Adaptateur swissdec

Guide de l'utilisateur

Historique des versions			
Version 1.0	2013-08-07	Marco Stettler	Version initiale français
Version 1.1	2013-10-15	Marco Stettler	Corrigé l'adresse du distributeur
Version 1.2	2014-01-30	Christoph Brunner	Recovery Tool & Patch Release 2.0_2
Version 1.3	2015-03-02	Marco Stettler	Patch Release 2.0_4

Table des matières

1. Introduction 1
1.1. Adaptateur swissdec 1
1.2. Présentation de swissdec 2
1.3. Interfaces 2
1.4. Références 5
2. Exigences liées au fonctionnement 6
2.1. Exigences du système 6
2.2. Structure de répertoire 9
2.3. Migration 10
3. Installation 11
3.1. Vérification des conditions préalables 11
3.2. Décompresser un package 11
3.3. Droits pour l'exécution (Unix seulement) 11
3.4. Configuration de l'environnement 12
3.5. Installation du module JCE Java 12
3.6. Application-réception 12
3.7. Application-intégration 19
3.8. Configuration de l'identification 21
3.9. Fenêtre de maintenance 21
3.10. Remarque conclusive 22
4. Test de l'installation 23
4.1. Installation 23
4.2. Configuration 23
4.3. Exécution des tests 24
5. Démarrage de l'adaptateur 25
5.1. Démarrage manuel 25
5.2. Démarrage comme service Windows 25
5.3. Unix script-init 27
6. Référence des configurations 29
6.1. Configuration Tomcat 29
6.2. Configuration de la réception 29
6.3. Configuration de l'application-intégration 30
7. Monitoring 32
7.1. Monitoring intégré 32
8. Recovery-Tool 34
8.1. Démarrage 34
8.2. Options 34
9. Problèmes et solutions 39
A. Annexe 41
A.1. Documents référencés 41
A.2. Glossaire 41
B. Exemples 42
B.1. Configuration 42

Liste des illustrations

1.1. Schéma d'installation de l'adaptateur swissdec 2
1.2. Interface du système de fichiers de l'adaptateur swissdec sM-client 3
3.1. Security Overview 14
3.2. Webservice Security Overview 15
3.3. SSL Handshake 17
3.4. Protocole Handshake SSL avec authentification mutuelle 17
3.5. Transport Layer Security Overview 18
5.1. tomcat6w.exe, Tomcat Service Properties 26
5.2. Tomcat Service Java Properties 26
5.3. Gestion des services Windows 27

Liste des tableaux

1.1. Pfade der Schnittstelle swissdec-Adapter - sM-Client 3
1.2. Chemin d'accès de l'interface de l'adaptateur swissdec - sM-client 4
2.1. swissdecAdapter.zip 9
3.1. swissdec-Adapter Receiver configuration de base 13
3.2. Security Overview 14
3.3. Webservice Security Signature 15
3.4. Webservice Security Encryption 16
3.5. swissdecAdapter Webservice Security Konfiguration 16
3.6. Configuration du protocole Transport Layer de l'adaptateur swissdec 18
3.7. Integration swissdec-Adapter configuration de base 20
3.8. Fichiers log 21
4.1. TestTool Konfiguration 23
6.1. swissdec-Adapter Receiver Grundkonfiguration 29
6.2. swissdec-Adapter Integration configuration 30
8.1. Recovery Tool, options générales 34

Liste des exemples

3.1. Standardconnector- Konfiguration Tomcat 13
3.2. Configuration connecteur Tomcat pour la planification SSL avec authentification mutuelle 18
3.3. Connecteur standard - Configuration Tomcat 19
B.1. Configuration standard réception 42
B.2. Configuration standard intégration 43
B.3. Configuration standard réception Tomcat 44
B.4. Configuration standard intégration Tomcat 45
B.5. Configuration standard identification 46

1. Introduction

Ce document décrit l'installation, la configuration et le fonctionnement de l'adaptateur *swissdec*. L'adaptateur swissdec est une application Java, composé de deux applications web, pour le remplacement des notifications swissdec concernant les domaines Tax [taxe] (attestations de salaire) ainsi que TaxAtSource [retenues à la source] (décomptes de l'impôt à la source). Conçu pour être intégré avec le *sM-Client* , il peut cependant aussi être utilisé de manière autonome.

1.1. Adaptateur swissdec

L'adaptateur swissdec offre les fonctionnalités suivantes:

- Réception et envoi de notifications *swissdec* conformes au protocole
- Transmission sécurisée des données salariales au moyen des protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security) ainsi que WS-Security (Web Services Security)
- Vérification de l'intégrité au moyen de la signature WS-Security

Note

La plate-forme swissdec est synchrone: chaque notification transmise par une société du distributeur est immédiatement traitée et redirigée vers le destinataire final. La société (source des données salariales) voit ainsi la totalité du système comme un ensemble. Si un destinataire final devait ne pas être traité avec la qualité requise, la fiabilité de tout le système serait réduite. Tous les participants doivent donc convenir d'une fiabilité minimale.

Nous désirons de prendre le point de vue du client. Ça veut dire qu'une solution internet s'adaptera aux heures d'ouverture courant. D'un autre côté les aspects économiques d'opération du destinataire (abordabilité) doivent aussi être respectés.

La disponibilité des systèmes doit être vu comme objectif prévu. Ça veut dire que l'importance de la solution augmente et cependant la disponibilité. L'objectif est une solution pragmatique ("lightweight construction" et "best effort"). Plage de temporisation défini:

- 7 jours par semaine à 24 heures
- Heures d'affluence: 6h à 20h

Domaine des valeurs défini:

- Heures d'affluence: Disponibilité des destinataires (m2m) 99.52% aux minimum
- Autres: Disponibilité des destinataires (m2m) 93.00% aux minimum

1.2. Présentation de swissdec

La plate-forme swissdec est un service orienté client – serveur, avec le distributeur considéré comme un intermédiaire. Le diagramme suivant donne un bref aperçu de la structure swissdec:

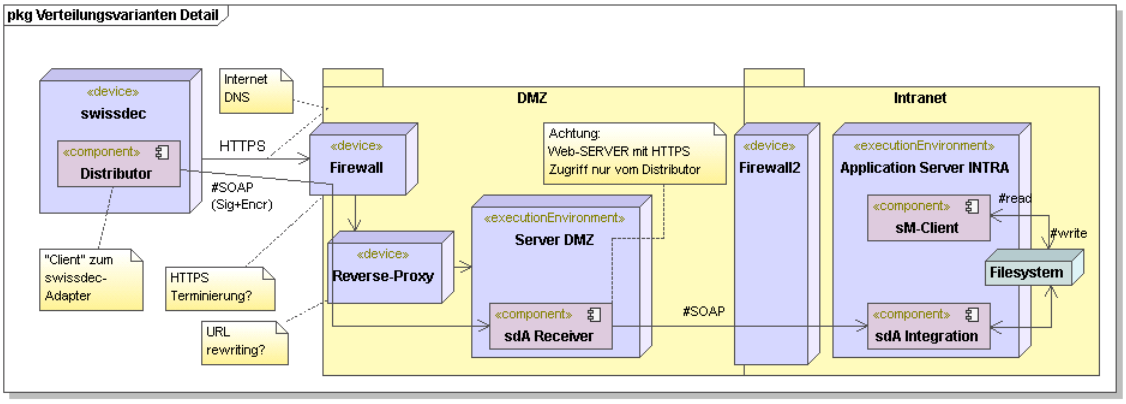


Figure 1.1. Schéma d'installation de l'adaptateur swissdec

1.3. Interfaces

1.3.1. swissdec

L'interface swissdec a déjà été implémentée dans le produit STEP de la société itServe, installée par plusieurs clients et appliquée par swissdec. La documentation swissdec peut être consultée sur le site internet http://www.swissdec.ch de l'association.

1.3.2. sM-Client

Une interface basée sur les fichiers intervient entre l'adaptateur swissdec et le *sM-Client*. L'adaptateur inscrit les notifications détaillées dans un répertoire-boîte de réception, qui sera interrogé par le *sM-Client*.

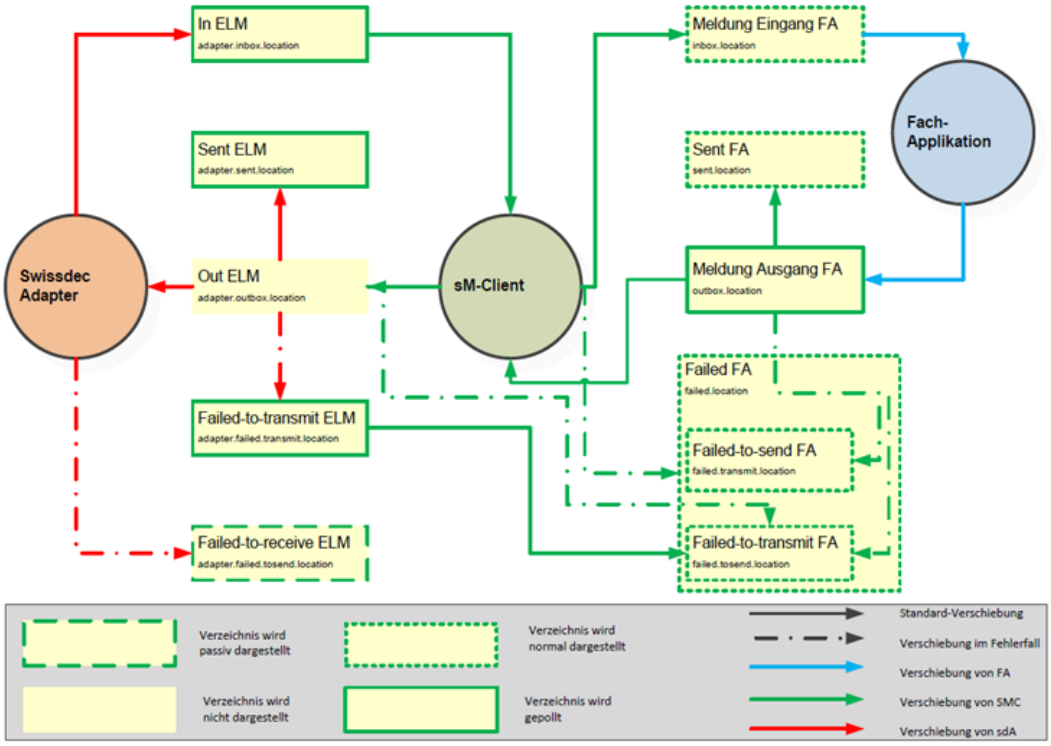


Figure 1.2. Interface du système de fichiers de l'adaptateur swissdec sM-client

sM-Client (Message-handler-elm.properties)	**PathID**	**Adaptateur swissdec (swissdecAdapter.properties)**
Dans le sM-client, ces répertoires sont relatifs à base.dir.adapter		L'adaptateur swissdec nécessite un chemin d'accès absolu dans ces fichiers de configuration
adapter.inbox.location	PATH_ELM_IN	released.filesystem.parent.xml
adapter.outbox.location	PATH_ELM_OUT	result.filesystem.parent.xml
adapter.sent.location	PATH_ELM_SENT	sent.filesystem.parent.xml
adapter.failed.receive	PATH_ELM_FAILED_TO_RX	failed.filesystem.parent.xml
adapter.failed.transmit.location	PATH_ELM_FAILED_TO_TX	undeliverable.filesystem. parent.xml

