



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

Bundesamt für Statistik BFS

Abteilung Interoperabilität und Register IOR

sedex Servicekatalog

Stand: Oktober 2025

Bundesamt für Statistik

Sektion sedex und Registerentwicklung

Espace de l'Europe 10

Schweiz – CH-2010 Neuchâtel

Tel: +41 800 866 700

E-Mail: sedexsupport@bfs.admin.ch

Inhaltsverzeichnis

1	sedex Services	4
1.1	Was ist sedex und warum sedex einsetzen?	4
1.2	Was sind Auftrag und rechtliche Grundlagen von sedex?	4
2	sedex-Meldung	5
2.1	Datendatei (Payload)	5
2.2	sedex-Umschlag (Envelope)	5
2.3	Technische Quittung (Receipt)	5
2.4	Meldungsklasse	5
3	sedex-Domänen	6
3.1	sedex-Teilnehmer	6
3.2	sedex-Meldungstyp	6
3.3	Autorisierung Meldungstyp	7
3.4	Domänenverwaltung	7
3.5	Reporting	8
4	sedex Messaging	9
4.1	sedex-Plattform	9
4.2	sedex-Client Software	9
4.3	sedex-Teilnehmerzertifikat	10
4.4	sedex Postfach	10
4.5	Message Dispatching	11
5	Webservices	12
5.1	sedex Webservice-Proxy (sedex WS-Proxy)	12
5.2	sedex Webservices	12
5.3	Webservice Anbieter Plattform	12
6	Nutzungskonditionen	14
6.1	Betriebliche Nutzungsrichtlinien	14
6.2	sedex Client Life Cycle Management	14
6.3	Nutzungsgebühren	14
6.4	Service Level	15
7	Help Center	17

7.1	sedex-Support.....	17
7.2	Technical user documentation for the sedex-Client.....	17
7.3	sedex NewsMail	17
7.4	sedex directories	17
8	Monitoring	18
8.1	sedex Client check	18
8.2	sedex System status	18
9	Sicherheit	19
9.1	Verschlüsselung	19
9.2	Authentisierung	19
9.3	Autorisierung	19
9.4	Datenintegrität.....	19
10	Gültigkeit	20

1 sedex Services

1.1 Was ist sedex und warum sedex einsetzen?

sedex steht für «**secure data exchange**» und ist eine **zentrale Kommunikationsplattform für die asynchrone Datenübermittlung zwischen Fachapplikationen** von Organisationseinheiten der öffentlichen Verwaltung. Die Datenübermittlung ist sicher, zuverlässig und nachvollziehbar. Sie eignet sich für grosse und für kleine Datenmengen.

Die Plattform sedex ist die bewährte schweizerische Datenaustauschplattform für die medienbruchfreie Digitalisierung verschiedenster Geschäftsprozesse im Bereich e-Government Schweiz. Der Einsatz von sedex erhöht die Produktivität durch Vollintegration der machine-to-machine (M2M) Kommunikation zwischen Fachapplikationen und bietet die folgenden Vorteile:

- Plattformunabhängiger Einsatz auf allen Betriebsumgebungen
- Einfach nutzbare Schnittstellen (Filesystem oder REST API)
- Sicherer und verlässlicher Versand sensibler Daten (nur der Empfänger kann die Daten entschlüsseln)
- Verschlüsselung während der gesamten Übertragung zwischen Fachapplikationen bei Verwendung der REST-Schnittstelle
- Nachvollziehbarkeit der Geschäftsfälle durch Quittungen und Protokollierung (Aufbewahrung mindestens zehn Jahre)
- Grosses Netzwerk mit mehr als 8000 teilnehmenden Fachapplikationen
- Versand an mehrere Empfänger gleichzeitig möglich (individuell verschlüsselt)
- Mehrstufige Geschäftsfälle sind mit Meldungsklassen abbildbar
- Nur autorisierte Teilnehmer können einen Geschäftsfall auslösen oder empfangen (auch domänenübergreifend)
- Übermittlung aller Datentypen bis 10GB (automatische Segmentierung durch sedex)

1.2 Was sind Auftrag und rechtliche Grundlagen von sedex?

Für die Registerharmonisierung wurde der Bund mit Art. 10 Abs. 3 Registerharmonisierungsgesetz (RHG; SR 431.02) beauftragt, den zuständigen Amtsstellen und Behörden für den Datenaustausch eine Informatik- und Kommunikationsplattform zur Verfügung zu stellen. Der Bund hat den Auftrag mit der Schaffung von sedex erfüllt und verfolgt damit die folgenden Ziele:

- Erbringung von erstklassigen und zeitgemässen Services für die öffentliche Verwaltung über alle föderalen Ebenen
- Unterstützung der Digitalisierung und der Automatisierung von Verwaltungsprozessen durch einfache und zuverlässige Datenübermittlungsservices
- Anbieten von kostentragenden und marktfähigen Services

Die Verwendung von sedex wird im Abschnitt 4 (Art. 11 bis 17) der Registerharmonisierungsverordnung (RHV; SR 431.021) geregelt.

