



# Directive concernant l'utilisation de sedex

<b>1</b>	<b>Contexte</b>	<b>2</b>
<b>1.1</b>	<b>But du présent document.....</b>	<b>2</b>
<b>1.2</b>	<b>Public-cible.....</b>	<b>2</b>
<b>1.3</b>	<b>Représentant de domaine .....</b>	<b>2</b>
<b>2</b>	<b>Bases légales</b>	<b>3</b>
<b>3</b>	<b>Responsabilités: principes généraux</b>	<b>4</b>
<b>4</b>	<b>Topologies importantes de participants sedex</b>	<b>5</b>
<b>4.1</b>	<b>Cas A: raccordement physique à sedex - raccordement de base .....</b>	<b>5</b>
4.1.1	Exigences minimales .....	6
4.1.2	Conséquences .....	6
<b>4.2</b>	<b>Cas B: raccordement physique à sedex - plusieurs domaines .....</b>	<b>7</b>
4.2.1	Exigences complémentaires .....	7
4.2.2	Conséquences .....	7
<b>4.3</b>	<b>Cas C: raccordement logique à sedex - plusieurs domaines .....</b>	<b>8</b>
4.3.1	Exigences complémentaires .....	8
4.3.2	Conséquences .....	9
<b>4.4</b>	<b>Cas D: raccordement sedex logique - routeur générique .....</b>	<b>9</b>
4.4.1	Exigences complémentaires .....	10
4.4.2	Conséquences .....	10
<b>4.5</b>	<b>Perspective : raccordement par interconnexion - Bus bridge .....</b>	<b>11</b>

# 1 Contexte

La plateforme d'échange de données sedex (*secure data exchange*) a été mise en production début 2008 dans le cadre de l'harmonisation des registres officiels de personnes pour la réalisation du nouveau recensement de la population. Depuis la mise en service de sedex, l'utilisation de cette plateforme a été étendue à de nombreux autres domaines en dehors de l'harmonisation des registres.

En sus de l'implémentation d'origine, typique (une organisation, un participant sedex, un domaine sedex), on trouve aujourd'hui un nombre croissant de configurations et d'installations plus complexes et techniquement très variées, par ex. centre de calcul informatique proposant un raccordement à sedex pour plusieurs organisations et plusieurs domaines via un seul sedex-Client physique. Cette évolution peut s'avérer dans certaine situation problématique au niveau de la protection des données.

Actuellement, lors de la commande d'un nouveau Client-sedex, il arrive régulièrement qu'on ne soit pas au clair sur les possibilités de raccordement; par ex. raccordement logique ou physique? Possibilité de partage d'un Client-sedex avec un autre domaine? Il est devenu nécessaire d'établir une réglementation uniforme des implémentations.

## 1.1 But du présent document

La présente directive tient compte de ces évolutions. L'implémentation de sedex dans l'infrastructure IT est catégorisée, accompagnée d'une description des compétences et responsabilités s'y rapportant. En outre, des exigences minimales ont été définies afin de permettre un échange de données sécurisé.

Les différentes possibilités de raccordement (topologies) sont documentées ci-après. Enfin, chaque topologie considérée est assortie d'informations relatives aux critères d'admission, aux mesures et aux conséquences qu'elle implique.

## 1.2 Public-cible

Ce document s'adresse aussi bien aux bénéficiaires de prestations (BP) qu'aux personnes responsables des domaines sedex (représentants de domaine). Il est également destiné aux personnes responsables d'infrastructures IT ou les exploitants de solutions en aval, comme des dispatcher, de bus ou de systèmes de traitement de messages.

## 1.3 Représentant de domaine

Le représentant de domaine veille à ce que son groupe de participants sedex respecte la présente directive. A noter que les participants sedex ne gèrent pas obligatoirement eux-mêmes l'exploitation de leur raccordement à sedex. Ils peuvent confier cette tâche à des tiers.

