Manuel PassaVD

Version 3.3.0
12.02.2024

Suivi des modifications

Version	Date	Nom	Remarque
0.1	11.11.2013	Christophe Rodriguez	Initialisation
0.2	19.11.2013	Christophe Rodriguez	Corrections
1.0	25.11.2013	Paul Meigniez	Première diffusion aux fournisseurs de logiciel CdH
1.1	15.01.2014	Christophe Rodriguez	-Nouveaux codes d'erreurs de quittance liés à la cryptographie -Utilisation de YAJWS -Revue des commandes d'exploitation -Précisions sur les appels de WS -Prise en charge des éléments « loopback » et « testData » dans l'enveloppe -Mises à jour automatiques
1.2.0	28.05.2014	Christophe Rodriguez	-Correction de la documentation concernant la configuration du proxy http -Précisions sur l'exécution de PassaVD en tant que service -Ajout d'exemples de valeurs pour l'installation manuelle
2.0.0	27.10.2014	Christophe Rodriguez	-Ajout compatibilité JAVA 8 -Ajout d'un service HTTP accessible depuis la page d'accueil du client qui permet de générer un message de test (loopback)
2.0.1	25.03.2015	Christophe Rodriguez	Ajout d'un paramètre booléen archiveWithSuffix permettant de désactiver le suffixe lors de l'archivage dans les répertoires sent et error
2.0.2	15.04.2015	Christophe Rodriguez	-Correction problème de paramètres manquants pour l'utilisation de PassaVD derrière un proxy -La page d'accueil du client PassaVD affiche dorénavant des informations concernant des problèmes d'installation
3.1.0	17.10.2019	Julien Hattab	Support vers OpenJDK
3.1.4.c02	07.01.2021	Julien Hattab	Patch log4j (CVE-2021-44228)
3.2.0	26.04.2023	Julien Hattab	Prise en charge de la nouvelle PKI ADCS
3.3.0	12.02.2024	Julien Hattab	Support Open JDK 17+

Table des matières

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 entres 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 faut intégrer un logiciel fourni par le canton de Vaud : l'adaptateur PassaVD.

1. Objectifs du document

Ce document décrit le système PassaVD du point de vue des applications participant à l'interconnexion avec le serveur PassaVD. Il est destiné en premier lieu aux fournisseurs de logiciels développant ce genre d'applications.
Les publics cibles de ce document sont :

- les architectes de logiciels ;
- les développeurs de logiciels ;
- les responsables de sécurité.

Ce manuel fixe les conditions de mise en œuvre pour les fournisseurs de logiciels qui souhaitent raccorder leurs applications à PassaVD.

2. Glossaire

Notion	Signification
Adaptateur	Elément de liaison entre les applications participant à l'interconnexion avec la plateforme PassaVD
Application	Logiciel participant à l'interconnexion avec la plateforme PassaVD
ID Participant	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

3. 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 et d'un fichier de données utiles.

Ceux-ci sont déposés dans des répertoires systèmes où est installé l'adaptateur PassaVD.

Celui-ci initie la connexion avec le serveur PassaVD pour effectuer des opérations d'envoi et de réception de documents.

La connexion se fait en HTTPS avec une authentification cliente et serveur. De plus, le fichier de données utiles est crypté avec le certificat public du destinataire et signé avec la clé privée de l'émetteur. Toutes ces opérations sont réalisées par l'adaptateur. Ainsi, le destinataire du message est le seul à pouvoir lire les données qui lui sont adressées.

Les requêtes émises par l'adaptateur passent par un Reverse Proxy à l'Etat de Vaud qui redirige les appels sur les bons systèmes en fonction du contexte d'appel.

Concernant l'accès aux registres RCPers et REF-INF par web services, l'adaptateur expose un Reverse Proxy HTTP pour accéder à ceux-ci. L'adaptateur PassaVD se charge de l'authentification pour communiquer avec les services correspondants.