Während Art. 11, 12 und 13 für die Verwendung von sedex innerhalb der Registerharmonisierung gültig sind, sind die folgenden Bestimmungen allgemein gültig:

- Art. 14 RHV definiert die Sicherheitsanforderungen an die Datenübermittlung, insbesondere bezüglich der Nachvollziehbarkeit und Verschlüsselung der Daten.
- Art. 15 RHV sieht insbesondere vor, dass **sedex als Datenübermittlungsplattform für weitere behördliche Zwecke** genutzt werden kann, wobei die Datenübermittlung nach den Richtlinien des BFS erfolgt.
- Art. 16 RHV verlangt, dass bei der Verwendung von sedex ausserhalb der Registerharmonisierung durch die Benutzerinnen und Benutzer dieselben Massnahmen des Datenschutzes ergriffen werden, müssen wie bei der Verwendung innerhalb der Registerharmonisierung.
- Art. 17 RHV regelt die Anforderungen an das sedex-Teilnehmerzertifikat.

Gemäss Art. 5 Abs. 4 der Registerharmonisierungsverordnung (RHV, SR 431.021) ist das BFS die beim Bund verantwortliche Stelle für sedex.

2 sedex-Meldung

Eine sedex-Meldung besteht aus einer beliebigen Datendatei, «Payload» genannt und einem sedex-Umschlag, «Envelope» genannt.

2.1 Datendatei (Payload)

Die Datendatei kann ein beliebiges Dateiformat (zum Beispiel: pdf, docx, zip, jpg, tar, xml usw.) mit einer Grösse bis 10 GB aufweisen. Die fachlichen Inhalte oder Konventionen (z.B. Verwendung von Standards) der Datendatei werden von den Domänen geregelt.

2.2 sedex-Umschlag (Envelope)

Der Umschlag ist eine standardisierte XML-Datei gemäss [eCH-0090, Version 1.0](#). Der Umschlag enthält u.a. die für die korrekte Zustellung einer Meldung erforderlichen Adressierungsinformationen sowie die Informationen zum Geschäftsfall (Meldungstyp).

2.3 Technische Quittung (Receipt)

Die technische Quittung ist eine standardisierte XML-Datei gemäss [eCH-0090, Version 2.0](#). Die technische Quittung wird ausgestellt, um dem Sender die erfolgreiche oder gescheiterte Übermittlung einer Meldung zu bestätigen. Die technische Quittung bestätigt in keinem Fall, dass der Empfänger die Meldung verarbeitet hat. Pro Empfänger einer Meldung wird eine Quittung ausgestellt, d.h. sendet der Sender eine Meldung an zwei Empfänger, so bekommt er zwei Quittungen.

2.4 Meldungsklasse

Innerhalb eines Geschäftsfalls (Meldungstyps) definiert die Meldungsklasse die fachliche Bedeutung der Meldung.

Meldungsklasse	Bedeutung	Beschreibung
0	Message	Initiale Meldung, Auslösung eines Geschäftsfall durch eine Fachapplikation
1	Response	Antwort der empfangenden Fachapplikation auf eine Meldung
2	Receipt	Fachliche Quittung (Empfangsbestätigung) der empfangenden Fachapplikation
3	Error	Fachliche Fehlermeldung der empfangenden Fachapplikation

3 sedex-Domänen

Eine sedex-Domäne bezeichnet einen Fachbereich (Nutzergruppe), der sedex verwendet.

Eine Domäne ist ein Verbund von sedex-Teilnehmern, die in einem spezifischen Kontext Geschäftsfälle abwickeln und dazu sedex-Meldungen austauschen. Jeder sedex-Teilnehmer ist Mitglied einer sedex-Domäne und erhält eine eindeutige, adressierbare ID (bekannt als sedex-ID).

Jede Domäne definiert ihre eigenen sedex-Meldungstyp. Ein Meldungstyp entspricht einem Geschäftsfall, der zwischen sedex-Teilnehmern abgewickelt wird. Jede sedex-Meldung wird einem Meldungstyp zugeordnet.

Jeder sedex-Teilnehmer ist für bestimmte Meldungstypen autorisiert. Eine Meldung kann nur zwischen zwei Teilnehmern ausgetauscht werden, wenn sowohl Sender als auch Empfänger für den jeweiligen Meldungstyp autorisiert sind und diese in der gleichen Umgebung (environment: production/test) sind.

sedex unterscheidet drei Arten von Domänen:

- Domänen innerhalb der Registerharmonisierung
- Domänen für weitere statistische Erhebungen des BFS
- Domänen für weitere behördliche Zwecke

Unter [Domains directory \(sedex.swiss\)](#) wird eine täglich aktualisierte Liste aller aktiven sedex-Domänen publiziert.

