Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
www.vd.ch – T +41 21 316 26 00

TABLE DES MATIÈRES

MANUEL PASSAVD



Date : 07.08.2012

Version : 3.4.1

INTRODUCTION **3**

1 GLOSSAIRE 4

2 ARCHITECTURE DE PASSAVD 5

3 LE PARTICIPANT 6

3.1 Domaine 7

3.2 Fonction 8

3.3 Exemples 8

4 RACCORDEMENTS À PASSAVD 9

4.1 Raccordement physique 9

4.2 Raccordement logique 9

4.3 Indépendance à l'égard de l'adressage des messages 9

5 ECHANGE DE DOCUMENTS 10

5.1 Enveloppe Passavd 10

5.2 Quittances Passavd (receipt) 10

6 UTILISATION DU CLIENT PASSAVD 11

6.1 Envoi d'un message 11

6.2 Réception d'un message 11

6.3 Réception d'une quittance 12

6.4 Interroger les registres cantonaux par Web Service 12

7 INSTALLATION DU CLIENT PASSAVD 13

7.1 Prérequis 13

7.2 Installation Assitée 13

7.2.1 Installation via l'assistant graphique 13

7.2.2 Installation en mode console 13

7.2.3 Installation sous macOS 13

7.2.4 Installation sous Windows 13

7.3 Installation manuelle 14

7.4 Mise à jour automatiques 15

7.5 Démarrage du client et installation en tant que service 15

7.6 Console Web et web services de la plateforme PassaVD 17

7.7 Suivi et configuration des logs 17

INTRODUCTION

PassaVD est une plateforme d'échange d'informations entre les communes, les entreprises et le canton de Vaud. Elle est basée sur la norme fédérale Sedex.

PassaVD a été développée principalement dans le but d'échanger des événements d'annonce entre les communes et le canton de Vaud, dans le cadre de la loi sur l'harmonisation des registres.

Par ailleurs, afin d'améliorer la qualité des registres, la plateforme permet d'accéder aux web services des registres REF-INF et RCPers.

Pour raccorder une application à PassaVD, il est nécessaire d'intégrer un logiciel fourni par le canton de Vaud : l'adaptateur PassaVD.

Ce document décrit le système PassaVD du point de vue des applications participant à l'interconnexion avec le serveur PassaVD. Il s'adresse en premier lieu aux fournisseurs de logiciels développant ce type d'applications.

Les publics cibles de ce document sont les suivants :

- Les architectes logiciels ;
- Les développeurs de logiciels,
- Les responsables de la sécurité ;
- Les équipes en charges de l'exploitation des logiciels.

Ce manuel définit les conditions de mise en œuvre applicables aux fournisseurs de logiciels souhaitant raccorder leurs applications à PassaVD.

1 GLOSSAIRE

Notion	Signification
Client Passavd	Elément de liaison entre les applications participant à l'interconnexion avec la plateforme PassaVD
Application 'cliente'	Logiciel participant à l'interconnexion avec la plateforme PassaVD
Participant ID	Identification explicite utilisée pour l'adressage des participants. Comparable à une adresse e-mail
Participant actif	Un participant qui peut envoyer et recevoir des messages
Participant inactif	Un participant ne peut ni envoyer ni recevoir des messages
Participant logique	Participant qui reçoit les messages qui lui sont adressés à travers la boîte aux lettres d'un participant physique
Participant physique	Participant qui dispose d'une boîte aux lettres

