



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral de la statistique OFS
Division Interopérabilité et registres IOR

Catalogue des services sedex

État : octobre 2025

Office fédéral de la statistique

Section sedex et registres

Espace de l'Europe 10

Suisse – CH-2010 Neuchâtel

Tél : +41 800 866 700

Courriel : sedexsupport@bfs.admin.ch

Table des matières

1	Services sedex	4
1.1	Qu'est-ce que sedex et pourquoi utiliser sedex ?	4
1.2	Quel est le mandat et le cadre juridique de sedex ?	4
2	Message sedex	5
2.1	Fichier de données (payload)	5
2.2	Enveloppe sedex (envelope)	5
2.3	Quittance technique (receipt)	5
2.4	Classe de message	5
3	Domaines sedex	6
3.1	Participants sedex	6
3.2	Type de message sedex	6
3.3	Autorisation par type de message	7
3.4	Gestion des domaines	7
3.5	Reporting	8
4	Messagerie sedex	9
4.1	Plateforme sedex	9
4.2	Logiciel client sedex	9
4.3	Certificat de participant sedex	9
4.4	Boîte aux lettres sedex	10
4.5	Message dispatching	10
5	Services Web	12
5.1	Proxy de service Web sedex (sedex Web Service Proxy)	12
5.2	Service Web sedex	12
5.3	Plateforme de fournisseur services Web	12
6	Conditions d'utilisation	14
6.1	Directives d'utilisation opérationnelles	14
6.2	Gestion du cycle de vie sedex	14
6.3	Frais d'utilisation	14
6.4	Niveaux de service	15
7	Help center	17

7.1	Support sedex	17
7.2	Technical user documentation for the sedex-Client.....	17
7.3	NewsMail sedex	17
7.4	sedex directories	17
8	Monitoring	18
8.1	Vérification du client sedex	18
8.2	État du système sedex.....	18
9	Sécurité	19
9.1	Cryptage.....	19
9.2	Authentification.....	19
9.3	Autorisation	19
9.4	Intégrité des données	19
10	Validité	20

1 Services sedex

1.1 Qu'est-ce que sedex et pourquoi utiliser sedex ?

sedex signifie « **secure data exchange** » et est une **plateforme de communication centrale pour la transmission asynchrone de données entre les applications métier** des unités d'organisation de l'administration publique. La transmission de données est sécurisée, fiable et traçable et convient aussi bien aux grandes qu'aux petites quantités de données.

La plateforme sedex est la plateforme éprouvée pour l'échange des données en Suisse, sedex assure la numérisation sans rupture de média de divers processus métier dans le domaine de la cyberadministration suisse. L'utilisation de sedex augmente la productivité grâce à l'intégration complète de la communication de machine à machine (machine-to-machine, M2M) entre les applications métiers. Elle offre les avantages suivants :

- fonctionnement sur toute plateforme et avec tout environnement d'exploitation,
- interfaces simples d'utilisation (système de fichiers ou API REST),
- envoi sécurisé et fiable de données sensibles (seul le destinataire peut décrypter les données),
- cryptage pendant toute la transmission entre les applications métiers lors d'utilisation de l'interface REST,
- établissement de reçus et de protocoles (conservés au moins dix ans) pour assurer la traçabilité des transactions métier,
- vaste réseau comptant plus de 8000 applications métier,
- possibilité d'envoi simultané à plusieurs destinataires (avec cryptage individuel),
- représentation des transactions métiers à plusieurs niveaux au moyen de classes de messages,
- seuls les participants autorisés peuvent déclencher une transaction métier ou le recevoir (également entre un domaine et un autre),
- transmission de tous les types de données jusqu'à 10 Go (sedex segmente les fichiers automatiquement).

1.2 Quel est le mandat et le cadre juridique de sedex ?

Pour l'harmonisation des registres, la Confédération a été chargée en vertu de l'art. 10, al. 3 de la loi sur l'harmonisation des registres (LHR ; RS 431.02), de mettre une plateforme informatique et de communication à la disposition des services et des autorités concernées. La Confédération a rempli son mandat en créant la plateforme sedex et poursuit les objectifs suivants :

- fournir des services d'excellence et adaptés aux exigences actuelles aux administrations publiques à tous les niveaux fédéraux ;
- soutenir la numérisation et l'automatisation des processus administratifs grâce à des services de transfert de données simples et fiables ;
- offrir des services viables en termes de coûts et compétitifs.

La section 4 (art. 11 à 17) de l'ordonnance sur l'harmonisation de registres (OHR, RS 431.021) définit l'utilisation de sedex.

Les art. 11, 12 et 13 s'appliquent en matière d'utilisation de sedex dans le cadre de l'harmonisation des registres. Les articles suivants ont une portée plus générale :

- L'art. 14 OHR définit les exigences de sécurité en matière de transmission des données, en particulier concernant la traçabilité et le cryptage des données.
- L'art. 15 OHR prévoit notamment que **sedex puisse être utilisé comme plateforme de transmission de données à d'autres fins officielles**, la transmission devant s'effectuer conformément aux directives de l'OFS.
- L'art. 16 OHR exige que les utilisateurs, lorsqu'ils recourent à sedex hors harmonisation des registres, prennent les mêmes mesures de protection des données que celles appliquées par les services qui tiennent les registres.
- L'art. 17 OHR règle les exigences relatives au certificat des participants raccordés à sedex.