## 2 Bases légales

La loi sur l'harmonisation des registres (LHR, RS 431.02) constitue la base légale de la plate-forme TIC sedex de la Confédération. Les dispositions générales relatives à sedex figurent dans les articles 10 et 14 LHR. Les dispositions détaillées relatives à l'utilisation, à la mise en œuvre, aux coûts de sedex ainsi qu'aux compétences en la matière sont définies dans l'ordonnance sur l'harmonisation des registres (OHR, RS 431.021). L'OFS est notamment désigné comme unité responsable de sedex à la Confédération.

L'utilisation de sedex à d'autres fins officielles est réglée dans l'art. 15 OHR. Dans de tels cas, l'échange de données via sedex se fait selon les directives de l'OFS. Les éventuelles redevances d'utilisation prévues sont définies dans l'ordonnance du 25 juin 2003 (RS 431.09) sur les émoluments et indemnités perçus pour les prestations de services statistiques des unités administratives de la Confédération. Les montants des redevances et indemnités sont publiés sous [www.sedex.ch \ Voraussetzungen\ sedex Produkt-Preismodell 2012](http://www.sedex.ch/Voraussetzungen/sedex-Produkt-Preismodell-2012).

### 3 Responsabilités: principes généraux

- La responsabilité de l'OFS en tant que fournisseur de prestations de sedex s'arrête au niveau de l'interface avec l'adaptateur sedex ou du dépôt des messages dans les répertoires (Inbox et Outbox) du Client-sedex, à l'intérieur de l'infrastructure du bénéficiaire de prestations (figure 1).
- La configuration correcte de l'infrastructure IT et du Client-sedex ainsi que le respect des dispositions en matière de protection des données sont du ressort de chaque organisation responsable de l'exploitation sur place.
- Les expéditeurs ou les domaines responsables répondent des contenus des messages.
- Le bénéficiaire de prestations ou le responsable de domaine est chargé du renouvellement des certificats qui sont utilisés en dehors du processus automatique de renouvellement.
- Les questions de détail avec le service sedex sont réglées dans des conventions cadre ou complémentaires avec les domaines.

Le fournisseur de prestations facture les éventuels coûts au domaine responsable. La répercussion de ces coûts aux participants effectifs est de la compétence des domaines.