2 ARCHITECTURE DE PASSAVD

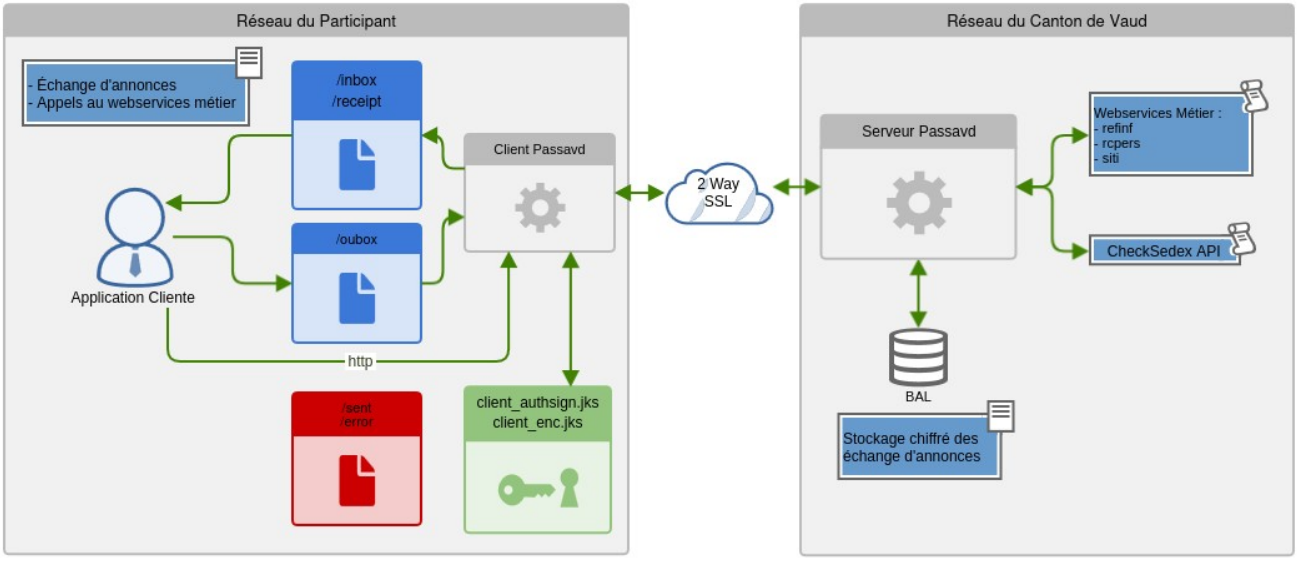
Les messages échangés via la plateforme sont composés d'une enveloppe XML contenant les informations d'adressage nécessaires au bon acheminement du message, ainsi que d'un fichier de données utiles.

Ces éléments sont déposés dans des répertoires système sur lesquels est installé l'adaptateur PassaVD. Celui-ci initie la connexion avec le serveur PassaVD afin d'effectuer les opérations d'envoi et de réception des documents.

La connexion s'effectue en HTTPS, avec une authentification mutuelle du client et du serveur. En outre, le fichier de données utiles est chiffré à l'aide du certificat public du destinataire et signé avec la clé privée de l'émetteur. L'ensemble de ces opérations est pris en charge par l'adaptateur. Ainsi, seul le destinataire du message est en mesure de lire les données qui lui sont adressées.

Les requêtes émises par l'adaptateur transitent par un reverse proxy de l'État de Vaud, lequel redirige les appels vers les systèmes appropriés en fonction du contexte d'appel.

Concernant l'accès aux registres RCPers et REF-INF via des web services, l'adaptateur expose un reverse proxy HTTP permettant d'y accéder. L'adaptateur PassaVD assure l'authentification nécessaire à la communication avec les services correspondants.



3 LE PARTICIPANT

Les participants à l'interconnexion PassaVD sont, par exemple, les services administratifs des communes, des cantons et de la Confédération. Ils sont identifiés par un identifiant unique (ID).

Cet identifiant est une chaîne de caractères comparable à une adresse de messagerie. Il est composé de trois parties :

```
<domaine>-<unité organisationnelle>-<code de fonction>
```

Le domaine permet d'identifier le type de participant : commune, canton, Confédération, etc. Il s'agit d'un chiffre compris entre 0 et 9, éventuellement précédé de la lettre T lorsqu'il s'agit d'un participant créé à des fins de test.

L'unité organisationnelle est un identifiant, le plus souvent métier. Par exemple, dans le cas d'une commune, il s'agit de son numéro OFS. Elle est composée de chiffres et de lettres majuscules.

La fonction décrit le secteur d'activité du participant. Il s'agit d'un nombre entier. La valeur 1 indique, par exemple, le secteur d'activité « Registre des habitants ».