Tableau 1.1. Pfade der Schnittstelle swissdec-Adapter - sM-Client

PathID	Description
PATH_ELM_IN	• sont au format standard swissdec : XML (validés par rapport à un schéma) • ont comme nom de fichier : [”Tax”|”TaxAtSource”]_DeclarationId_ [”MIXD”|”SPLT”]_Timestamp.zip • les notifications utilisées seront déplacées/ supprimées par le sM-client
PATH_ELM_OUT	• Des réponses ne seront créées que pour les décomptes de l'impôt à la source (résultat des décomptes de l'impôt à la source) • sont au format standard swissdec : XML (validés par rapport à un schéma); zippés • ont comme nom de fichier : DeclarationId.zip • les notifications utilisées seront déplacées par l'adaptateur swissdec • les notifications non utilisées seront déplacées par l'adaptateur swissdec
PATH_ELM_SENT	• Résultats des décomptes de l'impôt à la source envoyés • sont au format standard swissdec : XML (validés par rapport à un schéma); zippés • ont comme nom de fichier : DeclarationId.zip • seront lus par le sM-client afin de pouvoir clôturer le processus
PATH_ELM_FAILED_TO_RX	• Attestation de salaire et décompte de l'impôt à la source, erreur à la réception • les réponses de l'adaptateur swissdec seront également inscrites • non disponible dans chaque cas
PATH_ELM_FAILED_TO_TX	• Résultats des décomptes de l'impôt à la source, erreur à l'envoi

Tableau 1.2. Chemin d'accès de l'interface de l'adaptateur swissdec - sM-client

Veuillez consulter [DETAILSPEZ] pour les spécifications complètes sur les interfaces.

1.4. Références

- [ENDRECREQ] exigences swissdec – destinataire final
- [DETAILSPEZ] spécification détaillée - adaptateur swissdec

2. Exigences liées au fonctionnement

L'adaptateur swissdec se compose de deux applications Java. Les deux applications (réception et intégration) sont implémentées comme applications web Java et nécessitent un conteneur de servlets Java. Le package d'installation contient un conteneur Apache Tomcat préconfiguré et peut de ce fait être facilement décompressé.

L'application-réception implémente le protocole swissdec et doit pouvoir être accessible depuis l'internet via HTTPS. Typiquement, celle-ci est installée dans le *DMZ*.

L'application-intégration assure la communication avec le *sM-Client* ette interface est basée sur le système de fichiers. Cela signifie que l'application-intégration et le *sM-Client* ont besoin d'un système de fichiers commun. L'application-intégration peut être installée aussi bien sur le même système que l'application-réception que sur un système dédié ou sur le système du *sM-Client*.

La communication entre les deux applications se produit au moyen des protocoles HTTP et SOAP. Il s'agit de s'assurer qu'une telle connexion puisse être ouverte depuis l'application-réception (client, initie toujours la connexion) vers l'application-intégration.

2.1. Exigences du système

2.1.1. Plates-formes supportées

L'adaptateur swissdec est une simple application Java. Il fonctionne sur toutes les plates-formes qui supportent la version 1.6 de Java. Plates-formes testées et supportées:

- Windows 2008 Serveur 64 bits
- Windows 7
- Ubuntu 12.04 LTS

2.1.2. Démarrage comme service

En raison de l'architecture synchrone de swissdec, l'adaptateur swissdec doit fonctionner en permanence. Afin de garantir ce fonctionnement permanent, l'adaptateur swissdec devrait être configuré comme Service (sur Windows) ou comme Script au démarrage (sur Unix).

2.1.3. CPU

Les exigences relatives au CPU sont faibles. L'utilisation de processeurs multi-cœurs est recommandée.

Note

Une problématique due à l'architecture swissdec se pose : le distributeur de tous les destinataires finaux doit attendre avant que la quittance soit envoyée aux clients. C'est pourquoi swissdec a spécifié les exigences relatives à la performance suivantes :

- [ENDRECREQ], chapitre 3.10 : Une notification de salaire avec 100 personnes devrait être traitée en moins de 20 secondes.
- [ENDRECREQ], chapitre 3.10 : Une notification de salaire avec 100 personnes doit pouvoir être traitée en une minute.
- [ENDRECREQ], chapitre 3.10 : Une notification de salaire avec 2 000 personnes devrait être traitée en une minute.

2.1.4. Mémoire vive (RAM)

Un espace d'au moins 1 gigaoctet (Go) devrait être réservé pour l'adaptateur swissdec. Cela permet de recevoir des notifications jusqu'à environ 6 000 salariés. Au cas où des notifications plus importantes devaient être reçues, nous recommandons de réserver un espace de 4 gigaoctets. Cela permet de recevoir des notifications jusqu'à environ 20 000 salariés.

2.1.5. Disque dur

L'installation nécessite environ 150 mégaoctets (Mo). L'espace nécessaire sur le disque dur pour la durée de fonctionnement varie de manière significative et dépend du nombre et de la taille des notifications reçues. Comme valeur initiale, nous recommandons un espace de 1 gigaoctet sur le disque dur.

2.1.6. Limitations de tailles

La mémoire vive (RAM) disponible, ou la mémoire attribuée à la machine virtuelle Java, limite la taille des notifications. Afin de pouvoir vérifier ou créer la signature des notifications, la notification globale doit être sauvegardée dans la mémoire vive.

Note

- La machine virtuelle Java 32 bits est limitée à 1,6 Go
- Une notification avec 6 000 personnes nécessite une mémoire d'environ 1 Go
- Une notification avec 20 000 personnes nécessite une mémoire d'environ 4 Go

2.1.7. Réseau

L'adaptateur swissdec démarre une extrémité d'un service web, qui doit être accessible depuis l'internet. Un chemin d'accès depuis l'internet vers l'adaptateur swissdec doit également être créé. En outre, les éléments suivants doivent être configurés :

- URL: Pour pouvoir être accessible depuis l'internet, l'adaptateur swissdec a besoin de deux URL. L'association swissdec stipule qu'il faut attribuer une adresse unique pour chaque domaine (retenues à la source, taxes). Plus d'informations à ce sujet à la Section 2.1.7.2, « Proxy inverse ».

- Protocoles SSL/TLS: Afin de garantir la connexion, l'association swissdec stipule des protocoles SSL/TLS avec une authentification des clients : outre le HTTPS « normal » un certificat est demandé aux clients puis vérifié. Plus d'informations à ce sujet à la Section 2.1.7.3, « SSL/TLS ».

- Pare-feu: L'adaptateur swissdec n'ouvre aucune connexion dans l'internet. C'est pourquoi seul le chemin d'accès détaillé doit être configuré. La connexion peut être limitée au distributeur. Plus d'informations à ce sujet à la Section 2.1.7.1, « Pare-feu ».

2.1.7.1. Pare-feu

Des connexions détaillées doivent être autorisées sur l'adaptateur swissdec. L'adaptateur swissdec démarre par défaut sur le port 8080. Voir à ce sujet le Chapitre 6, *Référence des configurations*.

Note

L'adaptateur swissdec étant utilisé par un client (distributeur), la connexion détaillée peut être limitée à son adresse IP. Pour le distributeur effectif, l'adresse IP est:

- 194.11.148.11

Le distributeur de test, les adresses sont:

- 193.247.121.163

  193.247.102.165

2.1.7.2. Proxy inverse

Au cas où un proxy inverse est en place, les URL suivantes doivent être accessibles depuis l'extérieur:

```
http://<HOST>:<PORT>/webservice/tax/SalaryDeclarationConsumerService
```

```
http://<HOST>:<PORT>/webservice/tas/SalaryDeclarationConsumerService
```

2.1.7.3. SSL/TLS

L'association swissdec stipule que, pour le destinataire final, outre le HTTPS « normal » le client (distributeur) doit s'authentifier. Ceci afin de protéger le destinataire final. En principe, le destinataire final (utilisateur) décide comment et où planifier le protocole SSL/TLS avec authentification mutuelle. Les solutions suivantes peuvent alors être envisagées : La planification survient sur le serveur d'entrée ou le pare-feu.

- La planification survient sur le Tomcat de l'adaptateur swissdec. Vous trouverez la configuration concernée en annexe.

Les certificats pour les deux solutions sont consultables via le support *sM-Client* (http://jira.ctp-consulting.com).

2.1.8. Temps système

Il est important que le temps système du système sur lequel fonctionne la réception de l'adaptateur soit correct, car un horodatage sera généré au niveau du protocole Web Service Security. Si l'heure du distributeur et celle du destinataire final diffèrent, les notifications seront refusées. Il est recommandé d'actualiser automatiquement l'horloge au moyen du protocole d'heure réseau (NTP).

2.2. Structure de répertoire

Le tableau suivant montre la structure de répertoire d'une application installée (réception ou intégration) de l'adaptateur swissdec:

Répertoire	**Description**
bin	Scripts pour le démarrage et l'arrêt de l'adaptateur swissdec
conf	Fichiers de configuration
derbydb	Banque de données insérée pour l'adaptateur swissdec, application-intégration uniquement
jce	Modules de cryptographie Java (Java Crypto Extensions) pour Oracle/Sun et kit JDK (Java Development Kit) pour IBM de la version 1.6.
lib	Bibliothèques Java supplémentaires
logs	Fichiers log (identification)
temp	Fichiers temporaires pour la durée de fonctionnement
webapps	Les applications web pour l'adaptateur swissdec
work	Fichiers temporaires pour la durée de fonctionnement

Tableau 2.1. swissdecAdapter.zip

2.3. Migration

La version 2.0 de l'adaptateur swissdec étant la première version effective, une nouvelle installation du participant pilote est aussi recommandée. Une migration de l'environnement pilote n'est pas envisagée.