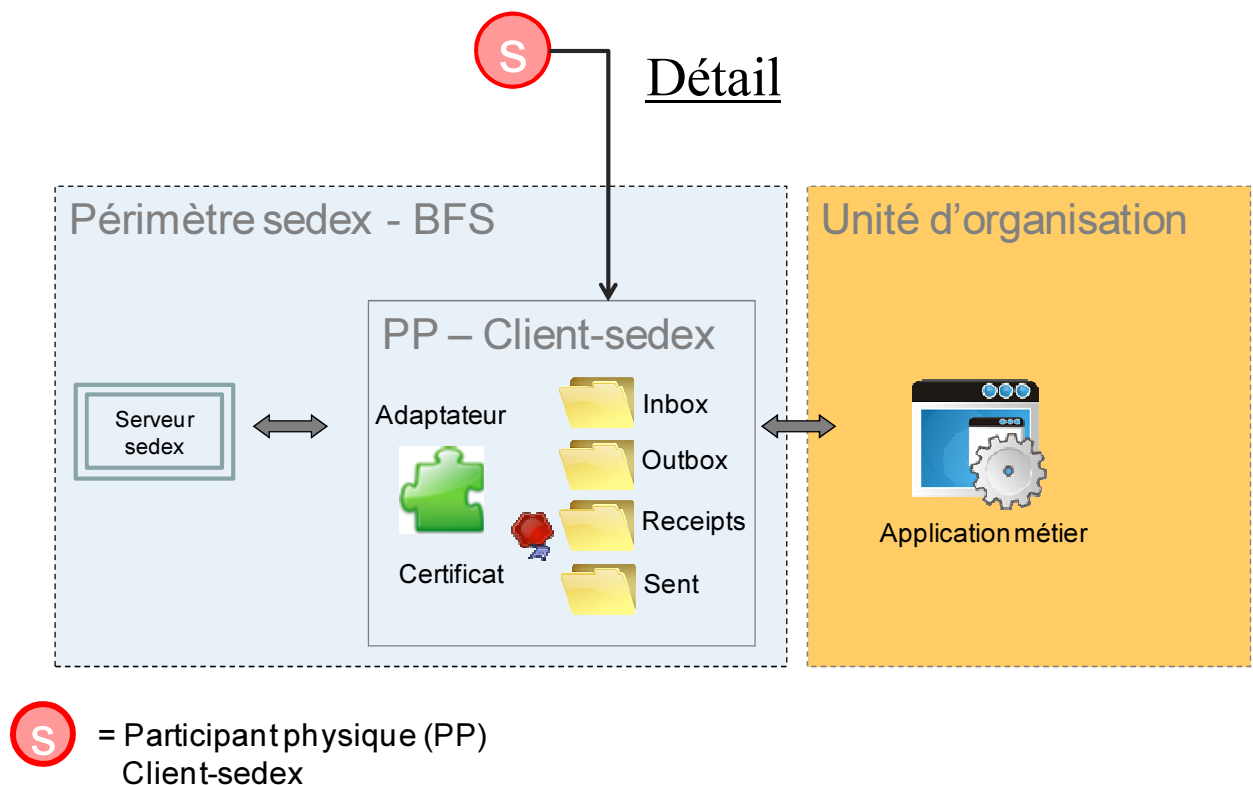


Figure 1: Graphique détaillé sur le raccordement physique à sedex.

## 4 Topologies importantes de participants sedex

Le terme "topologie" est utilisé ici pour catégoriser les installations sedex effectives. Le raccordement de base décrit ci-après est considéré comme l'installation la plus simple. Toutes les autres installations sont établies à partir de ce raccordement de base en devant répondre à des exigences complémentaires croissantes.

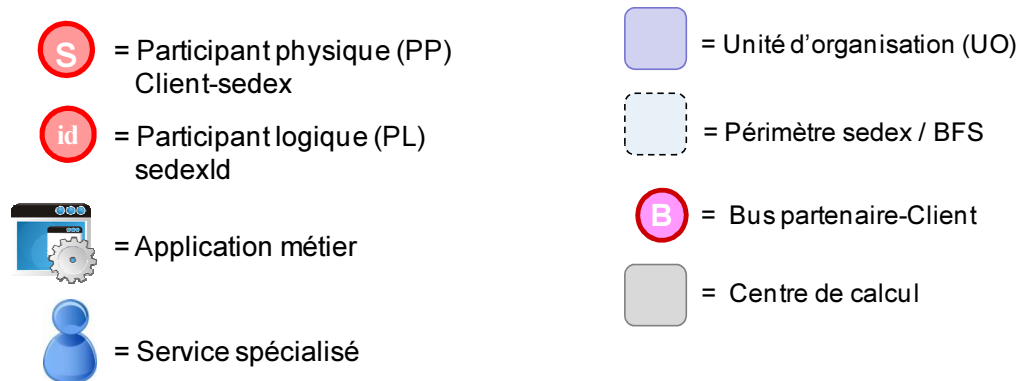


Figure 2: Légende des symboles utilisés dans les graphiques

### 4.1 Cas A: raccordement physique à sedex - raccordement de base

Une unité d'organisation ou un service spécialisé utilise une application métier pour le traitement de ses cas d'affaires.

Caractéristiques :

- Un Client-sedex est installé physiquement.
- Le participant sedex est attribué à un domaine sedex (domaine 1).
- L'installation n'a aucun participant sedex logique dépendant.
- Il n'y a pas de distribution locale des messages effectuée en aval. L'application métier utilise directement les répertoires du Client-sedex.