3.1 sedex-Teilnehmer

Ein sedex-Teilnehmer ist eine Organisationseinheit, welche an sedex angebunden ist. Jede Domäne bestimmt ihre Teilnehmer. Teilnehmer werden ausschliesslich für im [UID-Register \(www.uid.admin.ch\)](#) eingetragene Unternehmen und UID-Stellen erstellt. Jeder Teilnehmer ist Mitglied genau einer sedex-Domäne und erhält eine eindeutige, adressierbare ID. Unter [Participants directory \(sedex.swiss\)](#) wird eine täglich aktualisierte Liste aller aktiven sedex-Teilnehmer publiziert.

Teilnehmer können als physische oder logische Teilnehmer oder als Router erstellt werden.

Ein **physischer Teilnehmer** ist ein sedex-Teilnehmer mit einem eigenen physisch installierten sedex-Client. Somit entspricht ein physischer Teilnehmer einer Installation eines sedex-Clients auf einem Host oder als Container.

Ein **logischer Teilnehmer** verfügt nicht über einen eigenen sedex-Client und damit auch nicht über ein eigenes sedex-Teilnehmerzertifikat. Der Austausch der sedex-Meldungen erfolgt über einen für den logischen Teilnehmer berechtigten physischen Teilnehmer (sedex-Router) und die Nutzung von Webservices erfolgt über dessen sedex WS-Proxy.

Ein **sedex-Router** entspricht einem physischer sedex-Teilnehmer, der als Stellvertreter für bei ihm angesiedelte logische Teilnehmer genutzt wird. Als sedex-Router wird er nicht direkt über seine eigene Teilnehmer-ID (sedex-ID) adressiert, sondern indirekt über die sedex-IDs der logischen Teilnehmer, für die er zuständig ist. Die Meldungsverteilung zwischen Router und logischen Teilnehmer erfolgt über ein [Message Dispatching](#). Ein sedex-Router sollte ausschliesslich als solcher verwendet werden und selbst nicht für Meldungstypen berechtigt werden.

3.1.1 Umgebungen (Environment)

Über die sedex-Plattform können Meldungen in zwei virtuell getrennten Umgebungen, «production» und «test», ausgetauscht werden. Jeder Teilnehmer gehört entweder der Umgebung «production» oder «test» an. Ist diese einmal zugeordnet, kann sie nicht mehr geändert werden. Teilnehmer können nur gegenseitig Meldungen austauschen, wenn sie derselben Umgebung zugeordnet sind und für den entsprechenden Meldungstyp autorisiert sind. Meldungstypen (Geschäftsfälle) sind unabhängig von der Umgebung. Teilnehmer der Umgebung «test» erhalten eine Teilnehmer-ID (sedex-ID) mit Präfix «T».

3.2 sedex-Meldungstyp

Jede Domäne definiert ihre eigenen sedex-Meldungstypen. Ein Meldungstyp entspricht einem Geschäftsfall, der zwischen den sedex-Teilnehmern abgewickelt wird. Jede sedex-Meldung wird einem Meldungstyp zugeordnet. Dies erfolgt durch den Eintrag der entsprechenden Nummer (Message Type ID) im sedex-Umschlag.

Ein Meldungstyp besteht aus: Message Type ID, Name, Beschreibung, Status (active/inactive) und ist genau einer Domäne zugewiesen.

Unter [Message Types directory \(sedex.swiss\)](https://sedex.swiss/MessageTypesDirectory) wird eine täglich aktualisierte Liste aller aktiven sedex-Meldungstypen publiziert.

3.3 Autorisierung Meldungstyp

Damit ein sedex-Teilnehmer Meldungen eines Meldungstyps senden oder empfangen kann, muss er für diesen Meldungstyp autorisiert sein. Dabei muss dem Teilnehmer pro Meldungstyp eines der folgenden Rechte (Privilege) erteilt werden:

Privilege	Beschreibung
Initiator	Der Teilnehmer kann Geschäftsfälle des Meldungstyp auslösen (Meldungsklasse 0) und eingehende Meldungen des Meldungstyps empfangen und beantworten.
Sender	Der Teilnehmer kann eingehende Meldungen des Meldungstyps empfangen und beantworten (Meldungen mit Meldungsklasse > 0), aber keine Geschäftsfälle des Meldungstyp auslösen (Meldungsklasse 0)
Receiver	Der Teilnehmer kann Meldungen des Meldungstyp nur empfangen.

3.3.1 Domänenübergreifende Übermittlung (Cross-domain messaging)

sedex-Meldungen können zwischen Teilnehmern unterschiedlicher Domänen ausgetauscht werden. Dazu müssen beide Teilnehmer für den entsprechenden Meldungstyp autorisiert sein. Voraussetzung dafür ist die Genehmigung dieser Autorisierung sowohl durch die Domäneninhaberin des Teilnehmers als auch der Domäneninhaberin des Meldungstyps.