En vertu de l'art. 5, al. 4, de l'ordonnance sur l'harmonisation des registres (OHR, RS 431.021), l'OFS est l'unité responsable de sedex à la Confédération.

2 Message sedex

Un message sedex se compose d'un fichier de données, appelé « Payload » et d'une enveloppe sedex, appelée « Enveloppe ».

2.1 Fichier de données (payload)

Le fichier de données peut adopter tout format (pdf, docx, zip, jpg, tar, xml, etc.), sa taille est limitée à 10 Go. Les domaines définissent les contenus des fichiers de données et les conventions qui s'appliquent (normes p. ex.).

2.2 Enveloppe sedex (enveloppe)

L'enveloppe est un fichier XML standardisé conformément à la norme [eCH-0090, version 1.0](#). L'enveloppe contient notamment les informations d'adressage nécessaires à l'envoi d'un message ainsi que les informations relatives au cas d'affaire (type de message).

2.3 Quittance technique (receipt)

La quittance technique est un fichier XML standardisé conformément à la norme [eCH-0090, version 2.0](#). Elle est donnée pour indiquer à l'émetteur si son message a été délivré ou non. Toutefois, la quittance ne confirme pas que le destinataire a traité le message. Le système délivre une quittance technique pour chaque destinataire d'un message : si l'émetteur envoie un message à deux destinataires, il reçoit deux quittances.

2.4 Classe de message

Dans le cadre d'un cas d'affaire (type de message), la classe de message définit la signification métier de celui-ci.

Classe de message	Signification	Description
0	Message	Message initial, déclenchement d'un cas d'affaire par une application métier.
1	Response	Réponse de l'application métier destinataire à un message.
2	Receipt	Quittance (accusé de réception) émise par l'application métier destinataire.
3	Error	Message d'erreur émis par l'application métier destinataire.

3 Domaines sedex

Un domaine sedex désigne un secteur métier (groupe d'utilisateurs) qui utilise sedex.

Un domaine est une association de participants sedex qui traitent des cas d'affaires dans un contexte spécifique et échangent des messages sedex à cet effet. Chaque participant est membre d'un domaine sedex et reçoit un ID unique et adressable (appelé « sedex-ID »).

Chaque domaine définit ses propres types de messages sedex. Un type de message correspond à un cas d'affaire qui se déroule entre les participants sedex. Chaque message sedex est attribué à un type de message.

Chaque participant sedex est autorisé à utiliser certains types de messages. Un message ne peut être échangé entre deux participants que si l'expéditeur et le destinataire sont tous deux autorisés pour le type de message en question et qu'ils se trouvent dans le même environnement (environnement : production/test).

sedex distingue trois types de domaines :

- les domaines en lien avec l'harmonisation des registres,
- les domaines en lien avec d'autres enquêtes statistiques de l'OFS,
- les domaines prévoyant d'autres fins administratives.

Le site [Domains directory \(sedex.swiss\)](https://domains.directory(sedex.swiss)) publie une liste de tous les domaines sedex actifs, actualisée quotidiennement.

3.1 Participants sedex

Un participant sedex est une unité organisationnelle reliée à sedex. Chaque domaine définit ses participants, qui seront exclusivement des entreprises ou des entités IDE inscrites dans le [registre IDE](#). Chaque participant est membre d'un seul domaine sedex et se voit attribuer un identifiant unique adressable. Le site [Participants directory \(sedex.swiss\)](https://participants.directory(sedex.swiss)) publie une liste de tous les participants sedex actifs, actualisée quotidiennement.

Les participants peuvent être définis en tant que participant physique, participant logique ou routeur.

Un **participant physique** est un participant sedex avec son propre client sedex installé physiquement. Ainsi, un participant physique correspond à une installation d'un client sedex sur un hôte ou en tant que container.

Un **participant logique** ne dispose pas de son propre client sedex et donc pas non plus de son propre certificat de participant sedex. L'échange des messages sedex se fait via un participant physique autorisé pour le participant logique (routeur sedex) et l'utilisation de services Web se faisant via le proxy WS sedex du participant physique.

Un **routeur sedex** correspond à un participant sedex physique utilisé comme intermédiaire pour les participants logiques reliés. En tant que routeur, il n'est pas adressé directement via son propre identifiant de participant (sedex-ID), mais indirectement via les sedex-ID des participants logiques qui lui sont rattachés. Le routeur répartit les messages vers les participants logiques via un [Message dispatching](#). Un routeur sedex devrait être utilisé exclusivement en tant que tel et ne devrait pas être autorisé lui-même pour les types de messages.

3.1.1 Environnements (environnement)

La plateforme sedex permet d'échanger des messages dans deux environnements virtuellement distincts : « production » et « test ». Chaque participant ne peut être attribué qu'à un de ces environnements, et cette attribution ne peut être modifiée. Pour s'échanger des messages, les participants doivent être attribués au même environnement et avoir l'autorisation pour le type de message correspondant. Les types de message (cas d'affaire) sont indépendants de l'environnement. L'ID de participant (sedex-ID) des participants de l'environnement « test » est précédé du préfixe « T ».