3.1 Domaine

	Signification	Domaine de valeur pour l'unité organisationnelle
0	**Passavd** Domaine réservé pour la plateforme	Seule valeur possible : sedex
1	**Commune** Désigne une commune	Les valeurs admises sont les numéros OFS des communes politiques selon [3], par ex. 351 pour Berne
2	**Canton** Désigne un canton	Les valeurs admises sont les abréviations à deux lettres des cantons selon [3], par ex. SO pour Soleure
3	**Confédération** Désigne un office fédéral ou une application de la confédération	Unique valeur possible : CH
4	**ESB-TV** Désigne Event Bus Suisse	L'identifiant du bus partiel et l'identifiant du participant
5	**District** Désigne un district dans un canton	Les valeurs admises sont les numéros OFS des districts
6	**Institutions d'assurances sociales** Désigne une caisse de compensation AVS ou office AI	Numéro à 6 positions délivré par l'office fédéral des assurances sociales (OFAS) aux caisses de compensation/filiales AVS, aux offices AI et PC, à l'armée et aux milieux intéressés
7	**Entreprise privée** Désigne un participant de droit privé	Les valeurs admises sont attribuées par OFS aux entreprises privées participant à PassaVD. Ces numéros ne sont pas parlants. p. ex. 1 pour TI Informatique
8	**e-LP** Désigne les offices de poursuites et les créanciers membres de l'interconnexion e-LP	Les valeurs admises sont les abréviations à deux lettres des cantons, par ex. SO pour Soleure

Il est possible de distinguer des participants utilisés exclusivement à des fins de test. L'identifiant de ces participants est doté d'un préfixe « T » au niveau du domaine. De tels participants ne peuvent communiquer qu'entre eux.

3.2 Fonction

	Signification
0	PassaVD
1	Registre des habitants (RdH)
2	Informatique
3	Statistique
4	Registre du commerce
5	Administration fiscale
6	Commune bourgeoise
7	Administration militaire
8	Créancier
9	Office des poursuites

Les autres fonctions seront attribuées au fur et à mesure des besoins.

3.3 Exemples

Participant ID	Description
0-sedex-0	Désigne le système PassaVD lui-même
1-5586-1	Désigne le RdH de la commune politique de Lausanne
2-VD-2	Désigne le service cantonal de l'informatique du canton de Vaud

4 RACCORDEMENTS À PASSAVD

Il existe deux possibilités de raccorder un participant à PassaVD :

- Raccordement physique ;
- Raccordement logique.

Quel que soit le type de raccordement choisi, chaque participant possède un identifiant unique. En revanche, un participant logique ne possède pas de boîtes aux lettres.

4.1 Raccordement physique

Un participant est dit physique lorsqu'il dispose d'une boîte aux lettres. Il est alors en mesure d'interroger le serveur PassaVD afin de récupérer les nouveaux messages qui lui sont adressés, contrairement à un participant logique

4.2 Raccordement logique

Un participant est dit logique lorsqu'il reçoit les messages qui lui sont adressés via la boîte aux lettres d'un participant physique. La mise à disposition des messages entrants ainsi que la collecte des messages sortants doivent être prises en charge par le centre de calcul responsable de la gestion du participant physique.

Cette tâche est généralement assurée par un programme de type « dispatcher », développé et exploité par le centre de calcul.

Cette solution est principalement utilisée lorsque l'infrastructure informatique doit être partagée entre plusieurs participants.