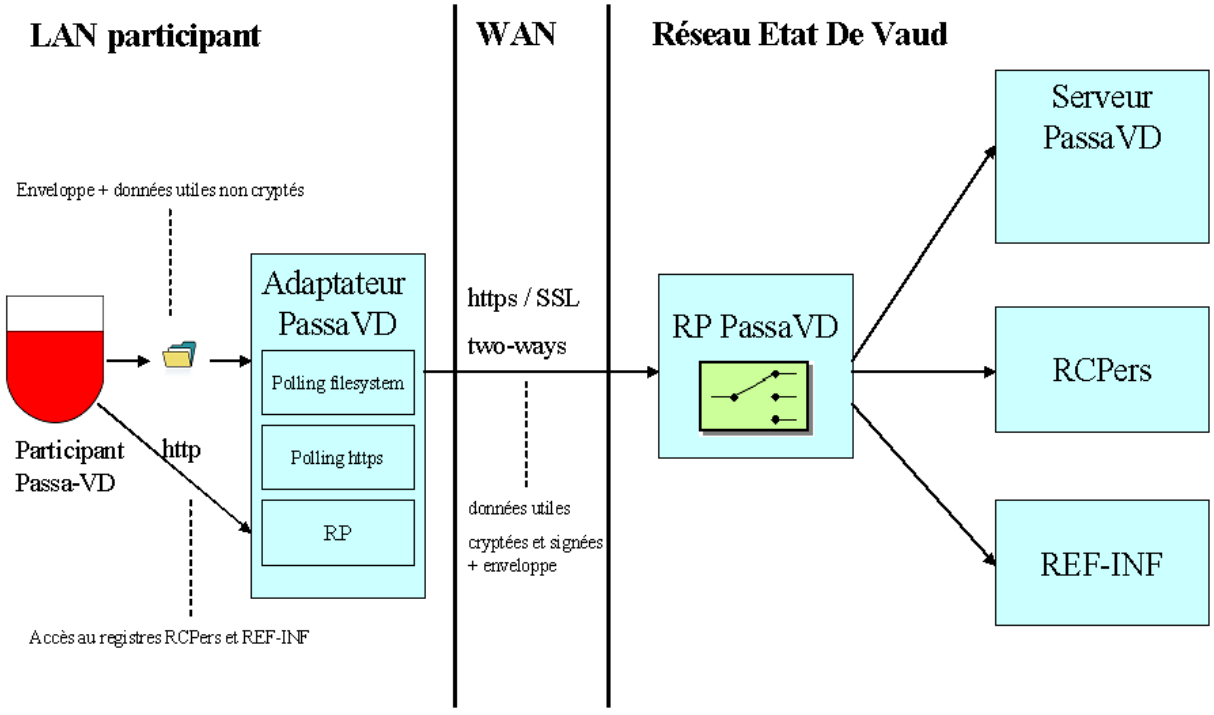

Figure 1 Architecture de PassaVD

4. Le participant

Les participants à l'interconnexion PassaVD sont par exemple les services administratifs des communes, les cantons et la Confédération. Ils sont identifiés par un ID univoque.
Celui-ci est une chaîne de caractères comparable à une adresse de messagerie. Il est décomposé en 3 parties:

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

Le domaine permet d'identifier le type de participant : une commune, un canton, la confédération, etc. Il s'agit d'un chiffre entre 0 et 9 avec éventuellement un T devant s'il s'agit d'un participant créé pour les tests.
L'unité organisationnelle est un identifiant le plus souvent métier, par exemple, dans le cadre d'une commune, son numéro OFS. Elle est composée de chiffres et de lettres en majuscule.
La fonction décrit le secteur d'activité du participant. Il s'agit d'un nombre entier. La fonction «1 » indique par exemple qu'il s'agit du secteur d'activité « Registre des habitants ».

4.1. Domaine

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.
9	réservé	

Il est possible de distinguer des participants qui ne servent qu'à des fins de test. L'ID de ces participants est muni d'un préfixe "T" (pour le nom de domaine). De tels participants peuvent uniquement communiquer entre eux.

4.2. Fonction

Les valeurs existantes pour les secteurs d'activités sont les suivantes :

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.

4.3. Exemples

- 0-sedex-0 (la valeur est donnée par la norme eCH-0090 : elle ne peut pas être modifiée) 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.

5. Possibilités de raccordement à PassaVD

Il existe deux possibilités de raccorder un participant à PassaVD :

- raccordement physique ;
- raccordement logique.

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

5.1. Raccordement physique

Un participant est dit physique lorsqu'il possède une boîte aux lettres. Autrement dit, il peut interroger le serveur PassaVD pour récupérer les nouveaux messages qui lui sont adressés, contrairement à un participant logique.

5.2. Raccordement logique

Un participant est dit logique lorsqu'il reçoit les messages qui lui sont adressés à travers la boîte aux lettres d'un participant physique. La mise à disposition des messages entrants et la récolte des messages sortants doivent être prises en charge par le centre de calcul chargé de la gestion du participant physique. Cette tâche est en général exécutée par un programme « dispatcher » développé par le centre de calcul.

Cette solution est utilisée surtout lorsqu'une infrastructure informatique est partagée.