3.4 Domänenverwaltung

Nur die von der Domäneninhaberin autorisierten Domänenvertreter und Domänenvertreterinnen können neue Meldungstypen, sedex-Teilnehmer, sedex-Teilnehmerzertifikate, Routingregeln und Konfigurationsänderungen in Auftrag geben. Die autorisierten Vertreter einer sedex-Domäne können auf der sedex-Kundenplattform ihre Domäne verwalten.

3.4.1 Teilnehmerverwaltung

Die Teilnehmer können in der Kundenplattform eingesehen und die folgenden Aufträge online erfasst werden. Nach Freigabe der Aufträge durch den sedex-Support werden diese Änderungen in die sedex-Plattform übernommen.

- Erstellung neuer Teilnehmer
- Aktivierung oder Deaktivierung von Teilnehmern
- Ändern der Namen oder Angaben zu Inhaberinnen von Teilnehmern
- Erteilen, Ändern oder Deaktivierung von Berechtigungen für Meldungstypen der eigenen Domäne
- Erstellen, Ändern oder Deaktivierung von Routingregeln logischer Teilnehmer auf Router der eigenen Domäne
- Ändern des Teilnehmertyps (physisch/logisch)

Folgende Aufträge können nicht in der Kundenplattform erfasst werden und müssen beim sedex-Support bestellt werden.

- Bestellen von neuen sedex-Teilnehmerzertifikaten
- Übertragung von Teilnehmern in eine andere Domäne
- Erteilen, Ändern oder Deaktivierung von Berechtigungen für Meldungstypen einer fremden Domäne.
- Erstellen, Ändern oder Deaktivierung von Routingregeln auf Router einer fremden Domäne.

Domänenübergreifende Aufträge benötigen die Autorisierung von Vertretern beider Domänen.

Die Bearbeitung erfolgt in der Regel innerhalb Tagesfrist aber spätestens nach zehn Arbeitstagen.

3.4.2 Router Verwaltung

Die sedex-Router können in der Kundenplattform analog zu den sedex-Teilnehmern verwaltet werden. Die Routingregeln werden bei den logischen Teilnehmern verwaltet.

3.4.3 Verwaltung der Meldungstypen

Meldungstypen können in der Kundenplattform eingesehen, aber nicht direkt bearbeitet werden. Die folgenden Vorgänge müssen beim sedex-Support bestellt werden:

- Erstellung neuer Meldungstypen
- Aktivierung oder Deaktivierung von Meldungstypen
- Ändern der Namen oder Beschreibung von Meldungstypen

Die Übertragung von Meldungstypen in eine andere Domäne benötigt die Autorisierung von Vertretern beider Domänen.

Die Bearbeitung erfolgt in der Regel innerhalb Tagesfrist aber spätestens nach zehn Arbeitstagen.

3.5 Reporting

Die folgenden Reports stehen den Domänenverantwortlichen zur Verfügung und können beim sedex-Support bestellt werden:

3.5.1 Periodische Reports

Name	Versand	Beschreibung
incomplete message transmissions [domain]	täglich	Die Meldungen aller Meldungstypen einer Domäne, deren Übermittlung fehlgeschlagen ist oder deren Empfang in den letzten 30 Tagen nicht erfolgreich quittiert wurde.
status reports [domain]	monatlich	Verschiedene Informationen zu Status und Konfiguration der Teilnehmer und Meldungstypen einer Domäne
traffic reports [domain] [PREVIOUS_MONTH]	täglich	Anzahl abgesendeter und empfangener Meldungen und Datenvolumen nach Teilnehmer im letzten Monat.
traffic reports [domain] [PREVIOUS_YEAR]	jährlich	Anzahl abgesendeter und empfangener Meldungen und Datenvolumen nach Teilnehmer im letzten Kalenderjahr.
traffic reports [domain] [PREVIOUS_12_MONTHS]	monatlich	Anzahl abgesendeter und empfangener Meldungen und Datenvolumen nach Teilnehmer in den letzten Monaten.
message list [domain] [PREVIOUS_DAY]	täglich	Die einzelnen Meldungen aller Meldungstypen einer Domäne, welche am Vortag gesendet wurden.
message list [domain] [PREVIOUS_MONTH]	monatlich	Die einzelnen Meldungen aller Meldungstypen einer Domäne, welche im Vormonat gesendet wurden.

3.5.2 Ad-hoc Reports

Name	Beschreibung
default_routings [domain]	Aufstellung aller logischen Teilnehmer aller Router einer Domäne.
traffic reports [domain] [period]	Anzahl abgesendeter und empfangener Meldungen und Datenvolumen im nach Teilnehmer in einer bestimmten Periode.
message list [domain][participant(s)][message id(s)][period]	Die einzelnen Meldungen für alle Meldungstypen einer Domäne in einer bestimmten Periode, optional einschränkbar auf bestimmte Teilnehmer oder bestimmte message Ids (usmid einer Meldung)

4 sedex Messaging

Der Anschluss an sedex ermöglicht den sicheren und nachvollziehbaren Datenaustausch zwischen den Fachapplikationen der angeschlossenen Teilnehmer. Die Übermittlung zwischen zwei **sedex-Clients** erfolgt asynchron über die **sedex-Plattform**. Dabei werden die **sedex-Teilnehmerzertifikate** für die Authentisierung, Autorisierung sowie Ver- und Entschlüsselung verwendet. Die Integration der Fachapplikationen erfolgt über das **sedex-Postfach**. Für die Integration logischer Teilnehmer wird ein **Message Dispatching** eingesetzt.