3. Installation

L'adaptateur swissdec est une application web Java. L'adaptateur doit être installé dans un espace où l'internet est accessible: typiquement le*DMZ*. Afin de pouvoir faire fonctionner l'adaptateur swissdec, les exigences du système établies au Chapitre 2, *Exigences liées au fonctionnement* doivent être satisfaites.

L'adaptateur swissdec est mis à disposition en tant que système d'archivage (fichiers ZIP) fonctionnant de manière autonome.

3.1. Vérification des conditions préalables

Veuillez vérifier, avant l'installation, les systèmes décrits au chapitre 2.1 Systemvorausetzungen et procédez à des modifications, au besoin.

Un kit JDK (Java Development Kit) de la version 1.6 doit être installé sur le système.

3.2. Décompresser un package

L'adaptateur swissdec est livré dans un fichier ZIP. Pour installer l'adaptateur, il s'agit de décompresser le fichier ZIP dans le répertoire d'installation souhaité. L'archive ZIP contient un répertoire racine« swissdecAdapter-<version> ». Ce répertoire ne doit donc pas être créé en complément.

3.3. Droits pour l'exécution (Unix seulement)

Lorsque vous installez l'adaptateur swissdec sous Unix, les étapes supplémentaires suivantes sont impératives. Elles sont nécessaires pour les deux applications (réception et intégration).

1. Changez dans le répertoire « <SWISSDECADAPTER_HOME>/bin »

2. Changez les droits du script sur « Exportable »

```
chmod +x *.sh
```

3.4. Configuration de l'environnement

Les variables d'environnement suivantes doivent être implémentées:

- JAVA_HOME – Répertoire d'installation du JDK 1.6 / 1.7

Windows

```
set JAVA_HOME=C:\Program Files\Java\jdk1.6.0_09
```

UNIX (varie selon la console utilisée ; cet exemple s'applique à la console bash)

```
export JAVA_HOME=/usr/java/jdk1.6.0_09
```

Normalement, cette variable d'environnement est implémentée lors de l'installation du kit JDK, aussi bien sous Windows que sous UNIX.

3.5. Installation du module JCE Java

En raison de la législation américaine, il est interdit d'inclure à la livraison du package d'installation le système Oracle dans Java Tools (outils Java) pour la « cryptographie illimitée » L'adaptateur swissdec dépendant de cette puissante cryptographie, les fichiers « Unlimited Strength Java(TM) Cryptography Extension Policy Files » doivent par la suite être installés. Le package de l'adaptateur swissdec contient ces fichiers pour la version 1.6 dans les répertoires jce/sun

- jce/sun
- jce/ibm

Pour installer ces fichiers, copiez tous les fichiers dans le répertoire souhaité (implémentation spécifique kit JDK) dans le répertoire

- <JDK_HOME>/jre/lib/security

Ces données peuvent être obtenues par téléchargement auprès du fabricant de l'implémentation JDK (Oracle/Sun ou IBM).

3.6. Application-réception

3.6.1. Configuration Tomcat

Le conteneur de servlets inclus à la livraison « Tomcat » peut être démarré avec la configuration livrée, à quelques exceptions près. Veuillez vérifier que le port standard 8080 n'est pas déjà utilisé sur l'ordinateur. S'il est déjà utilisé, dans le fichier <SWISSDECADAPTER_HOME>/conf/server.xml à la section "Connecteur" veuillez modifier la valeur définie pour « port » en indiquant une valeur libre.

```
<Connector port="8080" protocol="HTTP/1.1"
        connectionTimeout="20000"
        redirectPort="8443"/>
```

Exemple 3.1. Standardconnector- Konfiguration Tomcat

3.6.2. Configuration de la réception

Dès que l'archive ZIP est décompressée, vous devez ajuster la configuration. Vous trouverez une liste complète de tous les paramétrages possibles au Chapitre 6, *Référence des configurations* La section suivante décrit la configuration obligatoire qui doit être effectuée dans le fichier <SWISSDECADAPTER_HOME>/conf/swissdecAdapter.properties.

Option	**Description**
userAgent.institutionName	Nom descriptif de l'institution (p.e. „KSTV Bern“)
institution.tas.id	Information technique, pour quelles institutions sont capable de recevoir des messages d'impôt à la source (p.e. „BE“, „ZH“, „GE“, ...). DOIT être configuré correctement. Sinon la transmission est refusé.
institution.tax.id	Information technique, pour quelles institutions sont capable de recevoir des messages pour les certificat de salaire (p.e. „BE“, „ZH“, „GE“, ...). DOIT être configuré correctement. Sinon la transmission est refusé.
salarydeclaration.service.host	L'hôte sur lequel fonctionne l'intégration de l'adaptateur swissdec.
salarydeclaration.service.port	Le port sur lequel fonctionne l'intégration de l'adaptateur swissdec.

Tableau 3.1. swissdec-Adapter Receiver configuration de base

3.6.3. Configuration de la sécurité

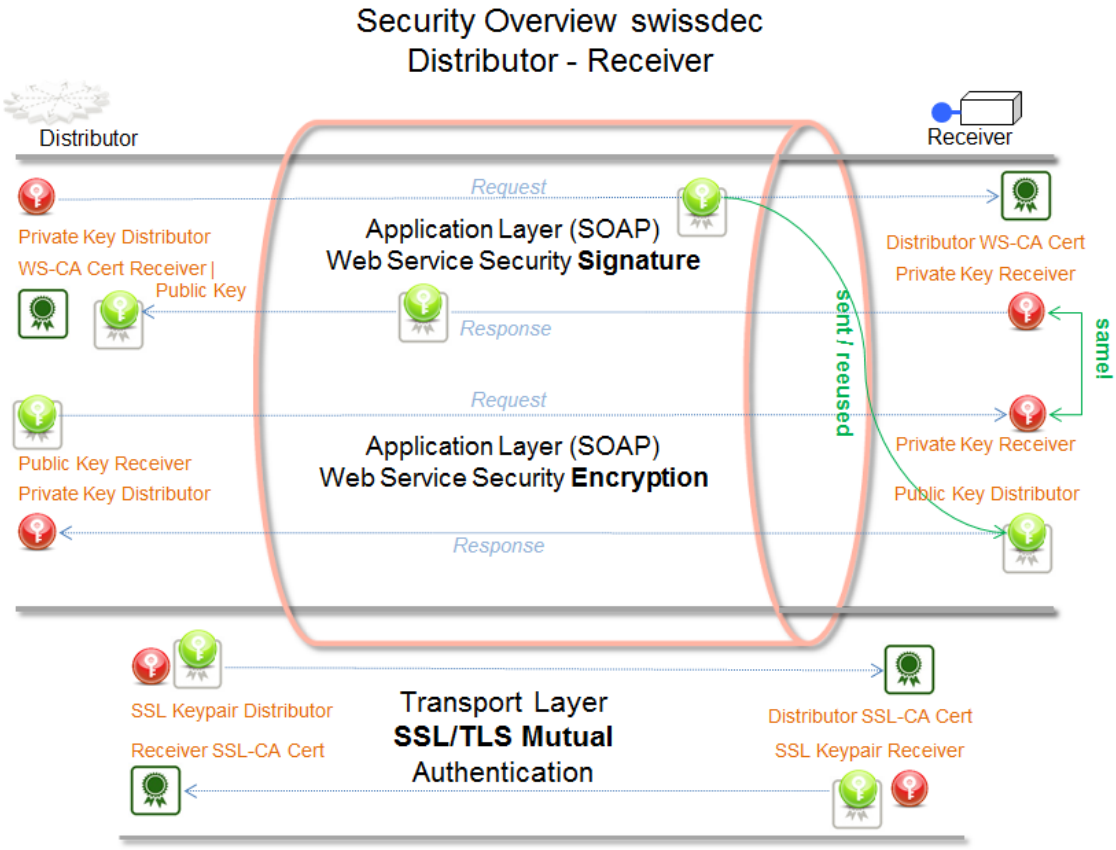


Figure 3.1. Security Overview

	Clé privée (Private Key)
	Certificat avec clé publique (Public Key). Dans ce qui suit, les "clés publiques" (public Key) seront identifiées avec le certificat qui contient la clé publique.
	Certificat CA

Tableau 3.2. Security Overview

3.6.3.1. Webservice Security

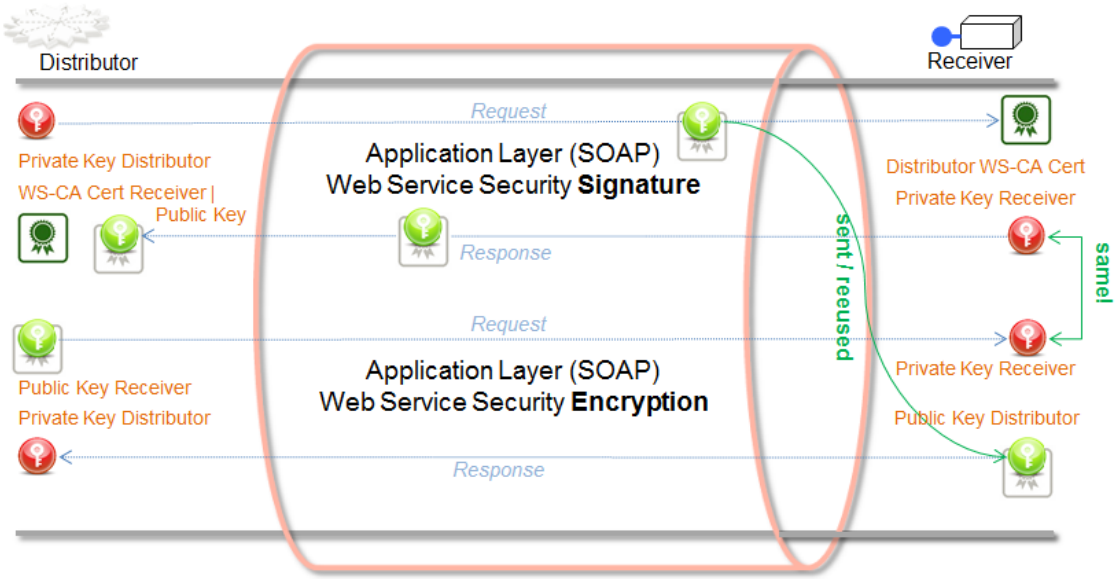


Figure 3.2. Webservice Security Overview

Signature

Requête	Le client (distributeur swissdec) signe la requête avec sa clé privée (Private Key) et envoie sa clé publique (Public Key) avec la requête. Sur la page du serveur (adaptateur swissdec), la clé publique envoyée avec la requête est vérifiée par rapport au certificat CA swissdec, de même que la signature. Au niveau du serveur, seul le certificat CA swissdec est nécessaire pour vérifier la signature.
Réponse	L'adaptateur swissdec signe la réponse avec sa clé privée. Le distributeur swissdec doit connaître sa clé publique, ou le certificat CA.