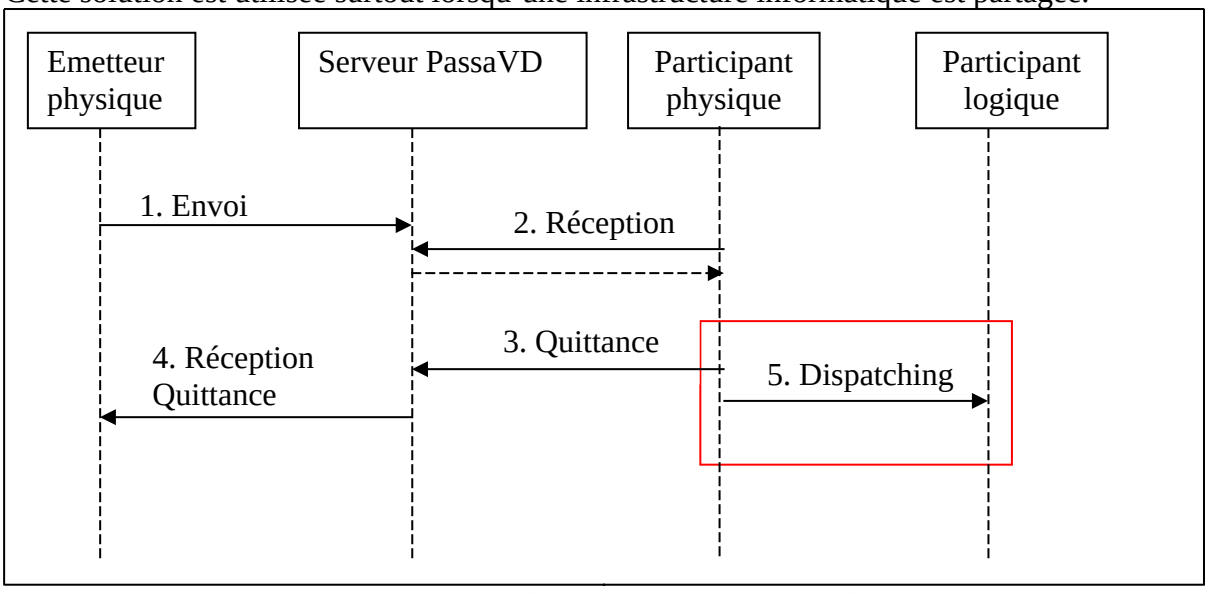

Figure 2 Raccordement logique et dispatching

5.3. Indépendance à l'égard de l'adressage des messages

Le type de raccordement d'un participant n'a aucune influence sur l'adressage des messages. L'émetteur d'un message n'a pas à se soucier de savoir si le destinataire est un participant logique ou physique.

6. Scénarios de communication

6.1. Envoi d'un document à un ou plusieurs destinataire physique et/ou logiques

Ce scénario 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.

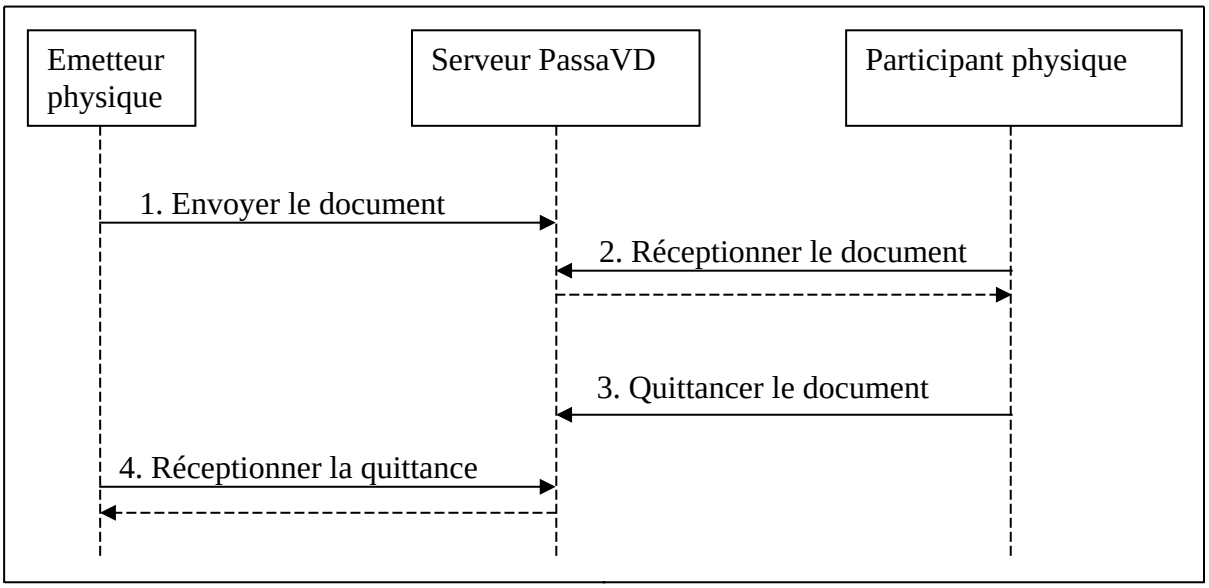

Figure 3 : Envoi réussi d'un message à un destinataire physique

Un émetteur envoie un document à un destinataire. Celui-ci arrive dans la boîte aux lettres d'un participant physique (sur le serveur PassaVD). Le participant physique (l'adaptateur du destinataire) télécharge le document puis émet une quittance de réception à l'intention de l'émetteur.
L'émetteur reçoit une quittance indiquant que le destinataire a bien reçu le message.

6.2. Envoi d'un document à une liste de distribution

Ce scénario permet à un émetteur d'envoyer un message à tous les participants intéressés par ce type d'information.
Dans ce cas, l'émetteur envoie le message à un destinataire qui est une liste de distribution.