3.2 Type de message sedex

Chaque domaine définit ses propres types de message sedex. Un type de message correspond à un cas d'affaire traité entre les participants sedex. Chaque message sedex est affecté à un type de message. Cela se fait par la saisie du numéro correspondant (message type ID) dans l'enveloppe sedex.

Un type de message se compose des éléments suivants : message type ID, nom, description, statut (« active » / « inactive ») ; il est attribué à un seul domaine.

Le site [Message Types directory \(sedex.swiss\)](https://sedex.swiss/MessageTypesDirectory) publie une liste de tous les types de message sedex actifs, actualisée quotidiennement.

3.3 Autorisation par type de message

Pour envoyer ou recevoir des messages d'un type donné, les participants doivent disposer de l'autorisation correspondante. Ils se voient attribuer un des droits suivants (privilege) par type de message :

Privilege	Description
Initiator	Le participant peut déclencher des cas d'affaire du type de message en question (classe de message 0), recevoir des messages entrants de ce type de message et y répondre.
Sender	Le participant peut recevoir des messages entrants de ce type de message et y répondre (classe de message > 0). Il ne peut pas déclencher des cas d'affaire du type de message (classe de message 0).
Receiver	Le participant peut uniquement recevoir des messages du type de message en question.

3.3.1 Transmission interdomaines (cross-domain messaging)

Les participants de différents domaines peuvent échanger des messages sedex. Les deux participants doivent disposer de l'autorisation pour le type de message correspondant. Tant le détenteur du domaine du participant que le détenteur du domaine du type de message doivent préalablement approuver cette autorisation.

3.4 Gestion des domaines

Seuls les représentants de domaine autorisés par le détenteur du domaine peuvent demander de nouveaux types de message, participants sedex, certificats de participants sedex et règles de routage ou demander une modification de la configuration. Les représentants autorisés d'un domaine sedex peuvent gérer leur domaine sur la plateforme client sedex.

3.4.1 Gestion des participants

Les participants peuvent être consultés dans la plateforme client et les commandes en ligne suivantes peuvent être saisies. Une fois les commandes validées par le support sedex, ces modifications seront intégrées dans la plateforme sedex.

- Création de nouveaux participants
- Activation ou désactivation de participants
- Modification des noms ou des informations sur les détenteurs des participants
- Octroi, modification ou désactivation des autorisations pour les types de messages de son propre domaine
- Création, modification ou désactivation de règles de routage des participants logiques sur les routeurs de son domaine
- Modification de la topologie (physique/logique) d'un participant

Les commandes suivantes ne peuvent pas être saisies dans la plateforme client et doivent être commandées auprès du support sedex.

- Commander de nouveaux certificats de participant sedex
- Transfert de participants dans un autre domaine
- Créer, modifier ou désactiver les autorisations pour les types de messages d'un autre domaine
- Création, modification ou désactivation de règles de routage des participants logiques sur les routeurs d'un autre domaine

Les commandes interdomaines nécessitent l'autorisation des représentants des deux domaines.

Le traitement se fait généralement dans un délai d'un jour, mais au plus tard dans les dix jours ouvrables.

3.4.2 Gestion des routeurs

Les routeurs sedex peuvent être gérés dans la plateforme client de la même manière que les participants sedex. Les règles de routage sont gérées chez les participants logiques.

3.4.3 Gestion des types de message

Les types de messages peuvent être consultés dans la plateforme client, mais ne peuvent pas être traités directement. Les opérations suivantes doivent être commandées auprès du support sedex.

- Création de nouveaux types de messages
- Activation ou désactivation des types de messages
- Modifier le nom ou la description des types de messages

Le transfert de types de messages vers un autre domaine nécessite l'autorisation des représentants des deux domaines.

Le traitement se fait généralement dans un délai d'un jour, mais au plus tard dans les dix jours ouvrables.

3.5 Reporting

Les rapports suivants sont à la disposition des responsables d'un domaine et peuvent être commandés auprès du support sedex :

3.5.1 Rapports périodiques

Nom	Envoi	Description
incomplete message transmissions [domain]	quotidien	Messages de tous types d'un domaine dont la transmission a échoué ou dont la réception n'a pas été confirmée au cours des 30 derniers jours.
status reports [domain]	mensuel	Diverses informations sur le statut et la configuration des participants et des types de message d'un domaine.
traffic reports [domain] [PREVIOUS_MONTH]	quotidien	Nombre de messages envoyés et reçus, et volume de données par participant au cours du mois précédent.
traffic reports [domain] [PREVIOUS_YEAR]	annuel	Nombre de messages envoyés et reçus et volume de données par participant au cours de l'année civile précédente.
traffic reports [domain] [PREVIOUS_12_MONTHS]	mensuel	Nombre de messages envoyés et reçus et volume de données par participant au cours des douze derniers mois.
message list [domain] [PREVIOUS_DAY]	quotidien	Messages de tous les types d'un domaine envoyés la veille.
message list [domain] [PREVIOUS_MONTH]	mensuel	Messages de tous les types d'un domaine envoyés le mois précédent.