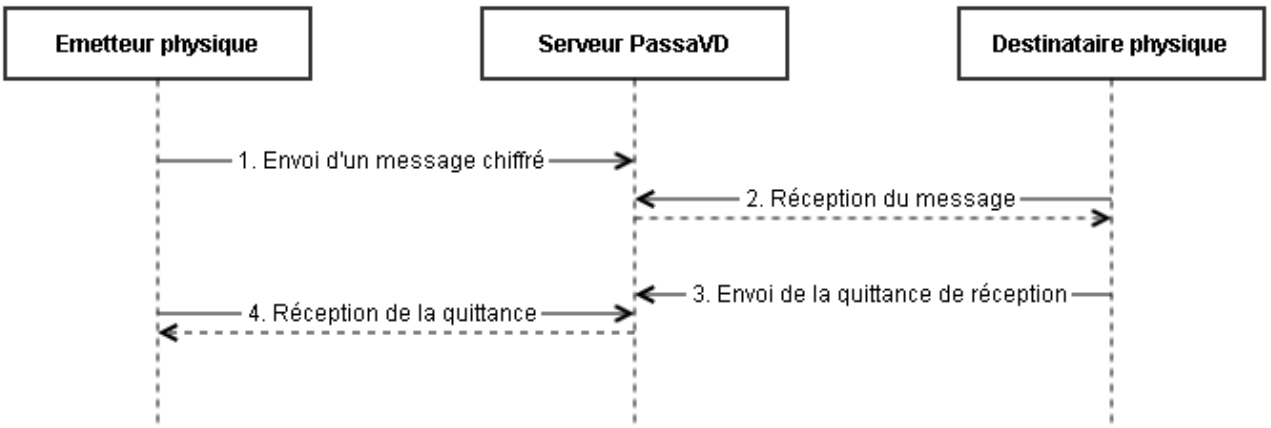
4.3 Indépendance à l'égard de l'adressage des messages

Le type de raccordement d'un participant n'a aucune incidence sur l'adressage des messages.

L'émetteur d'un message n'a pas à se préoccuper du fait que le destinataire soit un participant logique ou physique.

5 ECHANGE DE DOCUMENTS

PassaVD permet à un émetteur d'envoyer un message à un ou plusieurs destinataires et de recevoir des quittances de réception de ce document de chaque destinataire.



Un émetteur envoie un document à un destinataire. Celui-ci est déposé dans la boîte aux lettres d'un participant physique sur le serveur PassaVD. Le participant physique, via l'adaptateur du destinataire, télécharge ensuite le document et émet une quittance de réception à destination de l'émetteur.

L'émetteur reçoit ainsi une quittance confirmant que le destinataire a bien reçu le message.

5.1 Enveloppe Passavd

L'enveloppe d'un message PassaVD est un fichier XML respectant la norme eCH-0090. L'utilisation et la norme XSD eCH-0090 est décrite à l'adresse suivante :

https://docs.sedex.admin.ch/reference/sedex-envelope/

Elle est émise par un participant et permet au serveur PassaVD d'effectuer le routage.

5.2 Quittances Passavd (receipt)

La quittance d'un message PassaVD est un fichier XML respectant la norme eCH-0090. L'interprétation d'une quittance eCH-0090 est décrite à l'adresse suivante :

https://docs.sedex.admin.ch/reference/sedex-receipt/

6 UTILISATION DU CLIENT PASSAVD

L'adaptateur PassaVD est un logiciel qui fonctionne selon le même principe que l'adaptateur de la plateforme Sedex. Il est installé au sein de l'infrastructure du participant.

Il fonctionne de manière bidirectionnelle, ce qui signifie qu'il peut agir aussi bien en tant qu'émetteur qu'en tant que récepteur de messages PassaVD. Il assume notamment les tâches suivantes :

- Surveillance d'un répertoire du système de fichiers dans lequel l'application émettrice dépose les messages à envoyer ;
- Répétition automatique des tentatives d'envoi en cas de problème technique ;
- Interrogation périodique de la boîte aux lettres ;
- Téléchargement des messages depuis la boîte aux lettres, puis dépôt de ceux-ci dans le répertoire inbox du système de fichiers ;
- Mise à disposition d'un reverse proxy pour la consultation des registres RCPers et REF-INF.

Pour fonctionner, l'adaptateur PassaVD utilise plusieurs répertoires du système de fichiers :

- `outbox` : messages à envoyer ;
- `inbox` : messages reçus ;
- `sent` : messages traités ;
- `receipts` : quittances ;
- `errors` : messages n'ayant pas pu être envoyés.

L'interface exposée par l'adaptateur pour les échanges de documents repose sur un mécanisme de lecture et d'écriture de fichiers dans les répertoires outbox, inbox et receipts.