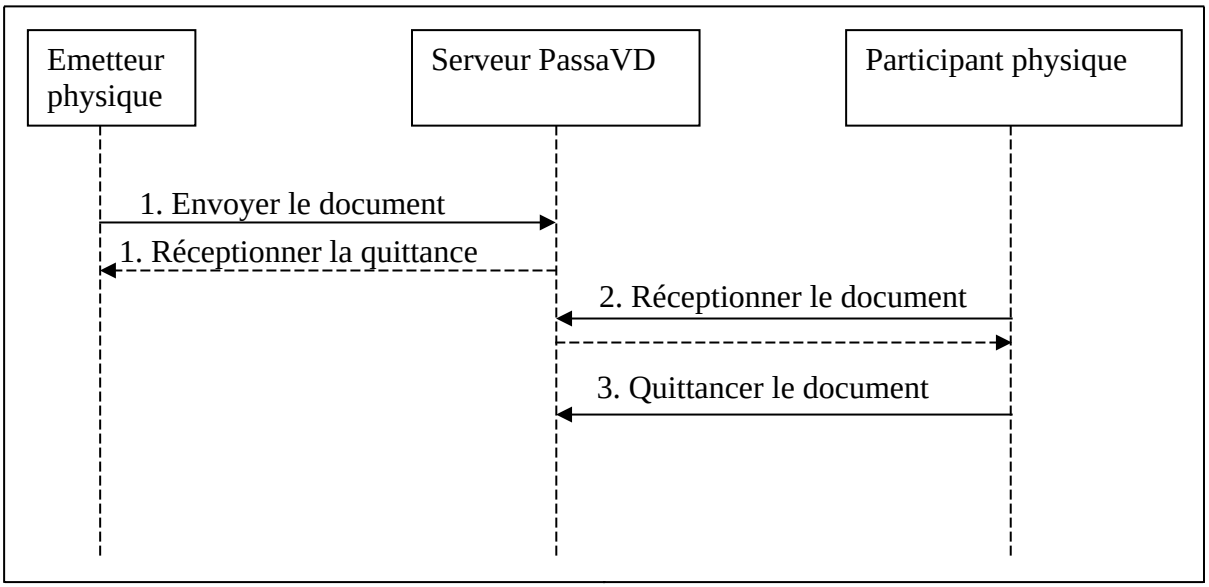

Figure 4 : Envoi réussi d'un message à une liste de distribution

L'émetteur envoie un document à destination d'une liste de distribution. Il reçoit immédiatement en retour du serveur PassaVD une quittance indiquant que le message bien été reçu par celui-ci. A la différence d'un envoi normal, il ne reçoit pas de quittance pour chaque destinataire de cette liste de distribution.

7. Contenu de l'enveloppe

L'enveloppe d'un message PassaVD est un fichier XML respectant le schéma XML eCH-0090 de la confédération disponible à l'adresse suivante :
http://www.bfs.admin.ch/bfs/portal/fr/index/news/00/00/12/06.html
Elle est émise par un participant et permet au serveur PassaVD d'effectuer le routage.

Les éléments à renseigner sont les suivants :

Nom de l'élément	Signification	Type	Oblig	Nb
messageId	C'est un identifiant unique qui permet à une application émettrice de corréler le message qu'elle envoie avec les quittances qu'elle reçoit	String, correspondant l'expression régulière. ([a-zA-Z] | [0-9] | -){1,36} Il est recommandé d'utiliser un UUID.	Oui	1
messageType	Définit le type de message. L'émetteur s'accorde avec le destinataire sur le type de message.	[0 ... 2699999] (sous-ensemble de xs:int)	Oui	1
messageClass	Définit dans le cadre du type de message la signification du message. Les valeurs suivantes sont prédéfinies : 0= Message initial 1= Réponse 2= Quittance 3= Erreur 4 et 9 et 11 – maxint = réservé pour des développements ultérieurs	xs :int	Oui	1
referenceMessageId	Cet élément est renseigné dans la réponse à un message pour permettre à l'émetteur original de faire la corrélation. Il est renseigné lorsque le messageClass = 1,2 ou 3	Idem que messageId	Non	1
senderId	Emetteur du message. Identifiant du participant.	String constitué de : <domaine-unité orga-fonction>	Oui	1
recipientId	Destinataire(s) du message	Format idem que le senderId	Oui	> 0
eventDate	Date métier de l'évènement auquel se réfèrent les données utiles	xsd:dateTime	Oui	1
messageDate	Date technique d'envoi du document	xsd:dateTime	Oui	1
loopback	Indique qu'il s'agit d'un message de test. Le destinataire	Pas de type	Non	0-1

	reçoit le message mais ne le stocke pas. L'émetteur reçoit tout de même une quittance.			
testData	Meta-data sous forme de clé-valeur qu'il est possible d'ajouter à une enveloppe. N'a pas d'incidence sur l'adressage.	Clé-valeur de type String	Non	0-n

8. Contenu de la quittance

La quittance d'un message PassaVD est un fichier XML respectant le schéma XML eCH-0090 de la confédération disponible à l'adresse suivante :
http://www.bfs.admin.ch/bfs/portal/fr/index/news/00/00/12/06.html

Les éléments présents sont les suivants :