3.5.2 Rapports ad hoc

Nom	Description
default_routings [domain]	Liste des participants logiques de tous les routeurs d'un domaine.
traffic reports [domain] [period]	Nombre de messages envoyés et reçus, et volume de données par participant au cours d'une période donnée.
message list [domain][participant(s)][message id(s)][period]	Messages de tous les types d'un domaine au cours d'une période donnée, qui peuvent au besoin être limités à certains participants ou à certains message ids (usmid d'un message).

4 Messagerie sedex

La connexion à sedex permet un échange de données sécurisé, fiable et traçable entre les applications métier des participants connectés. La transmission entre deux **clients sedex** s'effectue de manière asynchrone via la **plateforme sedex**. À cette fin, les **certificats des participants sedex** sont utilisés pour l'authentification, l'autorisation, le cryptage et le décryptage. L'intégration des applications métier s'effectue via la **boîte postale sedex**. Un **message dispatching** est utilisé pour l'intégration avec les participants logiques.

4.1 Plateforme sedex

Le serveur sedex se charge du routage des messages, de l'autorisation ainsi que de la journalisation centrale du trafic des messages. **La plateforme sedex est exploitée et surveillée en permanence dans les centres de calcul de l'Office fédéral de l'informatique et de la télécommunication OFIT, situés en Suisse.**

Après une livraison réussie, l'expéditeur reçoit une quittance positive et les données transmises sont supprimées sur la plateforme sedex. Si la livraison ne peut avoir lieu pour une raison quelconque, l'expéditeur reçoit une quittance négative avec la raison au plus tard après 31 jours. Toutes les transactions sont journalisées et la traçabilité est garantie à tout moment. Les journaux de transactions sont conservés pendant dix ans au moins.

Les indications des accusés de réception techniques (receipts) permettent à l'émetteur de suivre un message sedex. Cette forme de suivi des messages (message tracking) suffit généralement aux participants. Si nécessaire, il est possible de commander des journaux de transactions détaillés auprès du support sedex.

Il est aussi possible d'adresser un message sedex à plusieurs participants simultanément. Chaque destinataire physique reçoit alors son propre fichier de données (payload) spécifiquement crypté à son attention. Un tel message ne sera transmis que si tous les destinataires sont autorisés à recevoir le type de message utilisé. Si un des destinataires n'y est pas autorisé, le message ne sera transmis à aucun d'entre eux.

4.2 Logiciel client sedex

Le client sedex est un logiciel qui connecte l'application métier des participants sedex à la plateforme sedex. En règle générale, le client sedex fonctionne sur le même hôte que l'application spécialisée ou est accessible en toute sécurité pour l'application métier via le réseau.

Le client sedex est une application basée sur Java qui peut être installée sur des machines physiques ou virtuelles avec différents systèmes opérationnels (y compris Windows, macOS, Linux, AIX, etc.).

Il est possible de l'installer et de l'exploiter de différentes manières :

- en tant qu'installation autonome sur un hôte avec démarrage / arrêt (start / stop) manuel de l'application ou en tant que service en arrière-plan fonctionnant en permanence ;
- en tant que conteneur Docker sur une plateforme de conteneurs. sedex publie le client sedex en tant qu'image officielle du conteneur sur Docker Hub. Le conteneur du client sedex peut être utilisé sur une plateforme de conteneurs telle que Docker, Kubernetes, OpenShift, etc.

Comme ces deux types d'installation offrent les mêmes fonctionnalités, le choix dépend principalement des exigences et des préférences techniques et organisationnelles de l'organisation qui héberge le logiciel.

4.2.1 Documentation et logiciels

Documentation : [Technical user documentation for the sedex-Client](#)

Logiciels : [sedex Downloads](#)

4.3 Certificat de participant sedex

Un participant sedex physique doit pouvoir s'identifier avec un certificat de participant sedex spécifique. Ce certificat de participant sedex correspond à un certificat d'organisation (certificats spécifiques de classe C) et est utilisé à des fins d'authentification, d'autorisation ainsi que de cryptage et de décryptage. Pour l'obtention, la gestion et l'utilisation des certificats de participant sedex, l'OFS gère une plateforme de certificats basée sur l'infrastructure [Swiss Government PKI](#).

Les certificats sedex sont générés par le client sedex chez le participant. Ainsi, il est garanti que la clé privée associée à un certificat n'est connue que du participant. Les certificats ont une validité de trois ans. Le certificat du participant lui-même est public. **Par contre, la clé privée (fichier P12) ainsi que le mot de passe correspondant sont des composants de sécurité. Les composants de sécurité ne peuvent pas être copiés** (sauvegarde de sécurité et systèmes redondants exclus) **et / ou transmis à des tiers. L'utilisation des composants de sécurité en dehors du client sedex n'est pas autorisée.** En cas de révocation ou après l'expiration du certificat, l'utilisation de la plateforme sedex n'est plus possible immédiatement.

Le certificat sera automatiquement renouvelé en temps voulu par le client sedex. Afin que les messages qui ont été cryptés avec l'ancien certificat puissent également être décryptés, l'ancien et le nouveau certificat sont valables pendant un certain temps. La condition pour le renouvellement automatique du certificat est le respect des [directives opérationnelles](#).