Tableau 3.3. Webservice Security Signature

Pour le processus de signature du protocole Webservice Security, le certificat CA du client ainsi que sa propre paire de clés (clé privée et clé publique) seront également nécessaires sur la page du serveur.

Encodage

Request	Le client (distributeur swissdec) encode la requête avec la clé publique (Public Key) du destinataire. Sur la page du serveur (adaptateur swissdec), la requête est déchiffrée avec la clé privée correspondante.
Response	L'adaptateur swissdec encode la réponse avec la clé publique du distributeur swissdec qui a été envoyée avec la requête pour la signature du protocole Webservice Security. Il est ainsi garanti que seul le propriétaire de la clé privée correspondante peut déchiffrer la réponse.

Tableau 3.4. Webservice Security Encryption

Pour le processus d'encryptage du protocole Webservice Security, seule la clé privée du destinataire, qui est identique à celle nécessaire pour la signature Webservice Security, est nécessaire sur la page du serveur.

Configuration

Il ressort de l'illustration 3.2 que deux éléments pour le protocole Webservice Security sont nécessaires sur la page du serveur (adaptateur swissdec):

- Certificat CA swissdec
- Paire de clés (clé privée et clé publique) du destinataire

Le certificat CA devant seulement pouvoir être reconnu, il n'est pas configuré de manière explicite. Il suffit qu'il soit disponible dans le *Keystore* configuré. La clé privée du destinataire doit néanmoins être adressée explicitement dans le *Keystore* es options de configuration suivantes (swissdecAdapter.properties) commandent le comportement de l'adaptateur swissdec pour le protocole Webservice Security.

Option	**Description**
org.apache.ws.security.crypto.merlin.file	Chemin d'accès vers le *Keystore* avec les certificats pour le protocole Webservice Security.
wss4j.signatureUser	Alias du certificat dans le *Keystore* , dont la clé permet de signer la réponse (Private Key).
wss4j.privateKeyPassword	Mot de passe pour la clé privée (wss4j.signatureUser).
org.apache.ws.security.crypto.merlin.keystore.password	Mot de passe pour le *Keystore* .
noSecurity	Pour éteindre la sécurité du web service. lorsque vous utilisez un application firewall.

Tableau 3.5. swissdecAdapter Webservice Security Konfiguration

Note

Les certificats effectifs peuvent être commandés via le support *sM-Client* Support (http://jira.ctp-consulting.com).

Avertissement

Dès que les certificats Webservice Security sont installés pour la production, aucune transmission provenant aussi bien des "refapps" (reference application) que des outils de test ne sera acceptée. Cela est dû au fait que les signatures des notifications ne peuvent plus être vérifiées, le distributeur effectif ayant utilisé des certificats d'une autre autorité de certification (CA).

3.6.3.2. Transport Layer (SSL/TLS)

Le client crée une connexion vers le serveur. Habituellement, le serveur s'authentifie d'abord par rapport au client avec un certificat. Ensuite, soit le client envoie au serveur un nombre aléatoire secret encodé avec la clé publique du serveur, soit les deux parties prévoient un secret commun avec la méthode de l'échange de clés Diffie-Hellman. Une clé cryptographique sera alors déduite du secret. Cette clé sera par la suite utilisée pour encoder toutes les informations relatives à la connexion à l'aide d'une procédure d'encodage symétrique et pour garantir l'intégrité et l'authenticité des informations au moyen d'un code d'authentification de message.

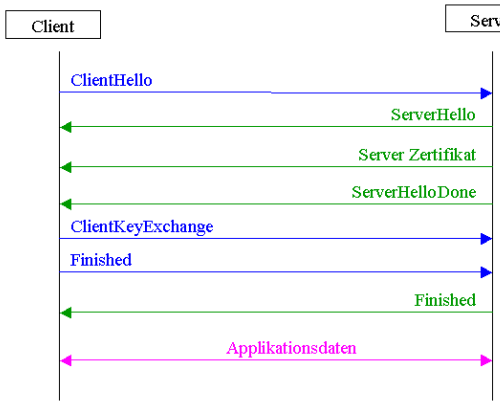


Figure 3.3. SSL Handshake

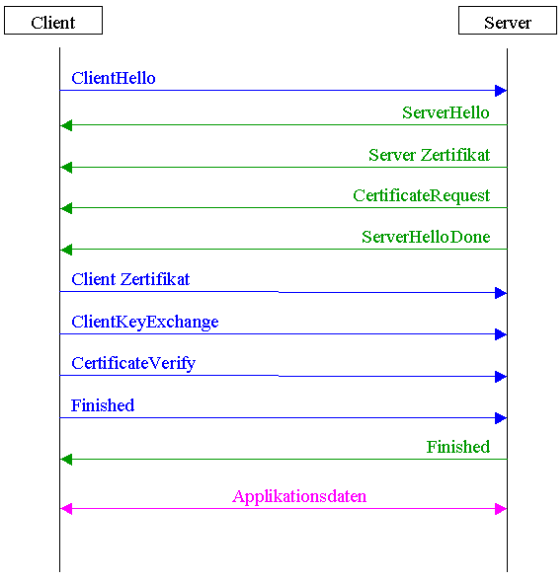


Figure 3.4. Protocole Handshake
SSL avec authentification mutuelle

Dans le cadre de l'authentification mutuelle, le serveur exige également du client qu'il s'authentifie avec un certificat. Cette exigence est stipulée dans les normes swissdec afin de garantir que toutes les parties se font mutuellement confiance.

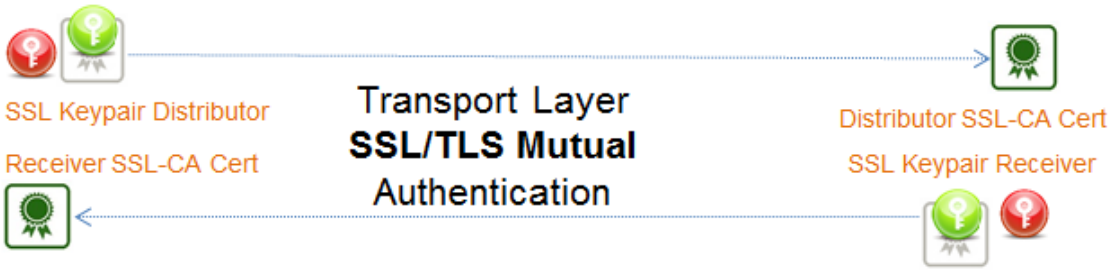


Figure 3.5. Transport Layer Security Overview

Pour simplifier, il est évident que les deux côtés (client/distributeur swissdec, serveur/adaptateur swissdec) devront utiliser aussi bien une paire de clés (clé privée avec la clé publique qui y correspond) pour s'identifier qu'un certificat CA pour la vérification.

La configuration des protocoles SSL/TLS pour l'adaptateur swissdec se trouve dans le fichier « conf/server.xml ». Si une planification devait être effectuée sur l'adaptateur, un exemple de configuration se trouve dans ce même fichier.

```
<Connector port="8443" protocol="HTTP/1.1"
        connectionTimeout="20000"
        scheme="https" secure="true" SSLEnabled="true"
        keystoreFile="[path]/server.jks" keystorePass="keystore pass"
        truststoreFile="[path]/truststore.jks" truststorePass="truststore pass"
        clientAuth="true" sslProtocol="TLS"/>
```

Exemple 3.2. Configuration connecteur Tomcat pour la planification SSL avec authentification mutuelle

Option	**Description**
port	Le port TCP sur lequel le serveur écoute.
keystoreFile	Le chemin d'accès vers le fichier *Keystore* . Relatif au répertoire <SWISSDECADAPTER_HOME>.
keystorePass	Mot de passe pour le fichier *Keystore*.
truststoreFile	Le chemin d'accès vers le fichier Truststore. Relatif au répertoire
eFile	<SWISSDECADAPTER_HOME>
truststorePass	Mot de passe pour le fichier Truststore.
clientAuth	La valeur "true" exige une authentification du client (authentification mutuelle).

Tableau 3.6. Configuration du protocole Transport Layer de l'adaptateur swissdec

Note

Keystore (avec la paire de clés) et le fichier Truststore (avec le certificat CA du distributeur swissdec) seront livrés dans un seul fichier pour simplifier. Ainsi, les deux données sont identiques!

Les certificats effectifs peuvent être commandés via le support sM-client (http://jira.ctp-consulting.com). En outre, le nom de l'hôte (entrée DNS [système de noms de domaine]) doit être communiqué et être accessible depuis l'internet avec l'installation de l'adaptateur swissdec.

Avertissement

Le Tomcat (conteneur de servlet de l'adaptateur swissdec) est limité dans la mesure où le mot de passe du fichier Keystore doit être identique au mot de passe de la clé privée qui y est contenue.

3.7. Application-intégration

3.7.1. Configuration Tomcat

Le conteneur de servlets inclus à la livraison « Tomcat » peut être démarré avec la configuration livrée, à quelques exceptions près. Veuillez vérifier que le port standard 9090 n'est pas déjà utilisé sur l'ordinateur. S'il est déjà utilisé, dans le fichier <SWISSDECADAPTER_HOME>/conf/server.xml à la section "Connecteur", veuillez modifier la valeur définie pour « port » en indiquant une valeur libre. Lorsqu'un port est modifié à cet emplacement, n'oubliez pas que la valeur pour "salarydeclaration.service.port"dans le fichier <SWISSDECADAPTER_HOME>/conf/swissdecAdapter.properties doit aussi être ajustée.

```
<Connector port="9090" protocol="HTTP/1.1"
        connectionTimeout="20000"
        redirectPort="8443"/>
```

Exemple 3.3. Connecteur standard - Configuration Tomcat

3.7.2. Configuration de l'application-intégration

Dès que l'archive ZIP est décompressée, vous devez ajuster la configuration. Vous trouverez une liste complète de tous les paramétrages possibles au Chapitre 6, *Référence des configurations* La section suivante décrit la configuration obligatoire qui doit être effectuée dans le fichier <SWISSDECADAPTER_HOME>/conf/swissdecAdapter.properties.