Nom de l'élément	Signification	Type	Oblig	Nb
eventDate	Date de l'évènement qui a conduit à la quittance.	xsd :dateTime	Oui	1
statusCode	Status du message : OK ou code d'erreur	Enumération sur la base de xsd :int.	Oui	1
statusInfo	Texte d'information sur le code de statut	Xsd :string, maxlength=255	Oui	1
messageId	ID du message auquel la quittance se réfère	Idem que dans l'enveloppe	Oui	1
messageType	Type de message du message auquel la quittance se réfère	Idem que dans l'enveloppe	Oui	1
messageClass	Classe de message du message auquel la quittance se réfère	Idem que dans l'enveloppe	Oui	1
senderId	Emetteur du message auquel la quittance se réfère	Idem que dans l'enveloppe	Oui	1
recipientId	Récepteur du message auquel la quittance se réfère	Idem que dans l'enveloppe	Oui	1

Les codes et statuts OK des quittances sont les suivants :

StatusCode	StatusInfo	Signification
100	Message correct transmitted	Le message a bien été transmis au destinataire. Il n'y aura pas d'autres quittances.
601	Message successfully sent	Le message a bien été transmis au serveur PassaVD. Il y aura une quittance pour chaque destinataire lorsque ceux-ci téléchargeront le message.

Les codes et statuts d'erreurs des quittances sont les suivants :

StatusCode	StatusInfo	Signification
202	No payload found. File : <nom_du fichier avec extension>	Uniquement pour l'adaptateur : Le fichier data n'a pas été déposé depuis plus de 2h dans le répertoire outbox
200	Invalid envelope syntax	L'enveloppe envoyée n'est pas valide selon la XSD
312	User certificate not valid	Le certificat X509 du client n'est pas valide
201	Duplicate message ID	Un autre message avec le même identifiant à été envoyé par le participant et n'a pas encore été reçu
310	Not allowed to send. Inactive.	L'emetteur n'est pas actif
310	Not allowed to send. Prohibited receipientIds = {ids}	Une règle de routage interdit l'envoi à un ou plusieurs destinataires
311	Not allowed to receive. Inactive RecipientsIds= {ids des inactifs)	Un ou plusieurs destinataires ne sont pas actifs
330	Message size exceeds limit	Le message est trop volumineux
203	Message to old to send.	La date messageDate renseignée dans l'enveloppe dépasse 30 jours
400	Network error. Can't validate enveloppe.	Uniquement pour l'adaptateur : Impossibilité de communiquer avec le serveur
500	No envelope found. File : <nom_du fichier avec extension>	Uniquement pour l'adaptateur : L'enveloppe n'a pas été déposé depuis plus de 2h dans le répertoire outbox
500	Part of recipients are not Distribution list	S'il y a une liste de distribution comme destinataire alors tous les destinataires doivent être des listes de distribution
500	Cannot encrypt file	L'adaptateur n'arrive pas à encrypter le fichier
500	Recipient certificate not valid	Le certificat du destinataire (fourni par le serveur) n'est pas valide
500	Recipient certificate signature not valid	Le signature du certificat du destinataire (fourni par le serveur) n'est pas valide
500	Recipient certificate unreadable	Le certificat du destinataire (fourni par le serveur) est illisible
500	Recipient cannot decrypt file	Le destinataire a reçu le fichier mais n'arrive pas à le décrypter
500	Sender certificate not readable	Le destinataire a reçu le fichier mais n'arrive pas à lire le certificat de l'émetteur
500	Sender certificate not valid	Le destinataire a reçu le fichier mais le certificat de l'émetteur n'est pas valide
500	Signature of sender certificate not valid	Le destinataire a reçu le fichier mais la signature du certificat de l'émetteur n'est pas valide
500	Integrity of file not valid	Le destinataire a reçu le fichier mais celui-ci est corrompu (problème d'empreinte)

9. L’adaptateur PassaVD

L’adaptateur PassaVD est un logiciel qui fonctionne selon le même principe que l’adaptateur de la plateforme Sedex. Il s’agit d’un logiciel qui est installé dans l’infrastructure du participant.

Il fonctionne de manière bidirectionnelle, ce qui veut dire qu’il peut aussi bien faire fonction d’émetteur que de récepteur de messages PassaVD. Il assume les tâches suivantes :

- surveillance d’un répertoire dans le système de fichiers, dans lequel l’application émettrice dépose les messages à envoyer ;
- répétition multiple de l’envoi, lorsqu’un problème technique surgit ;
- interrogation périodique de la boîte aux lettres ;
- téléchargement des messages depuis la boîte aux lettres. Ceux-ci sont déposés dans un répertoire inbox du système de fichier ;
- reverse proxy pour la consultation des registres RCPers et REF-INF.

L’adaptateur PassaVD a besoin de plusieurs répertoires du système de fichiers pour fonctionner :

- outbox (les messages à envoyer) ;
- inbox (les messages reçus) ;
- sent (les messages traités) ;
- receipts (les quittances) ;
- errors(les messages qui n’ont pas pu être envoyés).

L’interface exposée par celui-ci pour les échanges de documents fonctionne sur le principe de lecture et l’écriture de fichiers dans les répertoires outbox, inbox et receipts.