4.4 Boîte aux lettres sedex

Chaque participant sedex possède sa propre boîte aux lettres, qui comprend les répertoires suivants :

Répertoires	Description
Inbox	Messages reçus
Outbox	Messages à envoyer
Receipts	Quittances techniques des messages envoyés
Processed	Messages envoyés, que la transmission ait réussi ou non

L'accès de l'application métier à la boîte aux lettres sedex se fait via le client sedex, soit par l'interface de messagerie du système de fichiers sedex (sedex File System Messaging Interface), soit par l'API REST de messagerie sedex (sedex Messaging REST API). Il est possible de paramétrer l'interface selon le type de message. Comme l'échange de messages entre les participants est indépendant de l'interface choisie, l'émetteur et le destinataire peuvent la paramétrer à leur guise.

4.4.1 sedex File System Messaging Interface

L'accès de l'application métier s'effectue sur la base de fichiers (file I/O). Les messages se trouvent alors dans les répertoires de fichiers (inbox, outbox, receipts) sous forme non cryptée. La protection des fichiers relève de la responsabilité de l'exploitant du système de fichiers. Les répertoires sont créés automatiquement lors de l'installation du client sedex.

4.4.2 sedex Messaging REST API

Les applications métier peuvent aussi envoyer et recevoir des messages sedex via une API REST de messagerie basée sur https. Pour l'application métier, on crée dans le client sedex un utilisateur spécifique (technical user) permettant d'accéder à l'API REST. L'application métier passe par cet utilisateur pour échanger des messages sedex directement avec le client sedex. Lors de l'utilisation de l'API REST, les messages sont enregistrés sous forme cryptée dans la base de données locale du client sedex. En outre, le canal entre l'application métier et le client sedex est crypté par TLS. L'échange sécurisé de données entre le client sedex et l'application métier est donc assuré. Si tant l'émetteur que le destinataire recourent à l'interface REST, les données peuvent être cryptées pendant toute la transmission entre les applications métier.

4.5 Message dispatching

Tout comme pour le participant physique qui accède à sa boîte aux lettres, la distribution interne des messages (message dispatching) aux participants logiques peut se faire – en utilisant un routeur sedex – soit via l'interface de messagerie du système de fichiers sedex (sedex file system messaging interface), soit via l'API REST sedex (sedex Messaging REST API). Il est possible de paramétrer l'interface selon le type de message et le participant logique. Comme l'échange de messages entre les participants est indépendant de l'interface choisie, l'émetteur et le destinataire peuvent paramétrer celle-ci à leur guise.

4.5.1 Message dispatching avec sedex File System Messaging Interface

Lors d'un accès basé sur des fichiers (file I/O), l'exploitant du routeur sedex doit s'occuper lui-même de la distribution des messages entre l'application métier du participant logique et de son routeur sedex. Comme pour un courrier interne, l'exploitant doit mettre en oeuvre un mécanisme sécurisé pour transmettre un message entrant à l'application métier à laquelle il est adressé ou pour récupérer un message envoyé par celle-ci. Précisons qu'un message sedex envoyé à plusieurs participants logiques du routeur n'apparaît qu'une seule fois dans la boîte de réception. **La distribution de messages (message dispatcher) doit dupliquer ce message pour chaque participant logique.** Des produits tiers librement disponibles dans l'écosystème sedex peuvent prendre en charge la distribution des messages, par exemple l'outil [Open eGov MessageHandler pour sedex \(de\)](#). **Le support sedex n'offre toutefois aucun support pour les produits tiers.**

4.5.2 Message Dispatching avec sedex Messaging REST API

En cas d'accès au moyen de l'API REST de messagerie, la distribution des messages est intégrée dans le client sedex. Pour l'application métier de l'utilisateur logique, on crée dans le client sedex un utilisateur spécifique qui permet d'accéder à l'API REST. L'application métier passe par cet utilisateur pour échanger des messages sedex directement avec le client sedex. Lors de l'utilisation de l'API REST, les messages sont enregistrés sous forme cryptée dans la base de données locale du client sedex. Le canal entre l'application métier et le client sedex est de plus crypté par TLS. L'échange sécurisé de données entre le client sedex et l'application métier est donc assuré. **L'API REST de messagerie intègre d'ores et déjà la duplication des messages sedex envoyés à plusieurs participants logiques du routeur sedex.**

5 Services Web

5.1 Proxy de service Web sedex (sedex Web Service Proxy)

Le proxy de service Web sedex (en abrégé : WS proxy sedex) est un composant du client sedex qui permet aux applications métiers du participant d'accéder de manière sécurisée aux services Web de sedex et de fournisseurs tiers (voir Plateforme du prestataire Webservice) autorisés.

5.2 Service Web sedex

La configuration des services web sedex est contenue dans le client sedex et tous les participants sedex sont autorisés à les utiliser via le WS proxy sedex. Le fournisseur (provider) du service web est la plateforme sedex.