Option	Description
released.filesystem.parent.xml	Chemin à l'entrée du message (PATH_ELM_IN). Indiquez le chemin absolut, s.v.p. Doit être en correspondence avec le sM-Client.
failed.filesystem.parent.xml	Chemin au "failed to receive" (PATH_ELM_FAILED_TO_RX). Indiquez le chemin absolut, s.v.p. Doit être en correspondence avec le sM-Client.
result.filesystem.parent.xml	Chemin à la sortie du message (PATH_ELM_OUT). Indiquez le chemin absolut, s.v.p. Doit être en correspondence avec le sM-Client.
sent.filesystem.parent.xml	Chemin au "sent" (PATH_ELM_SENT). Indiquez le chemin absolut, s.v.p. Doit être en correspondence avec le sM-Client.
undeliverable.filesystem.parent.xml	Chemin au "failed to send" (PATH_ELM_FAILED_TO_TX). Indiquez le chemin absolut, s.v.p. Doit être en correspondence avec le sM-Client.
institution.tas.id	Information technique pour quelles institutions des transmission d'impôt à la source sont possible (p.e. „BE“, „ZH“, „GE“, ...). DOIT être configuré correctement. Sinon les transmission sont refusées.
institution.tax.id	Technische Angabe, für welche Institution Lohnausweise empfangen werden (zum Beispiel „BE“, „ZH“, „GE“, ...). MUSS richtig konfiguriert sein, da sonst Meldungen abgelehnt werden

Tableau 3.7. Integration swissdec-Adapter configuration de base

3.8. Configuration de l'identification

La configuration pour l'identification se trouve dans le fichier <SWISSDECADAPTER_HOME>/lib/log4j.xml. La configuration contenue dans le package établit 3 fichiers d'identification.

Fichier	Description
catalina.out	Identification du conteneur de servlet (Tomcat)
access.log	Résultats spécifiques, par exemple notifications détaillées, fenêtre de maintenance, etc.
swissdecAdapter.log	Identification de l'adaptateur swissdec

Tableau 3.8. Fichiers log

Par défaut, ces 3 fichiers sont inscrits dans le répertoire <SWISSDECADAPTER_HOME>/logs/ et un "roulement" est effectué quotidiennement.

Pour plus d'informations, veuillez consulter le site internet suivant: http://wiki.apache.org/logging-log4j/Log4jXmlFormat

3.9. Fenêtre de maintenance

Car les transmissions sur la plateforme swissdec sont synchrones, les clients voient quelles destinataires sont atteignables ou non. Il est possible d'annoncer des interruptions de fonctionnement prévues au moyen de la fenêtre de maintenance. On devrait planifier ceci à préférence entre 20:00 et 06:00 les jours de travail ou le week-end. Comme ça les clients sont informés avec un message au lieu d'une erreur. Pour enregistrer une fenêtre de maintenance, procédez comme suit:

1. Créez un fichier XML « PlannedMaintenance ». Vous trouverez un modèle (PlannedMaintenance.xml) dans le répertoire <SWISSDECADAPTER_HOME>/conf

2. Sauvegardez ce fichier dans le répertoire « maintenance.filesystem.parent.xml » de l'application-intégration de l'adaptateur swissdec. Le nom du fichier n'a aucune incidence ; l'extension du fichier doit être ".xml".

3. La fenêtre de maintenance sera signalée au prochain Ping du distributeur. Accessibilité du destinataire est testé par le distributeur cycliquement (toutes les 30 minutes). Pour ceci l'opération "PingConsumer" est éxécutée. L'accessibilité est confirmé par le destinataire. Dans ce processus le destinataire peut configurer des fenêtres de maintenance dans sa réponse.

4. Dès que la fenêtre de maintenance est passée, le fichier XML "PlannedMaintenance" est automatiquement supprimé.

Note

- Le nom du fichier n'a aucune incidence, l'extension du fichier doit obligatoirement être ".xml".

- Les pages "Start" et "End" dans le fichier XML "PlannedMaintenance" sont du type xs:dateTime. Cela signifie que les fuseaux horaires, ainsi que les heures d'été et d'hiver, doivent y être contenus.2013-08-31T13:40:47.0Z : Le Z désigne l'UTC
  - 2014-01-31T13:40:47.0+01:00 : UTC +1 heure, heure de l'Europe Centrale (heure d'hiver)
  - 2013-08-31T13:40:47.0+02:00: UTC +2 heures, heure de l'Europe Centrale (heure d'été)
- Les notifications seront transmises jusqu'à la comptabilité des salaires. Veuillez sélectionner le texte approprié dans les 3 langues (allemand, français et italien).
- Plusieurs fichiers XML « PlannedMaintenance » peuvent être classés dans le répertoire "maintenance.filesystem.parent.xml". L'adaptateur swissdec notifiera toujours le fichier suivant au distributeur ; et au cours du fonctionnement, le fichier sera automatiquement supprimé ou le fichier suivant sera notifié.

Exemple d'un fichier XML "PlannedMaintenance" :

```
<?xml version="1.0" encoding="UTF-8"?>
<PlannedMaintenance xmlns="http://www.itserve.ch/step/2.0/maintenance">
   <Start>2013-08-31T13:40:47.0+01:00</Start>
   <End>2013-09-01T13:40:47.0+01:00</End>
   <Messages>
      <Message language="de">Beschreibung Deutsch</Message>
      <Message language="fr">Beschreibung Französisch</Message>
      <Message language="it">Beschreibung Italienisch</Message>
   </Messages>
</PlannedMaintenance>
```

3.10. Remarque conclusive

Assurez-vous que les deux applications de l'adaptateur swissdec redémarrent automatiquement après une réinitialisation du système. Plus d'informations à ce sujet au Chapitre 5, *Démarrage de l'adaptateur*.

4. Test de l'installation

Pour pouvoir vérifier l'installation, swissdec met à disposition un outil de test. Il s'agit d'un simple service web-client, avec lequel les attestations de salaires et les décomptes de l'impôt à la source peuvent être envoyées au format V4 Draft swissdec.

4.1. Installation

L'outil de test est livré dans un fichier ZIP et doit seulement être décompressé. Une installation Java sera nécessaire pour l'exécution.

Avertissement

L'outil de test étant encodé conformément à swissdec, le JCE (module de cryptographie Java) doit être installé pour l'installation Java. Plus d'informations à ce sujet à la Section 3.5, « Installation du module JCE Java ».

4.2. Configuration

Avant de pouvoir procéder au test, les fichiers

- Config-TAS.xml
- Config-TAX.xml

doivent être adaptés. Il s'agit de fichiers Properties au format XML.

Option	Description
endpointURL	L'adresse de l'adaptateur swissdec à tester.
wssEncryptionCert	Le certificat utilisé pour l'encodage de la notification (clé publique de l'adaptateur swissdec).
sigrootcert	Le certificat utilisé pour vérifier la signature de la réponse (clé publique de l'adaptateur swissdec).
sslcert	Certificat avec la clé publique pour la clé privée SSL
sslkey	Clé privée SSL pour l'authentification client
sslpartnercacert	Certificat CA pour la vérification du certificat de serveur SSL/TLS.

Tableau 4.1. TestTool Konfiguration

Pour plus d'informations concernant la sécurité, veuillez consulter la Section 3.6.3, « Configuration de la sécurité ».

Note

La configuration incluse à la livraison convient pour la configuration par défaut de l'adaptateur swissdec.

L'option « sslpartnercacert » ne sera nécessaire qu'avec un HTTPS activé.

Les options « sslcert » et « sslkey » ne seront nécessaires qu'avec une authentification mutuelle activée.

4.3. Exécution des tests

Pour procéder à un test, le script batch ou shell correspondant sera exécuté.

Note

Les tests les plus simples sont:

- INTG_001_Smoke_TAS
- INTG_002_Smoke_TAX

5. Démarrage de l'adaptateur

5.1. Démarrage manuel

Les deux adaptateurs swissdec peuvent être démarré/arrêté avec les commandes suivantes dans la console:

Windows

```
<SWISSDECADAPTER_HOME>/bin/startup.bat
```

```
<SWISSDECADAPTER_HOME>/bin/shutdown.bat
```

Unix

```
<SWISSDECADAPTER_HOME>/bin/startup.sh
```

```
<SWISSDECADAPTER_HOME>/bin/shutdown.sh
```

Note

Avant le premier démarrage, veuillez procéder à la configuration décrite au chapitre Adapter Konfiguration.

5.2. Démarrage comme service Windows

Pour installer le Tomcat en tant que service Windows, procédez comme suit. Prenez en considération que les pas suivants doivent être fait pour chaqu'un des deux applications (receiver et integration).

1. Arrêtez l'adaptateur swissdec s'il est en cours de fonctionnement.
2. Ouvrez la ligne de commandes et parcourez-la jusqu'au répertoire <SWISSDECADAPTER_HOME>/bin/

   Vous devriez maintenant voir entre autres les trois fichiers suivants :

   - service.bat
   - tomcat6.exe
   - tomcat6w.exe
3. Effectuez les commandes suivantes :

```
service.bat install
tomcat6w.exe //ES//
```

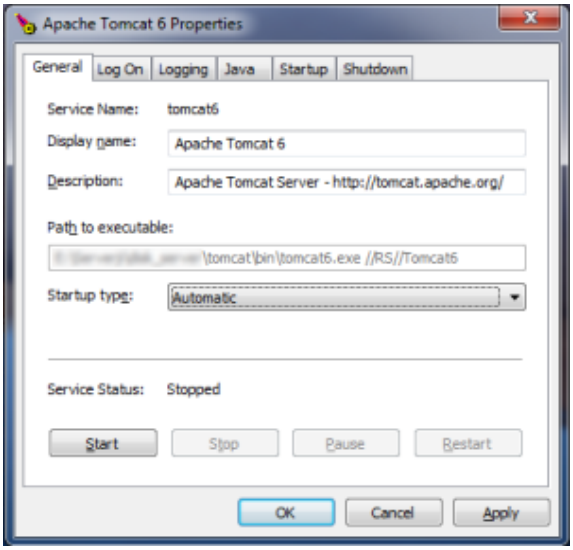


Figure 5.1. tomcat6w.exe, Tomcat Service Properties

Assurez que le valeur pour "Startup" est automatic.