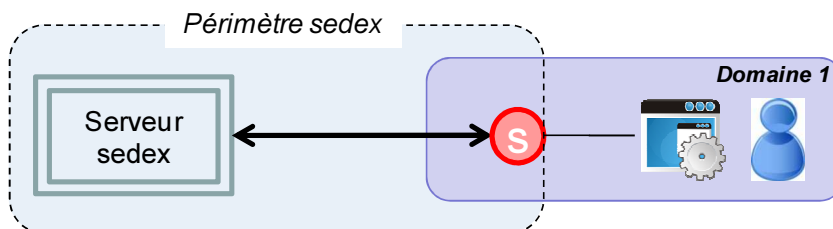


Figure 3: Le service spécialisé est raccordé physiquement. Exemple d'utilisation: commune, caisse-maladie.

### 4.1.1 Exigences minimales

Voici les exigences minimales auxquelles doit répondre l'infrastructure avec un Client-sedex:

- Les bases légales et les normes du domaine responsable doivent être respectées.
- L'installation doit être effectuée selon le manuel de sedex.
- L'infrastructure sur laquelle le Client-sedex est installée doit satisfaire aux prescriptions pertinentes en matière de protection des données et de sécurité informatique.
- Deux instances du Client-sedex ne peuvent jamais être activées simultanément avec le même sedex-ID. Si plusieurs instances du Client-sedex sont exploitées (par ex. pour des systèmes redondants), le maniement des messages et des quittances, dans le cas d'un changement d'instance (dit Failover), doit être réglé clairement.
- Les répertoires sedex doivent être visibles exclusivement par l'application métier de l'unité d'organisation.
- L'application métier doit traiter sans erreur tous les messages ainsi que leurs quittances.
- Selon la configuration du Client-sedex, les répertoires de ce dernier (par ex. *processed* ou *sent*) peuvent contenir des messages déjà traités. Ces répertoires doivent être administrés activement. Si les messages ne sont plus nécessaires (archivage), ils seront définitivement supprimés. Ils ne peuvent pas être éliminés simplement en les déplaçant dans la "corbeille".
- Les éléments de sécurité (certificat de la classe C, mots de passe) ne peuvent être utilisés que dans le cadre de l'implémentation de sedex. L'utilisation doit se dérouler en fonction des prescriptions du manuel sedex le plus récent. Toute autre utilisation n'est autorisée qu'avec l'accord préalable du fournisseur de prestations (OFS).
- Installer resp. Mettre à jour le plus rapidement possible la dernière version disponible de Client-sedex (« life cycle management »).

### 4.1.2 Conséquences

La topologie de la version de base a les conséquences suivantes:

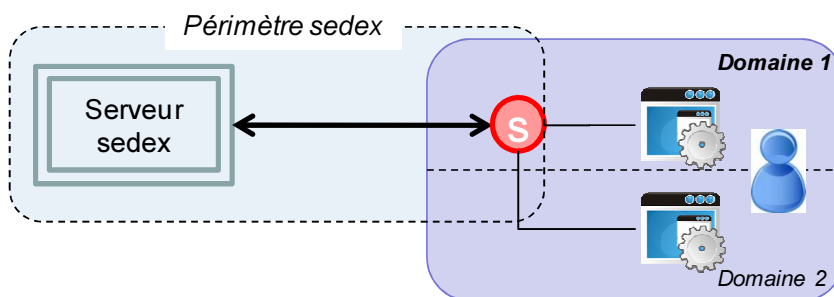
- Les messages sont cryptés de bout-en-bout à l'intérieur du périmètre sedex.
- Tous les messages contenus dans le Client-sedex sont attribués au même service spécialisé.
- La traçabilité est assurée sur l'ensemble de l'acheminement des données. Les rapports correspondants sont disponibles.
- L'OFS assure le support et est responsable de la transmission correcte des données ainsi que de toutes les composantes de sedex liées à la sécurité.

## 4.2 Cas B: raccordement physique à sedex - plusieurs domaines

Une unité d'organisation ou un service spécialisé utilise plusieurs applications métier vouées au traitement de ses cas d'affaires. Les cas d'affaires concernent différents domaines de sedex.