4.1 sedex-Plattform

Der sedex-Server übernimmt das Routing der Meldungen, die Autorisierung sowie die zentrale Protokollierung des Meldeverkehrs. **Die sedex-Plattform wird in den Rechenzentren des Bundesamts für Informatik und Telekommunikation BIT mit Standort Schweiz betrieben** und permanent überwacht.

Der Datenaustausch zwischen den Teilnehmern erfolgt asynchron in End-to-End verschlüsselter Form über die sedex-Plattform. Nach maximal 31 Tagen werden die vom Empfänger nicht abgeholten Daten auf der sedex-Plattform gelöscht. Der Sender erhält zu jeder versendeten Meldung vom System sedex eine Quittung pro Empfänger.

Nach erfolgreicher Zustellung wird dem Absender eine positive Quittung ausgestellt, zudem werden die übertragenen Daten auf der sedex-Plattform gelöscht. Kann die Zustellung aus irgendwelchen Gründen nicht erfolgen, erhält der Absender spätestens nach 31 Tagen eine negative Quittung mit der Begründung. Alle Transaktionen werden protokolliert. Die Nachvollziehbarkeit ist zu jedem Zeitpunkt gewährleistet. Die Transaktionsprotokolle werden mindestens zehn Jahre aufbewahrt.

Die Angaben in den technischen Quittungen (Receipts) erlauben dem sendenden Teilnehmer das grundlegende Verfolgen einer sedex-Meldung. In den meisten Fällen reicht diese Form der Meldungsverfolgung (Message Tracking) für Teilnehmer aus. Im besonderen Bedarfsfall können ausführliche Transaktionsprotokolle von Meldungen beim sedex-Support bestellt werden.

Eine sedex-Meldung kann auch gleichzeitig an mehrere Teilnehmer adressiert werden. Jeder physische Empfänger erhält dabei seine eigene für ihn verschlüsselte Datendatei (Payload). Eine solche Meldung wird nur dann übermittelt, wenn alle Empfänger für den Empfang des verwendeten Meldungstyps autorisiert sind. Ist schon nur ein Empfänger nicht autorisiert, wird die Übermittlung an alle Empfänger abgebrochen.

4.2 sedex-Client Software

Der sedex-Client ist eine Software, welche die Fachapplikation der sedex-Teilnehmer mit der sedex-Plattform verbindet. In der Regel wird der sedex-Client auf dem gleichen Host wie die Fachapplikation betrieben oder ist für die Fachapplikation über das Netzwerk sicher zugänglich.

Der sedex-Client ist eine Java-basierte Anwendung, die auf physischen oder virtuellen Maschinen mit verschiedenen Betriebssystemen (einschliesslich Windows, macOS, Linux, AIX usw.) installiert werden kann.

Der sedex Client kann auf verschiedene Arten installiert und betrieben werden:

- als eigenständige Installation auf einem Host mit manuellem Start/Stop der Applikation oder als permanent laufender Hintergrunddienst.
- als Docker-Container auf einer Container-Plattform. sedex veröffentlicht den sedex-Client als offizielles Container-Image auf Docker Hub. Der sedex-Client-Container kann auf einer Container-Plattform wie Docker, Kubernetes, OpenShift, etc. betrieben werden.

Da beide Installationsarten die gleiche Funktionalität bieten, hängt die Wahl in erster Linie von den technischen und organisatorischen Anforderungen und Präferenzen der Organisation ab, die den sedex-Client hostet.

4.2.1 Dokumentation und Software

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

Software: [sedex Downloads](#)

4.3 sedex-Teilnehmerzertifikat

Ein sedex-Teilnehmer muss sich mit einem speziellen sedex-Teilnehmerzertifikat ausweisen können. Dieses sedex-Teilnehmerzertifikat entspricht einem Organisationszertifikat (spezifische Class-C Zertifikate) und wird für die Zwecke Authentisierung, Autorisierung sowie Ver- und Entschlüsselung verwendet. Der Bezug, die Verwaltung und Nutzung der sedex-Teilnehmerzertifikate erfolgt automatisiert über eine Zertifikats-Plattform auf Basis der [Swiss Government PKI](#).