5.2.1 Service Web sedex : check-sedex

Ce service Web permet aux utilisateurs d'interroger les participants sedex et de vérifier leur authenticité et leurs autorisations sur la base de leurs certificats sedex. L'application métier émettrice peut y recourir pour vérifier s'il est possible d'envoyer un message sedex donné aux destinataires prévus. Voici les critères contrôlés :

- l'ID sedex de l'émetteur et du destinataire doivent être valides,
- l'émetteur et le destinataire doivent être des participants sedex actifs,
- l'émetteur et le destinataire ont chacun un certificat valide,
- l'émetteur est autorisé à envoyer des messages de ce type,
- le destinataire est autorisé à recevoir des messages de ce type,
- la taille du fichier de données ne doit pas dépasser la limite maximale autorisée (contrôle facultatif).

5.2.2 Service Web sedex : sedex external authorization service

Ce service Web sert à identifier les participants sedex, et à les authentifier et autoriser, en fonction des certificats sedex. Il est utilisé par les fournisseurs de services Web qui veulent rendre disponible leur service via le WS proxy sedex et qui veulent vérifier si une requête SOAP provenant d'Internet a bien été envoyée par un participant sedex et si celui-ci y est autorisé.

5.3 Plateforme de fournisseur services Web

Le client sedex permet aussi de traiter une communication de données synchrone. Il assure une communication de données cryptée entre l'utilisateur (consumer) et le fournisseur (provider) d'un service Web, sans influence sur le contenu.

Les participants sedex qui souhaitent utiliser des services web bénéficient d'une mise en oeuvre simplifiée et standardisée de ces services. Pour ce faire, l'application métier établit une connexion au sein de l'infrastructure protégée du participant sur le WS proxy du client sedex. Si le participant sedex dispose de l'autorisation requise pour un service Web, le client sedex reprend automatiquement de la plateforme sedex la configuration nécessaire pour permettre l'utilisation du service Web.

L'utilisateur de services Web a alors la certitude que c'est bien le fournisseur de services Web souhaité qui le renseigne. Quant à ce dernier, il peut vérifier l'authenticité et l'autorisation de l'utilisateur.

Les services Web actuellement disponibles :

Services Web	Provider	Lien
UPIServices	Centrale de compensation CdC	Interface UPIServices (admin.ch)
Service de consultation ASSH	Association suisse des services des habitants (ASSH)	Association suisse des services des habitants (ASSH) Demande carte d'assuré
eDéménagement Suisse – identification de personnes	eOperations Suisse SA	eDéménagement Suisse > eOperations
Webservice IDE	Office fédéral de la statistique OFS	Interfaces IDE Office fédéral de la statistique (admin.ch)
Webservices RegBL	Office fédéral de la statistique OFS	Registre des bâtiments et logements Office fédéral de la statistique (admin.ch)
Identifiant du dossier électronique du patient	Centrale de compensation CdC	Identifiant du dossier électronique du patient (admin.ch)

Chaque service Web mis en lien via le proxy de services Web sedex est affecté à des types de message bien précis. Les droits d'utilisation se gèrent comme les droits d'utilisation des messages sedex. Les points d'accès aux services Web sont gérés dans la plateforme sedex. La configuration du sedex WS-Proxy pour l'utilisation d'un service Web se fait automatiquement chez les participants autorisés.

6 Conditions d'utilisation

6.1 Directives d'utilisation opérationnelles

Le détenteur d'un participant physique sedex est tenu de respecter les directives opérationnelles suivantes :

- Le client sedex est un composant de sécurité qui doit impérativement être maintenu à jour. Le client sedex doit être mis à jour au moins une fois par an avec la dernière version ([recommended version](#)) du client sedex.
- Pour garantir la fiabilité de l'échange de messages et le renouvellement automatique des certificats, un client sedex doit être en service en permanence si possible.
- L'utilisation des composants de sécurité du certificat de participant sedex (clé privée et mot de passe correspondant) en dehors du client sedex n'est pas autorisée.
- Il faut s'assurer qu'il n'y a pas d'instances en double. Les instances doubles sont plusieurs installations de clients sedex qui se connectent avec le même identifiant et utilisent le même certificat de participant sedex et le même ID sedex. Cela peut se produire, par exemple, lorsque le client sedex est installé sur un nouvel hôte et que le client sedex sur l'ancien hôte n'a pas été correctement désinstallé.

Le support sedex peut désactiver avec effet immédiat les participants qui ne respectent pas les directives opérationnelles, qui présentent un problème de sécurité en raison de la version utilisée ou qui causent des problèmes techniques, et révoquer leurs certificats.

6.2 Gestion du cycle de vie sedex

6.2.1 Statuts des versions

Statuts des versions	Description
Recommended	Version la plus récente et recommandée. Seule cette version est disponible en téléchargement.
Supported	Version prise en charge. Les nouvelles versions de la plateforme sedex ou les modifications de l'infrastructure sont uniquement testées sur les versions client sedex supportées. La formation du personnel d'assistance porte exclusivement sur ces versions. En principe, l'assistance couvre les versions pendant 18 mois dès leur déploiement. Si une version pose problème, le support sedex peut la passer au statut « unsupported » avec effet immédiat.
Unsupported	Le certificat du client sedex n'est plus renouvelé. Il se peut que d'éventuels problèmes ne puissent ni être identifiés ni être reproduits. Avant toute demande d'assistance, l'utilisateur est prié de procéder à une mise à jour vers la dernière version « recommended » du logiciel.