9.1. Transmission d'un message

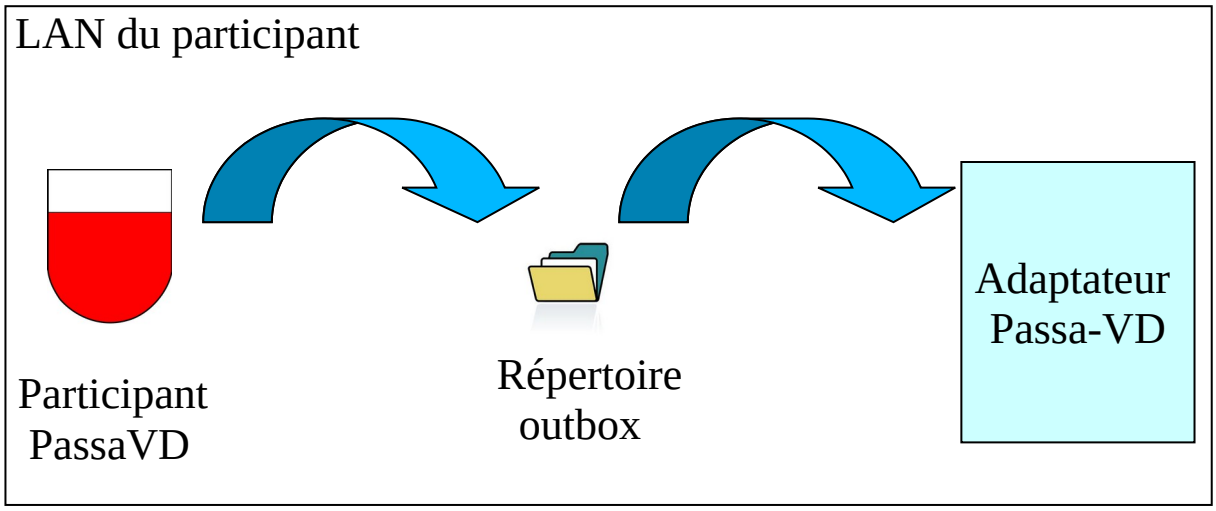

Figure 4 : Envoi d'un document à travers l'adaptateur

Pour envoyer un message, le participant doit déposer un fichier de données ainsi qu'une enveloppe au format ech90 dans le répertoire outbox du système de fichier de l'adaptateur.
L'enveloppe doit posséder un préfixe « envl_ » et doit se terminer par « .xml ».
Le fichier data doit commencer par « data_ » et peut avoir une extension quelconque.

Le nom des fichiers sans le préfixe ni le suffixe constitue l'identifiant de corrélation qui va permettre à l'adaptateur PassaVD d'identifier le couple « enveloppe / fichier data ».

Une fois les 2 fichiers déposés dans le répertoire outbox, l'adaptateur peut émettre les données au serveur.

Si tout se passe bien, les fichiers sont déplacés et renommés dans le répertoire sent avec comme suffixe la date d'envoi des données

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

De plus, un fichier de quittance au format ech-90 peut être généré immédiatement dans le répertoire receipts dans les situations suivantes :

- L'envoi s'est bien déroulé et le fichier a été transmis à une liste de distribution. Dans ce cas, une quittance est générée avec les éléments suivants :

Champ	Valeur
eventDate	Date de l'envoi
statusCode	100
statusInfo	Message correct transmitted
messageId	Repris de l'enveloppe
messageType	Repris de l'enveloppe
messageClass	Repris de l'enveloppe
senderId	Repris de l'enveloppe
recipientId	0-sedex-0

- L'enveloppe et le fichiers data ont été déposés dans le répertoire outbox et respectent bien le principe des préfixes data_* et envl_*.xml mais une erreur côté serveur est survenue. Dans ce cas, la quittance contient les éléments suivants :

Champ	Valeur	Valeur par défaut (si valeur originale non trouvée)
eventDate	Date de l'erreur	N/A
statusCode	<Code de l'erreur>	N/A
statusInfo	<Description de l'erreur>	N/A
messageId	Repris de l'enveloppe	0
messageType	Repris de l'enveloppe	0
messageClass	Repris de l'enveloppe	0
senderId	Repris de l'enveloppe	0-sedex-0
recipientId	0-sedex-0	N/A

- Il manque le fichier data et 2 heures se sont écoulées:

Champ	Valeur	Valeur par défaut (si valeur originale non trouvée)
eventDate	Date de l'erreur	N/A
statusCode	202	N/A
statusInfo	No payload found. File : <nom_du fichier avec extension>	N/A
messageId	Repris de l'enveloppe	0
messageType	Repris de l'enveloppe	0
messageClass	Repris de l'enveloppe	0
senderId	Repris de l'enveloppe	0-sedex-0
recipientId	0-sedex-0	N/A

- Il manque l'enveloppe et 2 heures se sont écoulées

Champ	Valeur	Valeur par défaut (si valeur originale non trouvée)
eventDate	Date de l'erreur	N/A
statusCode	500	N/A
statusInfo	No envelope found. File : <nom_du fichier avec extension>	N/A
messageId	0	N/A
messageType	0	N/A
messageClass	0	N/A
senderId	0-sedex-0	N/A
recipientId	0-sedex-0	N/A