Die sedex-Zertifikate werden durch den sedex-Client beim Teilnehmer generiert. So ist sichergestellt, dass der zu einem Zertifikat gehörende Private Key nur dem Teilnehmer bekannt ist. Die Zertifikate haben eine Gültigkeit von drei Jahren. Das Teilnehmerzertifikat selbst ist öffentlich. **Hingegen sind der Private Key (P12-Datei) sowie das zugehörige Passwort Sicherheitskomponenten. Sicherheitskomponenten dürfen nicht kopiert (Sicherheitsbackup und redundante Systeme ausgenommen) und / oder an Dritte weitergereicht werden. Die Verwendung der Sicherheitskomponenten ausserhalb des sedex-Client ist nicht erlaubt.** Bei einem Widerruf oder nach dem Ablauf des Zertifikats ist die Nutzung der sedex-Plattform per sofort nicht mehr möglich.

Das Zertifikat wird durch den sedex Client rechtzeitig automatisch erneuert. Damit auch Meldungen, welche mit dem alten Zertifikat verschlüsselt wurden, entschlüsselt werden können, sind während einer gewissen Zeit sowohl das alte als auch das neue Zertifikat gültig. **Voraussetzung für die automatische Erneuerung des Zertifikats ist das Einhalten der [betrieblichen Nutzungsrichtlinien](#).**

4.4 sedex Postfach

Jeder sedex-Teilnehmer besitzt sein eigenes Postfach. Das Postfach besteht aus den folgenden Ablagen:

Ablagen	Beschreibung
Inbox	Ablage der empfangenen Meldungen
Outbox	Ablage der zu sendenden Meldungen
Receipts	Ablage für die technischen Quittungen zu den versendeten Meldungen
Processed	Ablage für die versendeten Meldungen, unabhängig vom Erfolg der Übermittlung

Der Zugriff der Fachapplikation auf das sedex Postfach erfolgt über den sedex-Client entweder über das sedex File System Messaging Interface oder die sedex Messaging REST API. Die Wahl des Interfaces kann bei Bedarf je nach Meldungstyp gewählt werden. Der Meldungsaustausch zwischen Teilnehmern ist unabhängig von deren Wahl des Interfaces. Sender und Empfänger können damit das Interface frei wählen.

4.4.1 sedex File System Messaging Interface

Der Zugriff der Fachapplikation erfolgt datei-basiert (File I/O). Dabei liegen die Meldungen unverschlüsselt in den Dateiablagen (Ordner Inbox, Outbox, Receipts). Der Schutz der Dateien ist in der Verantwortung des Betreibers des Filesystems. Die Ablagen werden bei der Installation des sedex-Clients automatisch erstellt.

4.4.2 sedex Messaging REST API

Eine Fachapplikation kann sedex-Meldungen auch über ein https-basiertes Messaging REST API versenden und empfangen. Für die Fachapplikation wird für den Zugriff auf die Messaging REST-API ein eigener Benutzer («technical user») im sedex-Client angelegt. Mit diesem Benutzer kann die Fachapplikation direkt mit dem sedex-Client die sedex-Meldungen austauschen. Da bei Verwendung der Messaging REST API die Meldungen verschlüsselt in der lokalen Datenbank des sedex-Clients gespeichert werden und der Kanal zwischen Fachapplikation und sedex-Client über TLS verschlüsselt wird, ist hier der sichere Datenaustausch zwischen sedex-Client und Fachapplikation gewährleistet. Bei beidseitiger Nutzung durch Sender und Empfänger der REST-Schnittstelle können die Daten somit während der gesamten Übermittlung verschlüsselt zwischen den Fachapplikationen ausgetauscht werden.

4.5 Message Dispatching

Analog zum Zugriff eines physischen Teilnehmers auf sein Postfach, kann beim Einsatz eines sedex-Routers auch die interne Meldungsverteilung an die logischen Teilnehmer (Message Dispatching) entweder über das sedex File System Messaging Interface oder die sedex Messaging REST API erfolgen. Die Wahl des Interface kann bei Bedarf je nach Meldungstyp und je nach logischem Teilnehmer gewählt werden. Der Meldungs austausch zwischen Teilnehmern ist unabhängig von deren Wahl des Interfaces. Sender und Empfänger können damit das Interface frei wählen.

4.5.1 Message Dispatching mit sedex File System Messaging Interface

Beim datei-basierten (File I/O) Zugriff muss der Betreiber des sedex-Routers das Message Dispatching zwischen der Fachapplikation des logischen Teilnehmers und dessen sedex-Routers selbst bereitstellen. Analog einer Hauspost, muss dieser einen sicheren Mechanismus implementieren, um eine eingehende Meldung der adressierten Fachapplikation weiterzureichen bzw. eine von dieser versendete Meldung abzuholen. Dabei ist zu beachten, dass eine sedex-Meldung, welche an mehrere logischen Teilnehmer des Routers gesendet wird, nur einmal in der Inbox erscheint. **Der Message Dispatcher muss diese für jeden logischen Teilnehmer duplizieren.** Es gibt frei verfügbare Drittprodukte aus dem sedex-Ökosystem, welche dieses Message Dispatching übernehmen können, beispielsweise der [Open eGov MessageHandler für sedex](#). **Der sedex-Support bietet jedoch keinen Support für Drittprodukte.**