6.2.2 Versions prises en charge

Les versions actuellement prises en charge sont publiées sur www.sedex.ch (les versions qui n'y figurent pas sont considérées comme « unsupported »).

6.3 Frais d'utilisation

Le financement de sedex est équilibré en termes de coûts et de bénéfices et est assuré par les domaines sedex. Le modèle de tarification de l'utilisation de sedex vise à répartir équitablement les coûts totaux de sedex entre les domaines sedex en fonction de leur utilisation effective de sedex. Les critères de répartition des coûts sont revus régulièrement.

À compter du 1er janvier 2025, les tarifs d'utilisation de sedex suivants s'appliquent.

Article	Tarif hors TVA
Tarif annuel par participant physique	Fr. 360.–
Tarif annuel par participant logique	Fr. 120.–
Tarif par message envoyé	Fr. –.01
Tarif du volume de donnée envoyée par Mo	Fr. –.12

Compte tenu de l'utilisation croissante de sedex et de l'évolution des comportements des utilisateurs, le modèle de prix est mis à jour chaque année afin de refléter l'évolution des coûts et l'utilisation globale dans tous les domaines sedex. En règle générale, le modèle tarifaire applicable pour l'année suivante est publié fin septembre/début octobre. Si des augmentations de prix s'avéraient nécessaires, elles seraient communiquées au moins 12 mois à l'avance pour l'année suivante.

Les frais d'utilisation pour l'exercice comptable *EC* sont facturés annuellement durant l'exercice *EC* sur la base du volume convenu pour l'année en question. La différence par rapport à l'utilisation effective est prise en compte dans la facturation de l'année suivante.

La correction de l'année suivante est effectuée pour :

- Les frais de message sur la base du nombre de messages envoyés (nombre de Message ID créés et volume de données par destinataire adressé) pendant la période du 1er octobre de l'année *EP* au 30 septembre de l'année *EC* (exercice précédent : $EP=EC-1$) ;
- les frais par participants selon le nombre de participants actifs, physiques et logiques au jour de référence (30 septembre de l'année *EC*).

6.4 Niveaux de service

Les niveaux de service suivants s'appliquent aux services sedex.

6.4.1 Support sedex

Élément	Niveau de service (service level)
Période d'assistance	Du lundi au vendredi, de 8h30 à 12h et de 13h30 à 16h

6.4.2 sedex-Plattform

Élément	Niveau de service (service level)
Période d'assistance	Du lundi au dimanche de 0h à 24h
Maintenance	Dimanche 8h à 22h pour les changements importants, travaux de maintenance portant sur tout le système
Disponibilité par trimestre	Durée maximale d'une panne : 8 heures Nombre maximal de pannes : 3 Délai maximale de reprise par défaillance : 8 heures Durée maximale de perte de données : 2 heures
Niveau de protection	Protection de base : Permet de traiter des données personnelles ou fichiers non accessibles au public, au sens de la loi sur la protection des données (LPD)

6.4.3 Plateforme des certificats

Élément	Niveau de service (service level)	
Période d'assistance	Du lundi au vendredi de 7h à 18h	
Maintenance	Mercredi 18h à jeudi 6h	
Disponibilité par trimestre	Durée maximale d'une panne :	12 heures
	Nombre maximal de pannes :	3
	Délai maximale de reprise par défaillance :	12 heures
	Durée maximale de perte de données :	4 heures
Niveau de protection	Protection de base : Permet de traiter des données personnelles ou fichiers non accessibles au public, au sens de la loi sur la protection des données (LPD)	

6.4.4 Plateforme client sedex

Élément	Niveau de service (service level)	
Période d'assistance	Du lundi au dimanche de 0h à 24h	
Maintenance	Sur accord	
Disponibilité par trimestre	Durée maximale d'une panne :	2 jours ouvrables
	Nombre maximal de pannes :	3
	Délai maximale de reprise par défaillance :	Best Effort
	Durée maximale de perte de données :	Best Effort
Niveau de protection	Protection de base : Permet de traiter des données personnelles ou fichiers non accessibles au public, au sens de la loi sur la protection des données (LPD)	

7 Help center

7.1 Support sedex

Le support sedex offre une assistance lors de :

- Questions concernant les certificats d'organisation sedex,
- la configuration des participants sedex,
- l'installation et l'exploitation du client sedex,
- la définition des cas d'affaires et des types de messages sedex,
- mise à disposition de rapports d'utilisation et de journaux des transactions,
- problèmes spécifiques à sedex.

Le support sedex peut être contacté via les canaux suivants :

- Courriel : sedexsupport@bfs.admin.ch
- Téléphone : 0800 866 700

Sont exclues les prestations relatives aux applications métier, aux périphériques et aux infrastructures informatiques et de communication des utilisateurs finaux, ainsi que toutes les prestations non explicitement mentionnées dans le présent catalogue des services sedex.