4. Dans l'onglet "Java", augmentez la valeur "Initial memory pool" à 256 Mo et "Maximum memory pool" à au moins 1 024 Mo.

5. Complétez les « options Java » comme suit :

```
-XX:MaxPermSize=256m
-Dproperties.url=file:///C:/.../swissdecAdapter/conf/swissdecAdapter.properties
-Dderby.system.home=C:\...\swissdecAdapter\derbydb
```

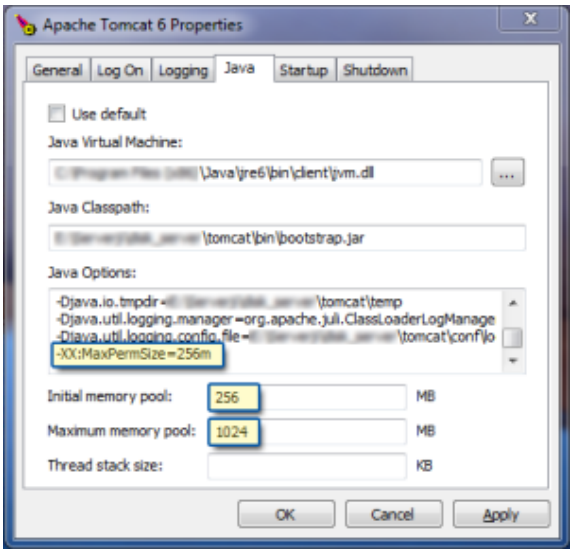


Figure 5.2. Tomcat Service Java Properties

Note

N'oubliez pas que les options "properties.url" et "derby.system.home" doivent être adaptées pour votre environnement.

- properties.url: indique <SWISSDECADAPTER_HOME>/conf/swissdecAdapter.properties
- derby.system.home: indique <SWISSDECADAPTER_HOME>/derbydb

6. Le service "Tomcat6" devrait à présent être installé. Vérifiez les paramètres au moyen de la gestion des services Windows.

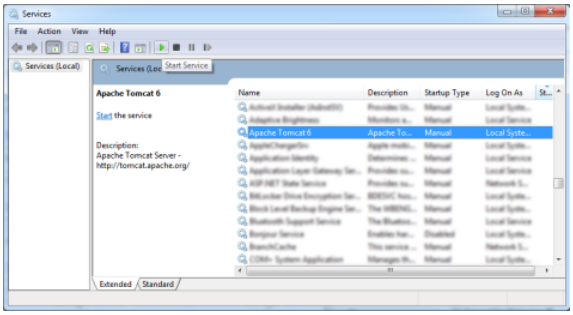


Figure 5.3. Gestion des services Windows

5.3. Unix script-init

Prenez en considération que tous les deux applications (receiver et integration) doivent être démarrées. Dans le répertoire <SWISSDECADAPTER_HOME>/bin/ se trouve un script init.d Skript (tomcat6.sh) pour le Tomcat inclus à la livraison. Vous devez adapter les variables suivantes dans le script:

```
JAVA_HOME=/usr/lib/jvm/java-6-openjdk
TOMCAT_USER=tomcat6
CATALINA_HOME=/opt/swissdecAdapter
CATALINA_PID=$CATALINA_HOME/bin/tomcat6.pid
```

Il est recommandé de déterminer un utilisateur pour l'adaptateur swissdec. Veuillez observer que les utilisateurs des répertoires, qui sont configurés dans le répertoire <SWISSDECADAPTER_HOME>/conf/swissdecAdapter.properties nécessitent des droits de lecture et d'écriture.

```
#!/bin/sh -e
# description: Tomcat6 service
# processname: java

# Get LSB functions
. /lib/lsb/init-functions

export JAVA_HOME=/usr/lib/jvm/java-6-openjdk
export TOMCAT_USER=tomcat6
export CATALINA_HOME=/opt/swissdecAdapter
export CATALINA_PID=$CATALINA_HOME/bin/tomcat6.pid

[ -d "$CATALINA_HOME" ] || { echo "Tomcat requires $CATALINA_HOME."; exit 1; }

case $1 in

   start|stop|run)
   if su $TOMCAT_USER bash -c "$CATALINA_HOME/bin/catalina.sh $1"; then
      log_success_msg "Tomcat $1 successful"
      [ $1 == "stop" ] &amp;&amp; rm -f $CATALINA_PID
   else
      log_failure_msg "Error in Tomcat $1: $?"
   fi
   ;;

   restart)
   $0 start
   $0 stop
   ;;

   status)
   if [ -f "$CATALINA_PID" ]; then
      read kpid &lt; "$CATALINA_PID"
      if ps --pid $kpid 2>&amp;1 1>/dev/null; then
         echo "$0 is already running at ${kpid}"
      else
         echo "$CATALINA_PID found, but $kpid is not running"
      fi
      unset kpid
   else
      echo "$0 is stopped"
   fi
   ;;

esac
exit 0
```

6. Référence des configurations

6.1. Configuration Tomcat

Veuillez consulter la documentation complète relative à la configuration sur le site internet suivant: http://tomcat.apache.org/tomcat-6.0-doc/config/index.html.

6.2. Configuration de la réception

Option	Description
failed.filesystem.parent.xml	Chemin d'accès vers "failed to receive" (PATH_ELM_FAILED_TO_RX). Demande de données de chemin d'accès absolu. Doit correspondre avec le sM-client.
userAgent.institutionName	Nom descriptif de l'organisme (par exemple "KSTV Bern")
institution.tas.id	Données techniques; pour quel organisme les notifications de décomptes de l'impôt à la source sont-elles reçues (par exemple "BE", "ZH", "GE", etc.). DOIT être correctement configuré, sinon les notifications seront rejetées
institution.tax.id	Données techniques; pour quel organisme les attestations de salaire sont-elles reçues (par exemple "BE", "ZH", "GE", etc.). DOIT être correctement configuré, sinon les notifications seront rejetées
tax.accept.ex	Définit si des certificats de salaires pour des personnes résidant à l'étranger sont acceptées (default = false).
salarydeclaration.service.protocol	Le protocole selon lequel fonctionne l'intégration de l'adaptateur swissdec.
salarydeclaration.service.host	L'hôte sur lequel fonctionne l'intégration de l'adaptateur swissdec.
salarydeclaration.service.port	Le port sur lequel fonctionne l'intégration de l'adaptateur swissdec.
salarydeclaration.service.context	Le contexte selon lequel fonctionne l'intégration de l'adaptateur swissdec.
salarydeclaration.service.name	Le nom sous lequel fonctionne l'intégration de l'adaptateur swissdec.
monitoring.enabled	Interrupteur, si le monitoring intégré est activé.
monitoring.user	Nom d'utilisateur pour l'authentification sur le monitoring intégré.

Option	Description
monitoring.pass	Mot de passe pour l'authentification sur le monitoring intégré.
org.apache.ws.security.crypto.merlin.file	Chemin d'accès vers le *Keystore* avec les certificats pour le protocole Webservice Security.
wss4j.signatureUser	Alias du certificat dans le *Keystore* , dont la clé permet de signer les réponses.
wss4j.privateKeyPassword	Mot de passe pour la clé privée (wss4j.signatureUser).
org.apache.ws.security.crypto.merlin.keystore.password	Mot de passe pour le *Keystore*.
noSecurity	Pour désactiver la sécurité des services Web. Par exemple, lorsque vous utilisez un Application Firewall.

Tableau 6.1. swissdec-Adapter Receiver Grundkonfiguration

6.3. Configuration de l'application-intégration

Option	Description
released.filesystem.parent.xml	Chemin d'accès vers l'entrée de la notification (PATH_ELM_IN). Demande de données de chemin d'accès absolu. Doit correspondre avec le sM-client.
failed.filesystem.parent.xml	Chemin d'accès vers "failed to receive" (PATH_ELM_FAILED_TO_RX). Demande de données de chemin d'accès absolu. Doit correspondre avec le sM-client.
result.filesystem.parent.xml	Chemin d'accès vers la sortie de la notification (PATH_ELM_OUT). Demande de données de chemin d'accès absolu. Doit correspondre avec le sM-client.
sent.filesystem.parent.xml	Chemin d'accès vers « sent » (PATH_ELM_SENT). Demande de données de chemin d'accès absolu. Doit correspondre avec le sM-client.
undeliverable.filesystem.parent.xml	Chemin d'accès vers "failed to receive" (PATH_ELM_FAILED_TO_RX). Demande de données de chemin d'accès absolu. Doit correspondre avec le sM-client.
maintenance.filesystem.parent.xml	Chemin d'accès vers le dossier des définitions de la fenêtre de maintenance. Demande de données de chemin d'accès absolu.
monitoring.enabled	Interrupteur, si le monitoring intégré est activé.

Option	Description
monitoring.user	Nom d'utilisateur pour l'authentification sur le monitoring intégré.
monitoring.pass	Mot de passe pour l'authentification sur le monitoring intégré.
commune.splitting	Division des communes activée pour les décomptes de l'impôt à la source. Lorsque la division des communes est activée, le résultat await.result est implicitement considéré comme "faux", car les communes ne peuvent plus donner de réponse.
la.splitting	Division des attestations de salaires activée.
await.result	Des résultats de décomptes de l'impôt à la source sont-ils attendus?
processing.default.hours	Après combien d'heures un éventuel résultat de décompte de l'impôt à la source peut-il être attendu?
housekeeping.days	Durée de conservation des notifications. Après l'utilisation, les notifications seront supprimées de la base de données interne. Ensuite, aucun résultat de décomptes de l'impôt à la source ne pourra plus être requis.

Tableau 6.2. swissdec-Adapter Integration configuration

7. Monitoring

L'adaptateur swissdec peut être contrôlé comme tout autre processus ou service standard. Si l'adaptateur swissdec a été enregistré en tant que service Windows, il est possible d'utiliser la « console Windows Gestion de l'ordinateur » pour vérifier ou modifier l'état du service.