4.5.2 Message Dispatching mit sedex Messaging REST API

Beim Zugriff via Messaging REST API ist das Message Dispatching bereits im sedex-Client integriert. Für die Fachapplikation des logischen Teilnehmers des sedex-Routers wird für den Zugriff auf die Messaging REST-API ein eigener Benutzer im sedex-Client angelegt. Mit diesem Benutzer kann die Fachapplikation direkt mit dem sedex-Client des sedex-Routers die sedex-Meldungen austauschen. Da bei Verwendung der Messaging REST API die Meldungen verschlüsselt in der lokalen Datenbank des sedex-Clients des sedex-Routers gespeichert werden und der Kanal zwischen Fachapplikation und sedex-Client über TLS verschlüsselt wird, ist hier der sichere Datenaustausch zwischen dem sedex-Client des sedex-Routers und Fachapplikation gewährleistet. **Das Duplizieren von sedex-Meldungen, welche an mehrere logischen Teilnehmer des sedex-Routers versendet werden, ist bei Verwendung der Messaging REST API bereits integriert.**

5 Webservices

5.1 sedex Webservice-Proxy (sedex WS-Proxy)

Der sedex Webservice-Proxy (kurz: sedex WS-Proxy) ist eine Komponente des sedex-Clients, mit welcher die Fachapplikationen des Teilnehmers über einen gesicherten Zugang die für den Teilnehmer autorisierten Webservices von sedex und Drittanbietern (siehe Webservice Anbieter Plattform) nutzen können.

5.2 sedex Webservices

Die Konfiguration für die sedex Webservices sind im sedex-Client enthalten und alle sedex-Teilnehmer sind autorisiert diese über den sedex-WS-Proxy zu nutzen. Anbieterin (Provider) des Webservice ist die sedex-Plattform.

5.2.1 sedex Webservice: check-sedex

Dieser Webservice dient der Abfrage von sedex-Teilnehmern und deren Autorisierungen. Er prüft die wesentlichen Elemente des sedex-Umschlags und kann von einer sendenden Fachapplikation optional für eine Vorprüfung genutzt werden, um zu prüfen, ob eine bestimmte sedex-Meldung erfolgreich an die vorgesehenen Empfänger übertragen werden kann. Geprüft werden:

- sedex-IDs von Absender und Empfänger sind gültig.
- Sender und Empfänger sind aktive sedex-Teilnehmer.
- Sender und Empfänger haben gültige Zertifikate.
- Der Sender ist autorisiert, Meldungen dieses Typs zu versenden.
- Der Empfänger ist autorisiert, Meldungen dieses Typs zu empfangen.
- Die Grösse der Nutzdatendatei übersteigt nicht das maximal zulässige Limit (optionale Prüfung).

5.2.2 sedex Webservice: sedex external authorization service

Dieser Webservice dient der Abfrage von sedex-Teilnehmern und deren Authentisierung und Autorisierungen auf Basis der sedex-Zertifikate. Verwendet wird dieser Service von Webservice Providern, welche ihren Webservice über den sedex WS-Proxy zugänglich machen wollen und prüfen wollen, ob eine aus dem Internet eingehende SOAP-Anfrage von einem sedex-Teilnehmer stammt und ob dieser berechtigt ist.

5.3 Webservice Anbieter Plattform

Mit dem sedex-Client kann auch eine synchrone Datenkommunikation abgewickelt werden. Es wird eine verschlüsselte Datenkommunikation zwischen Nutzer (Consumer) und Anbieter (Provider) eines Webservices sichergestellt, ohne Einfluss auf die Inhalte zu nehmen.

Den sedex-Teilnehmern, welche Webservices konsumieren wollen, wird eine vereinfachte und einheitliche Implementierung dieser Services angeboten. Dazu baut die Fachapplikation eine Verbindung innerhalb der geschützten Infrastruktur des Teilnehmers auf den WS-Proxy des sedex-Clients auf. Ist der sedex-Teilnehmer für einen Webservice autorisiert bezieht der sedex-Client die für den Aufruf des Webservices notwendige Konfiguration automatisch von der sedex-Plattform.

So kann sich der Webservice Consumer darauf verlassen, dass der tatsächlich gewünschte Webservice Provider Auskunft gibt. Und der Webservice Provider kann die Authentizität und Autorisierung des Consumer prüfen.