Caractéristiques :

- Un Client-sedex est installé physiquement.
- Le participant sedex est attribué à un domaine sedex (domaine 1).
- L'installation n'a aucun participant sedex logique dépendant.
- Il y a une distribution locale des messages effectuée en aval par un tiers via les types de message.



**Figure 4:** L'unité d'organisation ou le service spécialisé est raccordé(e) physiquement. Exemple d'utilisation: centre de calcul de communes de petite taille.

### 4.2.1 Exigences complémentaires

- **Les exigences minimales sont respectées (voir chapitre 4.1.1).**
- Cette topologie n'est autorisée que pour une petite organisation (par ex. petite commune, petite caisse AVS, etc.).
- L'activation de types de message d'autres domaines de sedex doit être préalablement approuvée par le responsable de domaine du participant sedex physique concerné.
- En complément aux exigences minimales, les répertoires sedex ne doivent pouvoir être visibles que par la solution en aval pour la répartition locale.
- Il convient si possible d'implémenter des quittances métiers dans les cas d'affaires.

### 4.2.2 Conséquences

Un raccordement couvrant plusieurs domaines a les conséquences suivantes:

- Les messages sont cryptés bout-en-bout à l'intérieur du périmètre sedex. En fonction de la solution de distribution locale située en aval, les messages ne sont éventuellement pas cryptés jusqu'au bout.
- Tous les messages contenus dans le sedex-Client sont attribués au même service spécialisé. Les messages doivent être traités correctement par les applications métiers via les types de message.
- La traçabilité est assurée sur l'ensemble de l'acheminement des données. Les rapports correspondants sont disponibles. Chaque domaine ne voit que ses types de message.

## Directive concernant l'utilisation de sedex

- L'OFS assure le support et est responsable de la transmission correcte des données ainsi que de toutes les composantes de sedex liées à la sécurité.

### 4.3 Cas C: raccordement logique à sedex - plusieurs domaines

Une unité d'organisation ou un service spécialisé utilise plusieurs applications métier vouées au traitement de ses cas d'affaires. Les cas d'affaires concernent différents domaines de sedex, par ex. l'Office fédéral des assurances sociales, qui échange des données dans divers domaines.

Caractéristiques :

- Un Client-sedex est installé physiquement, mais chaque unité d'organisation utilise un participant sedex logique subordonné.
- Le participant sedex physique est attribué à un domaine sedex (domaine 1).
- Il y a une distribution locale des messages effectuée en aval par un tiers via les sedex-ID.
- Le participant sedex physique ne dispose lui-même d'aucune autorisation.

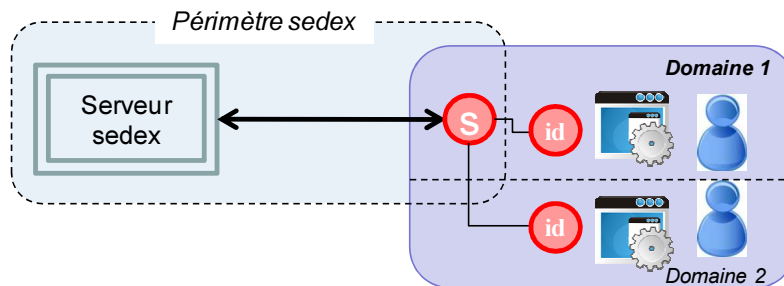


Figure 5: Les participants sont raccordés logiquement. Exemple d'utilisation: centre de calcul d'une unité d'organisation.

#### 4.3.1 Exigences complémentaires

- **Les exigences minimales sont respectées (voir chapitre 4.1.1).**
- L'activation de messages d'autres domaines de sedex doit être préalablement approuvée par le responsable de domaine du participant sedex physique concerné (domaine 1).
- Si les messages sont transmis physiquement plus loin, ils ne peuvent l'être qu'à l'intérieur de l'infrastructure de l'exploitant.
- Lors du raccordement d'un nouveau participant sedex, le responsable de domaine du participant sedex physique peut exiger une description de l'architecture (par ex. schéma d'architecture ou concept) du raccordement sedex effectif ainsi qu'un concept de sécurité. Les autres représentants de domaine doivent être d'accord avec la topologie de raccordement.