- Voir le chapitre Contenu de la quittance pour les autres cas

Le format du nom du fichier de quittance enregistré dans le répertoire receipt est le suivant:
Receipt_IDMY.xml
M = messageId
Y = numéro séquentiel univoque (UUID généré par l'adaptateur)

9.2. 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 au format suivant :
envl_Y.xml
data_Y.<extension>

Y = numéro séquentiel univoque (UUID généré par l'adaptateur)

9.3. Réception d'une quittance

L'adaptateur interroge régulièrement le serveur PassaVD afin de télécharger les quittances arrivées dans sa boîte aux lettres.
Les quittances sont stockées dans le répertoire Receipts avec comme nom de fichier :
Receipt_IDMY.xml
M = messageId
Y = numéro séquentiel univoque (UUID généré par l'adaptateur)

9.4. Reverse Proxy pour l'accès aux web services RCPers, REF-INF et CheckSedex

L'adaptateur PassaVD embarque un serveur web. Celui-ci est le point d'entrée pour accéder aux web services RCPers, REF-INF et CheckSedex (Il s'agit d'un Reverse Proxy HTTP).

Lorsque l'adaptateur reçoit un appel HTTP, il redirige celui-ci sur les services web RCPers, REF-INF ou PassaVD en établissant une connexion sécurisée avec l'Etat de Vaud.

Exemple de requête pour interroger RCPers :
http://<hostclient>:<port>/ws/rcpers/v1/listOfPersons?firstName=Jacqueline&name=dupont

Exemple de requête pour interroger REF-INF :
http://<hostclient>:<port>/ws/refinf/v1/listOfPostalLocalities?shortName=Orbe

WSDL du WebService CheckSedex :
http://<hostclient>:<port>/passavd/services/CheckSedexWebService?wsdl

Pour invoquer les web services de RCPers et REF-INF, il est obligatoire de renseigner le header HTTP «X-vd-ws-username ». Il permet de tracer plus précisément l'appelant.

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

9.5. Installation de l'adaptateur PassaVD

L'adapter PassaVD fonctionne sur la base d'un serveur JAVA OSGI Karaf.

Pré-requis techniques

- Connexion internet
- 512 Mo de mémoire vive (RAM)
- L'adapter a été testé avec la version OpenJDK 17 distribuée par AdoptOpenJDK - https://adoptopenjdk.net. Le client est compatible JAVA 17.

Autres pré-requis

- S'être annoncé comme nouveau participant
- Etre en possession de l'identifiant du participant
- Etre en possession des .jks d'authentification et de cryptage fournis par l'Etat de Vaud

Installation assistée

Un installateur IzPack est à disposition pour installer et configurer le logiciel à l'adresse : https://www.vd.ch/passavd

Vous pouvez installer PassaVD via un assistant graphique en exécutant la commande `java -jar passavd-installer.jar` ou en double-cliquant sur le jar

Vous pouvez aussi installer PassaVD avec cet assistant en mode console via la commande suivante : `java -jar passavd-installer-jar` -console

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

Concernant l'installation sous **MAC OSX**, il n'est pas possible d'utiliser le champ « Parcourir », pour définir l'emplacement du JDK. Il faut le renseigner manuellement en récupérant le chemin depuis un terminal via la commande :
`/usr/libexec/java_home –v`

Concernant l'installation sous **Windows 10**, l'installateur doit être exécuté comme administrateur. Pour cela, il faut :

1. lancer l'invite de commande (cmd) en tant qu'administrateur (clic droit sur "Invites de commandes" et sélection de "Exécuter comme administrateur) " ;
2. lancer le jar via la commande `java -jar passavd-installer.jar`.

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. Aller dans le répertoire config et adapter le fichier « passavd.cfg » 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	Exemple de valeur
outboxFolder	Répertoire d'envoi	Windows : Local : C:\\PassaVD1\\interface\\outbox Réseau: //serveur/interface/outbox Unix : /home/passavd/interface/outbox
errorsFolder	Répertoire des erreurs	Windows : Local: C:\\PassaVD1\\interface\\errors Réseau: //serveur/interface/errors Unix: /home/passavd/interface/errors
sentFolder	Répertoire des fichiers correctement transmis	Windows : Local : C:\\PassaVD1\\interface\\sent Réseau: //serveur/interface/sent Unix: /home/passavd/interface/sent
receiptsFolder	Répertoire des quittances	Windows : Local : C:\\PassaVD1\\interface\\receipts Réseau: //serveur/interface/receipts Unix: /home/passavd/interface/receipts
inboxFolder	Répertoire des fichiers reçus	Windows : Local: C:\\PassaVD1\\interface\\inbox Réseau: //serveur/interface/inbox Unix: /home/passavd/interface/inbox
echSchemaVersion	Version de l'enveloppe E-CH pour les fichiers envoyés et reçus	1 ou 2 (version 2 recommandée)
baseUrl	Url de base des appels	Environnement de test : https://val-s2w.vd.ch Environnement de production : https://s2w.vd.ch
participantId	Identifiant du participant	1-5586-1
userEncStorePassword	Mot de passe du .jks de cryptage	-

userAuthSignKeyStore Password	Mot de passe du .jks d'authentification	-
archiveWithSuffix	Booléen indiquant s'il faut ajouter un suffixe lors de l'archivage des enveloppes et data	true ou false