6.1 Envoi d'un message

Pour envoyer un message, le participant doit déposer, dans le répertoire outbox du système de fichiers de l'adaptateur, un fichier de données ainsi qu'une enveloppe au format ech90.

L'enveloppe doit porter le préfixe "`envl_`" et se terminer par l'extension "`.xml`".

Le fichier de données doit commencer par le préfixe "`data_`" et peut avoir une extension quelconque.

Le nom commun des fichiers, sans le préfixe ni le suffixe, constitue l'identifiant de corrélation. Celui-ci permet à l'adaptateur PassaVD d'associer correctement le couple enveloppe / fichier de données.

Une fois les deux fichiers déposés dans le répertoire `outbox`, l'adaptateur procède à l'envoi des données vers le serveur PassaVD.

En cas de succès, les fichiers sont déplacés et renommés dans le répertoire sent, avec l'ajout en suffixe de la date d'envoi des données.

En cas d'erreur lors de l'envoi, les fichiers sont déplacés et renommés dans le répertoire `errors`, avec l'ajout en suffixe de la date de l'erreur.

6.2 Réception d'un message

L'adaptateur interroge régulièrement le serveur PassaVD afin de télécharger les nouveaux messages arrivés dans sa boîte aux lettres. Ceux-ci sont enregistrés dans le répertoire **`inbox`** selon le format suivant :

- `envl_Y.xml`
- `data_Y.<extension>`

Où Y correspond à un numéro séquentiel unique (UUID) généré par l'adaptateur.

6.3 Réception d'une quittance

L'adaptateur interroge régulièrement le serveur PassaVD afin de télécharger les quittances arrivées dans sa boîte aux lettres. Celles-ci sont enregistrés dans le répertoire **`receipt`** selon le format suivant : `receipt_M_Y.xml`

Où M est le messageId et Y correspond à un numéro séquentiel unique (UUID) généré par l'adaptateur.

Se référer au chapitre 5.2 Quittances Passavd (receipt)

6.4 Interroger les registres cantonaux par Web Service

L'adaptateur PassaVD embarque un serveur web. Celui-ci constitue le point d'entrée pour l'accès aux web services RCPers, REF-INF et CheckSedex. Il agit comme un reverse proxy HTTP.

Lorsqu'un appel HTTP est reçu, l'adaptateur le redirige vers les services web RCPers, REF-INF ou PassaVD, en établissant une connexion sécurisée avec l'État de Vaud.

Requête pour interroger RCPers :

```
http://<hostclient>:<port>/ws/rcpers/v1/listOfPersons?
firstName=Jacqueline&name=dupont
```

Requête pour interroger REF-INF :

```
http://<hostclient>:<port>/ws/refinf/v1/listOfPostalLocalities?
shortName=Orbe
```

WSDL du web service CheckSedex :

```
http://<hostclient>:<port>/passavd/services/CheckSedexWebService?wsdl
```

IMPORTANT - Pour invoquer les web services RCPers et REF-INF, il est obligatoire de renseigner l'en-tête http : **`X-vd-ws-username`** - celui-ci permet une traçabilité plus précise de l'appelant.

Pour plus d'informations sur l'utilisation de ces web services, veuillez-vous référer au document TEC-ServicesEchangesDonneesPourCommunes.doc.

7 INSTALLATION DU CLIENT PASSAVD

Le client PassaVD repose sur une JVM (Java Virtual Machine) pour fonctionner.

7.1 Prérequis

- Connexion internet vers les URLs :
  - http://pki.vd.ch/ - CRL - Certificat Revocation List
  - https://val-s2w.vd.ch/ - Services Passavd de **TEST**
  - https://s2w.vd.ch/ - Services Passavd de **PRODUCTION**
- 512 Mo de mémoire vive
- Open JDK version 21 - https://adoptium.net/temurin/releases?version=21&os=any&arch=any
- Être en possession de l'identifiant du participant
- Être en possession des fichiers certificats d'authentification et de cryptage, transmis par l'Etat de Vaud (email + sms)

7.2 Installation Assitée

Un installateur IzPack est disponible pour installer et configurer le logiciel à l'adresse :

https://www.vd.ch/passavd

7.2.1 Installation via l'assistant graphique

Vous pouvez installer PassaVD en exécutant la commande suivante :

```
java -jar passavd-installer.jar
```

Ou en double-cliquant directement sur le fichier JAR.