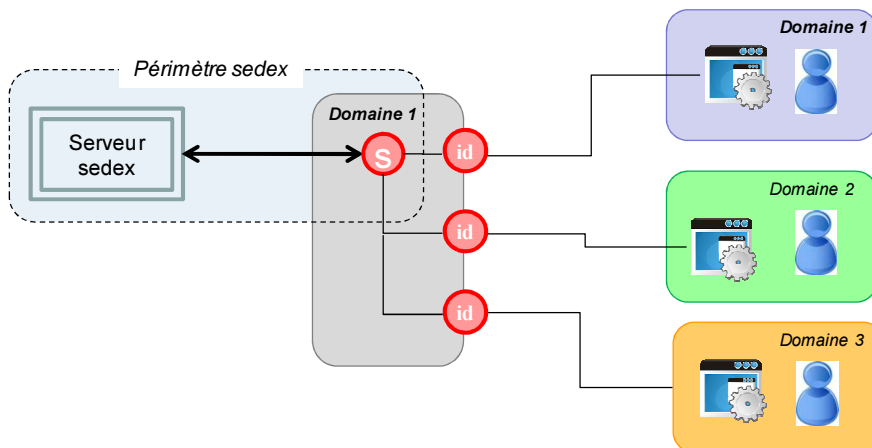
### 4.3.2 Conséquences

La topologie décrite a les conséquences suivantes:

- Les messages ne sont pas cryptés de bout-en-bout, car une distribution locale jusqu'au destinataire final est effectuée en aval par des solutions tierces.
- La traçabilité par sedex est assurée uniquement jusqu'au Client-sedex physique.
- Les messages contenus dans le Client-sedex doivent être attribués resp. transmis aux services spécialisés concernés à l'aide du sedex-ID. Les messages doivent ensuite être traités correctement par les applications métiers via les types de message.
- Le fournisseur de prestations ne dispose pas d'exploitations relatives à des solutions situées en aval.
- Le fournisseur de prestations ne répond pas du traitement incorrect des messages par des solutions tierces.
- Le fournisseur de prestations ne propose aucun support pour des solutions tierces.
- D'éventuelles investigations sont effectuées par le fournisseur de prestations selon le principe du "best effort".

## 4.4 Cas D: raccordement sedex logique - routeur générique

Plusieurs unités d'organisation ou services spécialisés utilisent plusieurs applications métier vouées au traitement de leurs cas d'affaires. Les cas d'affaires concernent différents domaines de sedex. Dans cette configuration, le Client-sedex fonctionne comme routeur.



**Figure 6:** Toutes les unités d'organisation sont raccordées logiquement. Exemple d'utilisation: organisations cantonales ou hébergeurs d'applications métier.

Caractéristiques :

- Un Client-sedex est installé physiquement. Chaque application métier ou unité d'organisation utilise un participant sedex logique subordonné séparé avec une identification sedex.
- Il y a une distribution locale étendue des messages effectuée en aval par un tiers (par un dispatcher ou une application analogue).

## Directive concernant l'utilisation de sedex

- Le participant sedex physique ne dispose lui-même d'aucune autorisation.
- Le participant physique est attribué à un domaine (domaine 1), les participants logiques peuvent être attribués à d'autres domaines.