7.1. Monitoring intégré

Les deux applications de l'adaptateur swissdec mettent à disposition des informations d'état via les services Restful.

```
http://<INTEGRATION_HOST>:<INTEGRATION_PORT>/integration/ws/monitoring
```

pour l'integration et

```
http://<RECEIVER_HOST>:<RECEIVER_PORT>/webservice/ws/monitoring
```

pour le receveur. Pour activer le monitoring, vous devez adapter les paramètres suivants dans le <SWISSDECADAPTER_HOME>/conf/swissdecAdapter.properties anpassen:

```
monitoring.enabled = true
monitoring.user = admin
monitoring.pass = admin
```

Avertissement

Assurez-vous que le monitoring de l'application-réception (http://<HOST>:<PORT>/webservice/monitoring) n'est pas disponible depuis l'internet.

Exemple de données du monitoring intégré:

```
<services xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:noNamespaceSchemaLocation="serviceresponse.xsd">
  <service name="SystemProperties">
    <state>OK</state>
    <message>
      <SystemProperties>
        <SystemProperty>
          <Key>java.runtime.name</Key>
          <Value>OpenJDK Runtime Environment</Value>
        </SystemProperty>
        ...
      </SystemProperties>
    </message>
    <runtimeInMs>8</runtimeInMs>
  </service>
  <service name="Database">
    <state>OK</state>
    <message>Last Distributor Ping: </message>
    <runtimeInMs>133</runtimeInMs>
  </service>
  <service name="Configuration">
    <state>OK</state>
    <message>
      <Configuration>
        <ConfigProperty>
          <Key>versioninfo</Key>
          <Value>2.0 (Build xxxxx)</Value>
        </ConfigProperty>
        ...
      </Configuration>
    </message>
    <runtimeInMs>1</runtimeInMs>
  </service>
  <service name="Settings">
    <state>OK</state>
    <message>
      <Configuration>
        <ConfigProperty>
          <Key>distributor.lastping</Key>
          <Value></Value>
        </ConfigProperty>
          ...
      </Configuration>
    </message>
    <runtimeInMs>0</runtimeInMs>
  </service>
  <executionTime>0,142"</executionTime>
</services>
```

8. Recovery-Tool

Avec l'outil de récupération vous pouvez visualiser et éventuellement exporter des informations reçu.

8.1. Démarrage

Une fois que l'outil de récupération est déballé, le programme peut être démarré avec le fichier RecoveryTool.bat (Windows) ou RecoveryTool.sh (Linux). L'outil de récupération est une application de console qui est commandée par le clavier. L'aide dans le programme peut être obtenu par la commande "h".

8.2. Options

Les options de commande suivantes sont toujours disponibles:

Option	Description
h	montre les opérations possibles
q	quitte l'outil de récupération
u	un niveau supérieur dans la structure de menu.

Tableau 8.1. Recovery Tool, options générales

8.2.1. Declarations

Dans ce menu, tous les messages stockés dans la base de données de l'intégration swissdecAdapter peuvent être recherchés et affichés.

8.2.1.1. list | l

Liste de toutes les déclarations. En entrant le numéro entre les crochets, les détails de la déclaration/personne sont représentée.

```
swissdecAdapter RecoveryTool V2.0_2

Running with: Sun Microsystems Inc. 1.6.0_21 (/usr/lib/jvm/jdk1.6.0_21/jre)
Running on: Linux 3.11.0-15-generic (amd64)

Type h or help for more information.

sdArT:~$ declarations
sdArT:~/declarations$ list
found 3 actions. type h to show list.
sdArT:~/declarations/list$ help

[1] TAS  INTG_001_Smoke_TAS_20140130_15201391091643
[2] TAX  INTG_002_Smoke_TAX_20140130_15201391091658
[3] TAX  REGR_001_TaxSplittingBug_20140130_15211391091680

[q] quit (Exit RecoveryTool)
[u] up (Go one Up)
sdArT:~/declarations/list$ 2
DECLARATION DETAILS:
Domain:    TAX
DeclarationID:  D0002
RequestID:   123456
ResponseID:   R143e3864462b
Time:    2014-01-30 15:21:03.0
TestCase:   TESTCASE
External state:  ACCEPTED with Warnings
Internal state:  processed
CompanyName:  INTG_002_Smoke_TAX_20140130_15201391091658
Nb. of Persons:  2
Contact:   ContactName
E-Mail:    dko@itserve.ch
Phone:    contactPhone

sdArT:~/declarations/list$
```

8.2.1.2. search | s

Recherche PKID (clée interne) ou DeclarationID

```
swissdecAdapter RecoveryTool V2.0_2

Running with: Sun Microsystems Inc. 1.6.0_21 (/usr/lib/jvm/jdk1.6.0_21/jre)
Running on: Linux 3.11.0-15-generic (amd64)

Type h or help for more information.

sdArT:~$ declarations
sdArT:~/declarations$ search
Enter what you are looking for: D0007
found 9 actions. type h to show list.
sdArT:~/declarations/search$ h

[1] TAS  FUNK_001_TAS_RESULT_PROC_20140131_10331391160800
[2] TAS  FUNK_002_TAS_RESULT_SUCC_20140131_10331391160831
[3] TAS  FUNK_003_TAS_SPLITTING_20140131_10341391160847
[5] TAS  FUNK_005_TAS_NORESULT_20140131_10341391160872
[6] TAS  FUNK_007_DUPLICATE_20140131_10341391160895
[7] TAS  FUNK_008_UNDELIVERABLE_20140131_10351391160904
[8] TAS  FUNK_009_WRITE_ORIGINAL_20140131_10351391160919
[9] TAS  INTG_001_Smoke_TAS_20140131_10351391160937
[47] TAS  INTG_001_Smoke_TAS_20140203_15031391436191

[q] quit (Exit RecoveryTool)
[u] up (Go one Up)
sdArT:~/declarations/search$ 5
DECLARATION DETAILS:
Domain:    TAS
DeclarationID:  D0007
RequestID:   reqId
ResponseID:   R143e7a6617c14a
Time:    2014-01-31 10:34:37.0
TestCase:   PRODUCTIVE
External state:  ACCEPTED with Warnings
Internal state:  contributions delivered
CompanyName:  FUNK_005_TAS_NORESULT_20140131_10341391160872
Nb. of Persons:  7
Contact:   Marcel René Müller
E-Mail:    ComplexEnd2End@xxxxx.ch
Phone:    031 345 23 87

sdArT:~/declarations/search$
```

8.2.2. Recovery

En mode de récupération des déclarations touchées par des erreur peuvent être visualisées et exportées.

8.2.2.1. newTaxRemarks | n

Montre toutes les certificats de salaire qui ont mis les nouveaux remarques. Cette commande peut prendre un moment.

```
swissdecAdapter RecoveryTool V2.0_2

Running with: Sun Microsystems Inc. 1.6.0_21 (/usr/lib/jvm/jdk1.6.0_21/jre)
Running on: Linux 3.11.0-15-generic (amd64)

Type h or help for more information.

sdArT:~$ recovery
sdArT:~/recovery$ newTaxRemarks
found 4 actions. type h to show list.
sdArT:~/recovery/newTaxRemarks$ help

[0] INTG_002_Smoke_TAX_20140130_15201391091658      123.4500.0178.12  ...
[1] INTG_002_Smoke_TAX_20140130_15201391091658      756.9876.5432.10  ...
[2] REGR_001_TaxSplittingBug_20140130_15211391091680  123.4500.0178.12     ...
[3] REGR_001_TaxSplittingBug_20140130_15211391091680  123.4500.0178.12     ...

[q] quit (Exit RecoveryTool)
[u] up (Go one Up)
sdArT:~/recovery/newTaxRemarks$
```

8.2.2.2. splitting | s

Affiche et exportation (option "reexport") tous les declarations affectés par l'erreur de fractionnement.

```
swissdecAdapter RecoveryTool V2.0_2

Running with: Sun Microsystems Inc. 1.6.0_21 (/usr/lib/jvm/jdk1.6.0_21/jre)
Running on: Linux 3.11.0-15-generic (amd64)

Type h or help for more information.

sdArT:~$ recovery
sdArT:~/recovery$ splitting
found 2 actions. type h to show list.
sdArT:~/recovery/splitting$ help

[3] TAX  REGR_001_TaxSplittingBug_20140130_15211391091680
[reexport] reexport 1 found declarations

[q] quit (Exit RecoveryTool)
[u] up (Go one Up)
sdArT:~/recovery/splitting$ reexport
reexport 1 found declarations

THE FILES WILL BE SPLITTED!

do you want to reexport into directory /home/.../.../reexport? this directory is created if not exists! [y|N] y
Please enter your Canton abbreviation [AI | BE | VD | ...] BE
sdArT:~/recovery/splitting$
```

8.2.3. Statistique

Affiche un bref aperçu des déclarations reçues.

```
swissdecAdapter RecoveryTool V2.0_2

Running with: Sun Microsystems Inc. 1.6.0_21 (/usr/lib/jvm/jdk1.6.0_21/jre)
Running on: Linux 3.11.0-15-generic (amd64)

Type h or help for more information.

sdArT:~$ statistics
Total TAX: 2
Total TAX productive: 0
Total TAS: 1
Total TAS productive: 1
sdArT:~$
```

9. Problèmes et solutions

Notification

```
Caused by: org.apache.ws.security.components.crypto.CredentialException: Failed to load credentials.
   Inner Exception: [Keystore was tampered with, or password was incorrect]
```

Mot de passe *Keystore* erroné dans la réception de l'adaptateur swissdec swissdecAdapter.properties (Property ‘org.apache.ws.security.crypto.merlin.keystore.password').

Notification

```
Caused by: java.io.FileNotFoundException: abTst_server.jks (No such file or directory)
```

Le *Keystore* référencé dans la réception de l'adaptateur swissdec swissdecAdapter.properties n'existe pas (Property ‘org.apache.ws.security.crypto.merlin.file')

Notification

```
Caused by: java.security.UnrecoverableKeyException: Cannot recover key
```

Mot de passe de la clé privée erroné dans la réception de l'adaptateur swissdec swissdecAdapter.properties (Property ‘wss4j.privateKeyPassword')

Notification

```
Caused by: java.security.InvalidKeyException: Illegal key size
```

Les modules de cryptographie Java ne sont pas installés.