7.2.2 Installation en mode console

Il est également possible d'installer PassaVD en mode console avec la commande :

```
java -jar passavd-installer.jar -console
```

En mode console, les répertoires configurés à l'étape 4 de l'installation ne sont pas créés automatiquement par l'installateur. Vous devez donc les créer manuellement avant de démarrer PassaVD.

7.2.3 Installation sous macOS

Sur macOS, le champ « Parcourir » pour définir l'emplacement du JDK n'est pas disponible. Vous devez renseigner le chemin manuellement, que vous pouvez obtenir depuis un terminal avec la commande :

```
/usr/libexec/java_home -v
```

7.2.4 Installation sous Windows

Sous Windows, l'installateur doit être exécuté avec les droits administrateur :

Ouvrir l'invite de commandes (cmd) en tant qu'administrateur :

Clic droit sur Invite de commandes → Exécuter en tant qu'administrateur.

Lancer le JAR via la commande :

```
java -jar passavd-installer.jar
```

7.3 Installation manuelle

Voici les étapes d'installation :

1. Télécharger le tar.gz à l'adresse https://www.vd.ch/passavd
2. Dézipper le logiciel
3. Adapter le fichier config/`passavd.properties` en fonction de votre environnement

Attention : sous Windows, les répertoires réseau ne doivent pas être mappés avec une lettre car celle-ci est inaccessible lorsque PassaVD tourne en mode service.

Paramètre	Description
passavd.port*	Port du service http, par défaut le port est **8080**
passavd.outboxFolder	Répertoire de dépôt de fichiers et enveloppes pour envoi
passavd.errorsFolder	Répertoire des fichiers qui n'ont pas pu être envoyés
passavd.sentFolder	Répertoire des fichiers envoyés correctement
passavd.receiptsFolder	Répertoire des quittances
passavd.inboxFolder	Répertoire des arrivées de messages
passavd.echSchemaVersion	La version du schéma ech-0090 utilise (1 ou 2)
passavd.baseUrl	Url de base du service rest de l'Etat de Vaud. Environnement de test : https://val-s2w.vd.ch Environnement de production : https://s2w.vd.ch

passavd.participantId	L'identifiant du participant (ex. 2-VDTEST-1)
passavd.userEncKeyStorePassword	Le mot de passe du JKS de chiffrement
passavd.userAuthSignKeyStorePassword	Le mot de passe du JKS d'authentification
passavd.archiveWithSuffix	Flag indiquant s'il faut ajouter un suffixe lors de l'archivage des enveloppes et data
proxy.enable*	Activation d'un proxy http (false ou true)
proxy.host*	Hostname du serveur hébergeant le proxy http
proxy.port*	Port TCP du serveur hébergeant le proxy http

*Paramètres optionnels

Exemple de valeur pour les répertoires :

- Windows :
  - Local : C:\\PassaVD1\\interface\\outbox
  - Partage réseau : //serveur/interface/outbox
- Unix : /home/passavd/interface/outbox

4. Indiquer l'emplacement complet de la JVM dans les fichiers suivants

Fichier	Description
yajsw/bin/setenv.bat	set JAVA_HOME=${passavd.jdkpath}
yajsw/bin/setenv.sh	export JAVA_HOME=${passavd.jdkpath}

5. Adapter le fichier `yajsw/conf/wrapper.conf`

Paramètre	Description
wrapper.working.dir	Racine d'installation du service passavd (ex. c:/Passavd)
wrapper.logfile	Fichier de log du wrapper (ex. c:/Passavd/log/wrapper.log)
wrapper.java.command	Emplacement du binaire JAVA

6. Installation des certificats : Déposer les fichiers JKS (contenant votre clé privée et certificat), fournis par le canton de Vaud dans le répertoire `security`. Ils doivent avoir comme nom « client_authsign.jks » et « client_enc.jks ».

