date, the information is delivered on an *as is* basis without any warranties, express or implied. *Sage* will not accept any liability for errors or omissions and will not be liable for any damage (including, without limitation, damage for loss of business or loss of profits) arising in contract, tort or otherwise from the use of or reliance on this information or from any action or decisions taken as a result of using Information.

Our products include functions that could help and accompany users to comply with the GDPR. However, we would like to draw your attention to the fact that the sole use of our products does not guarantee your compliance with the GDPR.

The information provided hereby is not to be construed as professional nor legal advice, if you need more advice on GDPR compliance, you should consult a suitably qualified professional.