Notification

```
Caused by: javax.xml.ws.soap.SOAPFaultException: Marshalling Error: Connection refused
 at org.apache.cxf.jaxws.JaxWsClientProxy.invoke(JaxWsClientProxy.java:156)
 at $Proxy205.saveSalaryDeclaration(Unknown Source)
```

L'application-réception n'a aucune connexion avec l'intégration. Veuillez contrôler la configuration suivante dans la réception swissdecAdapter.properties:

```
salarydeclaration.service.protocol = http://
salarydeclaration.service.host = localhost
salarydeclaration.service.port = 9090
salarydeclaration.service.context = integration/ws
salarydeclaration.service.name = SalaryDeclarationServiceFacade
salarydeclaration.service.interface =
ch.itserve.lohnstandard.receiver.shared.bi.ISalaryDeclarationFacade
```

Assurez-vous que la configuration est adaptée à votre infrastructure et qu'une connexion HTTP peut être ouverte sur l'URL configurée à partir de l'application-réception.

A. Annexe

A.1. Documents référencés

[ENDRECREQ] *Directives relatives à la transmission de données salariales.*. Endreceiver Requirements.. swissdec. Version 4 (20130514).

[DETAILSPEZ] *Adaptateur swissdec.*. Spécifications détaillées.. itServe AG. V1.0 (20130430).

A.2. Glossaire

DMZ	Un réseau informatique avec des possibilités d'accès, contrôlées en matière de sécurité, sur le serveur correspondant
Keystore	Un Keystore est une banque de données des clés et des certificats dans un fichier.
sM-Client	Le sM-client offre une fonctionnalité pour l'envoi et la réception de notifications dans différents formats
STEP	Produit de la société itServe AG, destinataire *swissdec*.
swissdec	Label de qualité pour les systèmes de comptabilité des salaires. Standards XML pour la procédure unifiée de communication des salaires (ELM).

B. Exemples

B.1. Configuration

```
                #
# Copyright 1996-2013 itServe AG. All rights reserved.
#
# This software is the proprietary information of itServe AG
# Bern Switzerland. Use is subject to license terms.
#

# RECEIVER INDENTIFICATION
userAgent.institutionName=KSTV Bern
institution.tas.id=BE
institution.tax.id=BE
tax.accept.ex=false

# INTERNAL COMMUNICATION
salarydeclaration.service.protocol=http://
salarydeclaration.service.host=localhost
salarydeclaration.service.port=9090
salarydeclaration.service.context=integration/ws
salarydeclaration.service.name=SalaryDeclarationServiceFacade

# MONITORING
monitoring.enabled=false
monitoring.user=admin
monitoring.pass=admin

# WS-SECURITY CONFIGURATION
wss4j.signatureUser=abtst-server
wss4j.privateKeyPassword=abtst
org.apache.ws.security.crypto.merlin.file=security/abTst_server.jks
org.apache.ws.security.crypto.merlin.keystore.password=htabern
```

Exemple B.1. Configuration standard réception

```
                #
# Copyright 1996-2013 itServe AG. All rights reserved.
#
# This software is the proprietary information of itServe AG
# Bern Switzerland. Use is subject to license terms.
#


# RECEIVER INDENTIFICATION
institution.tax.id=BE
institution.tas.id=BE

# DIRECTORY CONFIGURATION
released.filesystem.parent.xml=data/received
failed.filesystem.parent.xml=data/failed
result.filesystem.parent.xml=data/result
sent.filesystem.parent.xml=data/sent
undeliverable.filesystem.parent.xml=data/undeliverable
maintenance.filesystem.parent.xml=data/maintenance

# MONITORING
monitoring.enabled=false
monitoring.user=admin
monitoring.pass=admin

# BEHAVIOUR CONFIGURATION
commune.splitting=false
la.splitting=false
write.original.xml=false
await.result=false
processing.default.hours=168

housekeeping.days=180
```

Exemple B.2. Configuration standard intégration

```
                <?xml version='1.0' encoding='utf-8'?>
<!--

   Copyright 1996-2013 itServe AG. All rights reserved.

   This software is the proprietary information of itServe AG
   Bern Switzerland. Use is subject to license terms.

-->
<Server port="8005" shutdown="SHUTDOWN">

   <!--APR library loader. Documentation at /docs/apr.html -->
   <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on"/>
   <!--Initialize Jasper prior to webapps are loaded. Documentation at /docs/jasper-howto.html -->
   <Listener className="org.apache.catalina.core.JasperListener"/>
   <!-- Prevent memory leaks due to use of particular java/javax APIs-->
   <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener"/>
   <!-- JMX Support for the Tomcat server. Documentation at /docs/non-existent.html -->
   <Listener className="org.apache.catalina.mbeans.ServerLifecycleListener"/>
   <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener"/>

   <GlobalNamingResources>
      <Resource name="UserDatabase" auth="Container"
            type="org.apache.catalina.UserDatabase"
            description="User database that can be updated and saved"
            factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
            pathname="conf/tomcat-users.xml"/>
   </GlobalNamingResources>

   <Service name="Catalina">
      <Connector port="8080" protocol="HTTP/1.1"
            connectionTimeout="20000"/>

      <!-- Uncomment for activate SSL/TLS termination and mutual authentication -->
      <!-- <Connector port="8443" protocol="HTTP/1.1"
            connectionTimeout="20000"
            scheme="https" secure="true" SSLEnabled="true"
            keystoreFile="[path]/server.jks" keystorePass="keystore pass"
            truststoreFile="[path]/truststore.jks" truststorePass="truststore pass"
            clientAuth="true" sslProtocol="TLS"/> -->

      <Engine name="Catalina" defaultHost="localhost">
         <Realm className="org.apache.catalina.realm.UserDatabaseRealm"
               resourceName="UserDatabase"/>
         <Host name="localhost" appBase="webapps" deployOnStartup="false"
            unpackWARs="false" autoDeploy="false"
            xmlValidation="false" xmlNamespaceAware="false">

            <Context path="/webservice" docBase="swissdecAdapter-webservice-2.0_5.war" reloadable="false"/>
         </Host>
      </Engine>
   </Service>
</Server>
```

Exemple B.3. Configuration standard réception Tomcat

```
                <?xml version='1.0' encoding='utf-8'?>
<!--

   Copyright 1996-2013 itServe AG. All rights reserved.

   This software is the proprietary information of itServe AG
   Bern Switzerland. Use is subject to license terms.

-->
<Server port="8006" shutdown="SHUTDOWN">

   <!--APR library loader. Documentation at /docs/apr.html -->
   <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on"/>
   <!--Initialize Jasper prior to webapps are loaded. Documentation at /docs/jasper-howto.html -->
   <Listener className="org.apache.catalina.core.JasperListener"/>
   <!-- Prevent memory leaks due to use of particular java/javax APIs-->
   <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener"/>
   <!-- JMX Support for the Tomcat server. Documentation at /docs/non-existent.html -->
   <Listener className="org.apache.catalina.mbeans.ServerLifecycleListener"/>
   <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener"/>

   <GlobalNamingResources>
      <Resource name="UserDatabase" auth="Container"
            type="org.apache.catalina.UserDatabase"
            description="User database that can be updated and saved"
            factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
            pathname="conf/tomcat-users.xml"/>
   </GlobalNamingResources>

   <Service name="Catalina">
      <Connector port="9090" protocol="HTTP/1.1"
               connectionTimeout="20000"/>

      <Engine name="Catalina" defaultHost="localhost">
         <Realm className="org.apache.catalina.realm.UserDatabaseRealm"
               resourceName="UserDatabase"/>
         <Host name="localhost" appBase="webapps" deployOnStartup="false"
            unpackWARs="false" autoDeploy="false"
            xmlValidation="false" xmlNamespaceAware="false">

            <Context path="/integration" override="true" docBase="swissdecAdapter-integration-2.0_5.war"
                  reloadable="false"/>
         </Host>
      </Engine>
   </Service>
</Server>
```

Exemple B.4. Configuration standard intégration Tomcat

```
<?xml version="1.0" encoding="UTF-8" ?>
<!--

   Copyright 1996-2013 itServe AG. All rights reserved.

   This software is the proprietary information of itServe AG
   Bern Switzerland. Use is subject to license terms.

-->
<!DOCTYPE log4j:configuration SYSTEM "log4j.dtd">
<log4j:configuration debug="false" xmlns:log4j="http://jakarta.apache.org/log4j/">
   <appender name="CATALINA" class="org.apache.log4j.DailyRollingFileAppender">
      <param name="File" value="${catalina.base}/logs/catalina.out"/>
      <param name="DatePattern" value="yyyy-MM-dd"/>
      <layout class="org.apache.log4j.PatternLayout">
         <param name="ConversionPattern" value="%d [%t] %-5p %c - %m%n"/>
      </layout>
   </appender>
   <appender name="FILE" class="org.apache.log4j.DailyRollingFileAppender">
      <param name="File" value="${catalina.base}/logs/swissdecAdapter.log"/>
      <param name="DatePattern" value="yyyy-MM-dd"/>
      <layout class="org.apache.log4j.PatternLayout">
         <param name="ConversionPattern" value="%d [%t] %-5p %c - %m%n"/>
      </layout>
   </appender>
   <appender name="ACCESS" class="org.apache.log4j.FileAppender">
      <param name="File" value="${catalina.base}/logs/access.log"/>
      <param name="ImmediateFlush" value="true"/>
      <layout class="org.apache.log4j.PatternLayout">
         <param name="ConversionPattern" value="%d [%t] %-5p %c - %m%n"/>
      </layout>
   </appender>

   <logger name="ch.itserve.lohnstandard">
      <level value="INFO"/>
   </logger>

   <logger name="ch.itserve.lohnstandard.receiver.webservice.SwissdecAdapterStartupListener">
      <level value="DEBUG"/>
   </logger>

   <logger name="ch.itserve.lohnstandard.receiver.integration.impl.SwissdecAdapterStartupListener">
      <level value="DEBUG"/>
   </logger>

   <logger name="org.apache.catalina">
      <level value="INFO"/>
      <appender-ref ref="CATALINA"/>
   </logger>

   <logger name="org.apache.ws">
      <level value="ERROR"/>
      <appender-ref ref="FILE"/>
   </logger>
   <logger name="org.hibernate">
      <level value="ERROR"/>
   </logger>
```

Exemple B.5. Configuration standard identification

```
   <logger name="access">
      <level value="INFO"/>
      <appender-ref ref="ACCESS"/>
   </logger>

   <root>
      <level value="INFO"/>
```