### 4.4.1 Exigences complémentaires

- **Les exigences minimales sont respectées (voir chapitre 4.1.1).**
- Cette topologie n'est autorisée que pour des organisations de grande taille (par ex. centre de calcul pour des solutions communales, centre de calcul cantonal).
- L'activation des messages d'autres domaines de sedex doit être préalablement approuvée par le responsable de domaine du participant physique concerné.
- Tous les représentants de domaine qui participent doivent être mis au courant de cette topologie et se déclarer d'accord avec cette dernière. Les représentants de domaine assurent directement la coordination.
- Lors du raccordement d'un nouveau participant sedex, le responsable de domaine du participant sedex physique peut exiger une description de l'architecture (par ex. schéma d'architecture ou concept) du raccordement sedex effectif ou un concept de sécurité. Les autres représentants de domaine doivent être d'accord avec la topologie de raccordement.
- Les représentants de domaine peuvent au besoin vérifier sur place si la topologie de raccordement et le concept de sécurité auprès du partenaire hébergeur sont mis en œuvre correctement.

### 4.4.2 Conséquences

La topologie décrite a les conséquences suivantes:

- Les messages ne sont pas cryptés bout-en-bout, car une distribution locale jusqu'au destinataire final est effectuée en aval par des solutions tierces.
- La traçabilité par sedex est assurée uniquement jusqu'au Client-sedex physique.
- Les messages disponibles dans le Client-sedex doivent être attribués resp. transmis aux services spécialisés concernés à l'aide du sedex-ID. Les messages doivent ensuite être traités correctement par les applications métier via les types de message.
- Le fournisseur de prestations ne dispose pas d'exploitations relatives à des solutions situées en aval.
- Le fournisseur de prestations ne répond pas du traitement incorrect des messages par des solutions tierces.
- Le fournisseur de prestations ne propose aucun support pour des solutions tierces.
- D'éventuelles investigations sont effectuées par le fournisseur de prestations selon le principe du "best effort".

### 4.5 Perspective : raccordement par interconnexion - Bus bridge

Cette constellation est décrite comme perspective possible. Elle n'existe pas encore. Deux exploitants de bus autorisent leurs participants respectifs à échanger les données de manière transparente.

Dans ce cas, il n'y a pas de sedex-ID pour chaque application métier ou unité d'organisation. Les participants bus ont chacun une propre identification bus. Ils sont donc des participants physiques d'un bus partenaire. Le passage entre sedex et le bus partenaire se fait via un bridge. Si le bus partenaire répond aux mêmes exigences que le bus sedex, cette constellation correspond alors à une installation standard de sedex avec un client physique par participant. En conséquence, il y a un cryptage de bout-en-bout des participants bus.

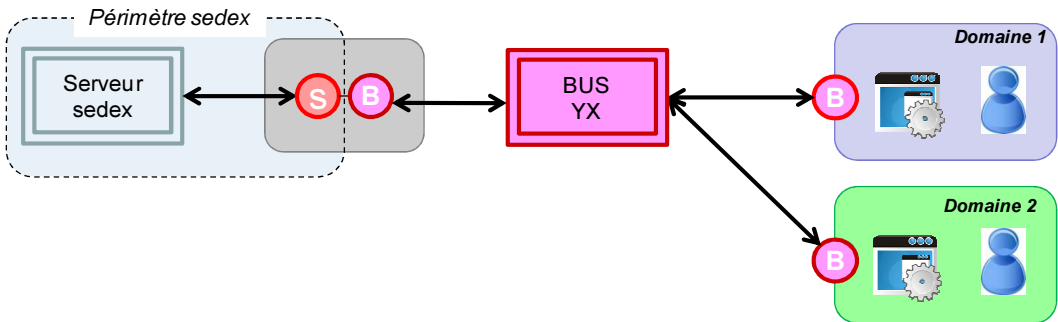


Figure 7: Topologie possible d'un raccordement via une interconnexion

### Glossaire

Infrastructure AdminPKI	Infrastructure Public-Key de l'OFIT (Swiss Gouvernement PKI) Elle sert à l'établissement des certificats sedex.
BUS	Infrastructure de transport pour un échange de messages asynchrone
BP	Bénéficiaire de prestations de l'offre sedex (un domaine)
FP	Fournisseur de prestations Dans le présent document, le fournisseur de prestations de sedex est toujours l'OFS.
PL	Participant sedex logique
PP	Participant sedex physique

### Annexe

Esquisse d'architecture et questions y relatives