7.4 Mise à jour automatiques

L'adapter PassaVD effectue des mis à jour automatique à distance.

Les éléments suivants sont susceptibles d'être modifiés :

- Les librairies présentes dans le sous répertoire lib
- Configuration passavd.properties et wrapper.conf
- Certificats JKS et autres fichiers liés à la sécurité

Cette fonctionnalité est principalement utilisée dans le but de renouveler les certificats de sécurité sans intervention humaine.

IMPORTANT : Le processus PassaVD doit disposer des droits nécessaires pour effectuer des modifications sur ces éléments. En cas d'erreur lors de la mise à jour, notamment en raison de restrictions liées aux droits d'accès, le client PassaVD peut échouer lors de son redémarrage.

7.5 Démarrage du client et installation en tant que service

Le client PassaVD est livré avec le Java Wrapper Service YAJWS. Celui-ci permet de créer un service PassaVD dans Windows et Linux. Il redémarre aussi automatiquement le client PassaVD en cas de plantage ou de problème grave de la JVM.

Attention : sous Windows, toutes les commandes doivent être exécutées en tant qu'administrateur (clic droit sur le .bat et sélectionner "Exécuter en tant qu'administrateur")

Commande	Description
bin/runConsole.sh bin/runConsole.bat	Démarrer PassaVD en mode console. Cette commande peut être utilisée lors du premier démarrage pour valider le fonctionnement du client Passavd. L'installation en tant que service n'est pas nécessaires pour ces commandes
bin/installService.sh bin/installService.bat	Installe un service PassaVD dans le système. Le nom du service est défini dans le fichier de configuration `yajws/conf/wrapper.conf`. Dans ce fichier, vous pouvez éventuellement définir un utilisateur spécifique avec lequel s'exécute le processus PassaVD via les propriétés suivantes : Pour Windows : • wrapper.ntservice.account • wwrapper.ntservice.password Pour Unix: • wrapper.app.account • wrapper.app.password Cet utilisateur doit avoir les droits d'accès sur les répertoires de

	l'interface PassaVD. Une fois que le service est installé, ce fichier de configuration ne doit pas être modifié. Il faut d'abord désinstaller le service avant de le modifier.
bin/uninstallService.sh bin/uninstallService.bat	Désinstalle le service PassaVD
bin/startService.sh bin/startService.bat	Démarre le service PassaVD
bin/stopService.sh bin/stopService.bat	Stoppe le service PassaVD
bin/queryService.sh bin/queryService.bat	Permet de savoir entre autres si le service est installé, actif et s'il démarre automatiquement.

7.6 Console Web et web services de la plateforme PassaVD

En plus des WebServices REF-INF, RCPers et CheckSedex, le client PassaVD mets à disposition des services spécifiques à la plateforme PassaVD.

URL	Description
http://<hostclient>:<port>	Page d'accueil du client PassaVD.
http://<hostclient>:<port>/passavd/console	Application WEB permettant entre autres de connaître l'état de connexion des participants
http://<hostclient>:<port>/passavd/services/ping	Url permettant d'effectuer un ping afin de tester la connectivité avec le serveur PassaVD
http://<hostclient>:<port>/sendloopback	Envoi d'un nouveau message de test (loopback) au participant 0-sedex-0
http://<hostclient>:<port>/loopback	Affiche la dernière quittance de test reçue (loopback)
bin/queryService.sh bin/queryService.bat	Permet de savoir entre autres si le service est installé, actif et s'il démarre automatiquement.

7.7 Suivi et configuration des logs

Les logs de l'application sont enregistrés dans le répertoire logs, 4 fichiers sont créés spécialement dans le sous répertoire log pour faciliter le monitoring spécifique à la plateforme PassaVD :

- passavd.log – suivi technique du client passavd
- passavd_outbox.log– suivi de l'envoi d'un document
- passavd_inbox.log – suivi de la réception d'un document
- wrapper.log – fonctionnement du wrapper Java

La configuration des logs se trouve dans le répertoire config/logback.xml