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

Fichier	ligne
bin/setenv.bat	set JAVA_HOME=<emplacement JVM> Exemple: set JAVA_HOME=C:\Program Files\Java\jdk-11.0.2
bin/setenv.sh	export JAVA_HOME=<emplacement JVM> Exemple: export JAVA_HOME=/usr/lib/jvm/jdk-11.0.2
yajws/bat/setenv.bat	set JAVA_HOME=<emplacement JVM> Exemple: set JAVA_HOME=C:\Program Files\Java\jdk-11.0.2
yajws/bin/setenv.sh	export JAVA_HOME=<emplacement JVM> Exemple: export JAVA_HOME=/usr/lib/jvm/jdk-11.0.2

5. Changer les ports d'écoute (si les ports par défaut ne conviennent pas)

Les ports par défaut sont les suivants :

Paramètre	Description	Valeur par défaut	Fichier de configuration
org.osgi.service.http.port	Port HTTP	8080	etc/org.ops4j.pax.web.cfg
rmiRegistryPort	Port RMI	1099	etc/org.apache.karaf.management.cfg
rmiServerPort	Port RMI	44444	etc/org.apache.karaf.management.cfg
wrapper.tray.port	Port YAJWS	15002	yajws/conf/wrapper.conf

6. Configurer un proxy HTTP (si nécessaire) dans le fichier etc/system.properties en ajoutant les 8 variables systèmes suivantes à la fin du fichier:

# Proxy HTTP 	
http.proxyHost=<nomduhost>
http.proxyPort=<port>
http.proxyUser=<utilisateur>
http.proxyPassword=<mot de passe>
	# Proxy HTTPS
	https.proxyHost=<nomduhost>
	https.proxyPort=<port>
	https.proxyUser=<utilisateur>
	https.proxyPassword=<mot de passe>

7. 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 ».

L'adapter est configuré. A l'exception du fichier wrapper.conf de yajws, les paramètres et fichiers de configurations qui ne sont pas cités dans ce chapitre ne doivent pas être modifiés.

Pour les opérations d'administration, veuillez vous référer au chapitre suivant.

9.6. Mises à jour automatiques

L'adapter PassaVD peut être mis à jour automatiquement à distance.

Les éléments suivants sont susceptibles d'être modifiés :

- les composants
- les fichiers de configuration système
- les certificats et autres fichiers liés à la sécurité

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

9.7. Exploitation de l'adapter PassaVD

Informations générales

Le serveur 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 Vista+, toutes les commandes doivent être exécutées en tant qu'administrateur (clic droit sur le .bat et sélectionner "Exécuter en tant qu'administrateur")

Commandes spécifiques à YAJWS

Commande	Description
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.

Autres commandes

Les commandes ci-dessous permettent de démarrer et de stopper PassaVD sans installer de service.

Commande	Description
bin/startConsole.sh bin/startConsole.bat	Permet de démarrer PassaVD en mode console. Le terminal affiche la console Karaf une fois le serveur démarré. Lorsque le terminal est fermé, le serveur PassaVD est stoppé.
bin/start.sh bin/start.bat	Equivalent au startConsole.sh mais sans arriver dans la console Karaf. Lorsque le terminal est fermé, le serveur PassaVD est stoppé.
bin/startNohup.sh	Permet de démarrer en arrière-plan le serveur PassaVD. Cette commande est uniquement disponible sous Unix.
bin/stop.sh bin/stop.bat	Arrêter un serveur PassaVD qui a été démarré avec l'une des commandes ci-dessus.

Console et web services de la plateforme

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)

En cas de problème de configuration du client PassaVD, tous ces services sont redirigés sur une page d'erreur HTML (code HTTP 500) avec une description des différents problèmes.

Suivi et configuration des logs

Les logs de l'application sont enregistrés dans le répertoire logs.
3 fichiers sont créés spécialement pour faciliter le monitoring spécifique à la plateforme PassaVD :

- transmettreUnDocument.log – suivi de l'envoi d'un document
- receptionnerUnDocument.log – suivi de la réception d'un document
- miseAjourAutomatique.log – suivi des mises à jour automatiques

De plus, le fichier karaf.log permet d'obtenir plus de détails.

Concernant YAJWS, un fichier est créé pour les logs spécifiques au wrapper dans le répertoire yajws/log

La configuration log4j des logs se trouve dans le répertoire etc/org.ops4j.pax.logging.cfg

Connexion JMX

La configuration JMX se trouve dans le fichier etc/org.apache.karaf.management.cfg.

Pour vous connecter à Karaf en JMX, vous devez utiliser une URL au format suivant :
service:jmx:rmi://<ip>:< rmiServerPort>/jndi/rmi://<ip>:< rmiRegistryPort>/karaf-passavd

Les comptes utilisateurs du service JMS sont éditables dans le fichier etc/users.properties