7.2 Technical user documentation for the sedex-Client

La [documentation d'utilisateur \(docs.sedex.admin.ch\)](https://docs.sedex.admin.ch) sedex contient, outre les clients sedex actuels et les release notes, des explications techniques complètes sur les différentes formes d'exploitation d'un client sedex et l'intégration de sedex dans une application spécialisée. Cette documentation s'adresse aux spécialistes IT qui exploitent des clients sedex ou qui intègrent sedex dans leur application spécialisée et n'est disponible qu'en anglais.

7.3 NewsMail sedex

Le NewsMail sedex vous informe sur les thèmes suivants :

- publications de nouvelles versions du client sedex,
- avis de service (notifications de maintenances et d'interruptions de sedex),
- informations générales sur sedex.

Inscription : [Abonnement NewsMail sedex](#)

7.4 sedex directories

Vous trouverez dans [sedex directories \(www.sedex.swiss\)](https://www.sedex.swiss) les listes des [participants sedex](#), les [types de message sedex](#) et les [domaines sedex](#). Les données sont actualisées quotidiennement.

8 Monitoring

8.1 Vérification du client sedex

Différents outils permettent de vérifier le bon fonctionnement du client sedex.

8.1.1 sedex Client Pinger

Pour vérifier si votre client sedex est correctement installé pour l'échange de messages, le support sedex peut recourir à la fonction sedex-Client Pinger pour envoyer un message test à votre client sedex et évaluer la quittance technique.

8.1.2 Page de monitoring du client sedex

La page de monitoring locale du client sedex contient une liste de paires clé / valeur pour la surveillance des opérations. Vous pouvez consulter la page de monitoring via HTTP ou via le système de fichiers.

8.2 État du système sedex

Sur mandat de l'Office fédéral de la statistique (OFS), l'Office fédéral de l'informatique et de la télécommunication (OFIT) exploite la plateforme sedex et en surveille le fonctionnement à l'aide de différents systèmes de monitoring. Le Centre de contrôle opérationnel de l'OFIT (OCC) met à disposition un monitoring permettant de vérifier l'état et la disponibilité du système (uniquement accessible depuis le réseau de l'administration fédérale) : [00_DashboardSHVMain - Visionneuse de rapports \(admin.ch\) \(de\)](#).

9 Sécurité

9.1 Cryptage

La sécurité des données est le critère déterminant de la transmission de données via sedex : autrement dit, le système doit empêcher que ces données puissent être consultées ou modifiées. Pour respecter ces exigences de sécurité, sedex recourt à un triple cryptage sur la base de méthodes de cryptage éprouvées et des technologies de pointe :

1. Cryptage des messages de bout en bout
2. Cryptage de transmission OSCI
3. Cryptage des canaux TLS

Ainsi, le contenu d'un message sedex est crypté selon trois méthodes avant d'être transmis par Internet. Il bénéficie donc d'une triple protection contre la consultation ou la modification.

Les trois niveaux de sécurisation cryptographique sont expliqués ci-dessous.

9.1.1 Cryptage des messages de bout en bout

Dans sedex, la transmission des messages est cryptée de bout en bout. Des procédés cryptographiques asymétriques assurent que tout message envoyé via le client sedex puisse uniquement être décrypté par le destinataire auquel le message est adressé.

Cette procédure garantit que le message reste crypté à tout moment de son acheminement : rien ni personne ne peut le consulter ou le modifier. Même sur le serveur sedex, le message est stocké temporairement sous forme cryptée. Seul le destinataire prévu peut récupérer le message sur le serveur sedex, puis le décrypter.

En résumé, grâce au cryptage de bout en bout, sedex garantit :

1. Confidentialité : seul le destinataire prévu est en mesure de décrypter et de lire le message
2. Intégrité : authenticité garantie du contenu du message
3. Origine : authenticité garantie de l'émetteur

9.1.2 Cryptage de transmission OSCI

Pour la transmission d'un message du client sedex émetteur au serveur sedex, puis du serveur sedex au client sedex destinataire, sedex recourt à Governikus, un hub de messages certifié selon le standard OSCI. Un message sedex (déjà crypté de bout en bout) est alors transmis sous la forme d'un ou de plusieurs messages OSCI cryptés une nouvelle fois. À cet effet, chaque message OSCI est en outre sécurisé au moyen d'un cryptage de transmission OSCI.

9.1.3 Cryptage des canaux TLS

Toute la communication entre le client sedex et le serveur sedex se fait via le protocole https, sécurisé par TLS.

9.2 Authentification

L'authentification des participants sedex est effectuée sur la base de leurs certificats de participants sedex (certificats d'organisation .X509 de classe C). Seules les organisations identifiées et autorisées peuvent donc participer au réseau sedex.

9.3 Autorisation

sedex dispose de son propre système d'autorisation interne pour contrôler le flux des messages. Il est possible de paramétrer les privilèges de chaque participant individuellement pour chaque type de message. Le système fait en sorte qu'un message ne puisse être envoyé ou reçu par un participant que s'il lui a été accordé le droit (privilege) correspondant.

9.4 Intégrité des données

Les procédures de cryptage de bout en bout et les procédures de signature, reposant toutes sur des procédés cryptographiques asymétriques éprouvés, garantissent la confidentialité et l'inaltérabilité des données transmises.

10 Validité

Le présent catalogue de services sedex est valable à partir du 1er octobre 2025. Sous réserve de modifications.