Aktuell stehen die nachfolgenden Webservices zur Verfügung:

Webservices	Provider	Link
UPIServices	Zentrale Ausgleichsstelle ZAS	Schnittstelle UPIServices (admin.ch)
Abfragedienst VSED	Verband Schweizerischer Einwohnerdienste (VSED)	Verband Schweizerischer Einwohnerdienste (VSED) Abfrage Versichertenkarte
eUmzugCH – Personen Identifikation	eOperations Schweiz AG	eUmzugCH › eOperations
UID-Webservice	Bundesamts für Statistik BFS	UID-Schnittstellen Bundesamt für Statistik (admin.ch)
GWR Webservices	Bundesamt für Statistik BFS	Gebäude- und Wohnungsregister Bundesamt für Statistik (admin.ch)
Identifikator für das elektronische Patientendossier	Zentrale Ausgleichsstelle ZAS	Der Identifikator für das elektronische Patientendossier (admin.ch)

Den vom sedex Webservice-Proxy vermittelten Webservices der Webservice Provider sind Meldungstypen zugeordnet. Die Verwaltung der Rechte für die Nutzung erfolgt analog der Verwaltung der Rechte für die Nutzung von sedex-Meldungen. Die Zugangspunkte für die Webservices werden in der sedex-Plattform verwaltet. Die Konfiguration des sedex WS-Proxy für die Nutzung eines Webservices erfolgt bei den berechtigten Teilnehmern automatisch.

6 Nutzungskonditionen

6.1 Betriebliche Nutzungsrichtlinien

Die Inhaberin eines physischen sedex-Teilnehmers ist verpflichtet die folgenden betrieblichen Richtlinien einzuhalten:

- Der sedex-Client ist eine Sicherheitskomponente, die zwingend auf dem aktuellen Stand zu halten ist. Der sedex-Client muss mindestens einmal pro Jahr auf die neueste Version ([recommended version](#)) des sedex-Clients aktualisiert werden.
- Um den zuverlässigen Meldungs austausch und die automatische Zertifikatserneuerung zu gewährleisten, sollte ein sedex-Client möglichst ständig in Betrieb sein.
- Die Verwendung der Sicherheitskomponenten des sedex-Teilnehmerzertifikats (Private Key und das zugehörige Passwort) ausserhalb des sedex-Clients ist nicht erlaubt.
- Es muss sichergestellt werden, dass keine doppelten Instanzen auftreten. Doppelte Instanzen sind mehrere sedex-Client Installationen, die sich mit derselben Identität melden und dasselbe sedex-Teilnehmerzertifikat sowie dieselbe sedex-ID verwenden. Dies kann beispielsweise vorkommen, wenn der sedex-Client auf einem neuen Host installiert und der sedex-Client auf dem alten Host nicht ordnungsgemäss zurückgebaut wurde.

Der sedex-Support kann Teilnehmer, welche die betrieblichen Richtlinien nicht einhalten, aufgrund der Version ein Sicherheitsproblem darstellen oder technische Probleme verursachen, umgehend deaktivieren und deren Zertifikate revozieren.

6.2 sedex Client Life Cycle Management

6.2.1 Versionsstatus

Status einer Version	Beschreibung
Recommended	Aktuellste und empfohlene Version. Nur diese Version steht im Download zur Verfügung
Supported	Unterstützte Version. Neue Versionen der sedex-Plattform oder Änderungen an der Infrastruktur werden ausschliesslich an unterstützten sedex-Client Versionen getestet. Der Support wird nur auf diesen Versionen geschult. Versionen sind in der Regel 18 Monate nach dem Release unterstützt. Der sedex-Support kann problematische Versionen umgehend auf den Status «Unsupported» setzen.
Unsupported	Das Zertifikat des sedex-Clients wird nicht mehr erneuert. Allfällige Probleme können unter Umständen nicht reproduziert oder nachvollzogen werden. Bei Support-Anfragen wird zunächst ein Update auf die neueste (recommended) sedex-Client Version vorausgesetzt.

6.2.2 Unterstützte Versionen

Die aktuell unterstützten Versionen werden auf www.sedex.ch publiziert (dort nicht aufgeführte Versionen sind im Status «Unsupported»)

6.3 Nutzungsgebühren

Die Finanzierung von sedex erfolgt kostenneutral und wird durch die sedex-Domänen bereitgestellt. Das Modell der sedex Nutzungsgebühren strebt eine faire Verteilung der Gesamtkosten von sedex auf die sedex-Domänen gemäss ihrer effektiven Nutzung von sedex an. Die zugrunde liegenden Kostenallokationsschlüssel werden regelmässig überprüft.

Seit dem 1. Januar 2025 gelten folgende sedex Nutzungsgebühren.

Artikel	Gebühr exkl. MWST
Jahresgebühr physischer Teilnehmer	Fr. 360.–
Jahresgebühr logischer Teilnehmer	Fr. 120.–
Gebühr pro versendete Meldung	Fr. –.01
Gebühr versendete Daten pro MB	Fr. –.12

Aufgrund der weiterhin stark steigenden Nutzung von sedex sowie sich veränderndem Nutzungsverhalten wird das Preismodell jährlich an die Gesamtnutzung aller sedex-Domänen und die Kostenentwicklung angepasst. Das für das kommende Folgejahr gültige Preismodell wird in der Regel Ende September/ Anfang Oktober publiziert. Sofern Preissteigerungen notwendig werden, werden diese in der Regel mit einem Vorlauf von mindestens 12 Monaten für das übernächste Jahr angekündigt.

Die Verrechnung der Nutzungsgebühren für das Rechnungsjahr *RJ* erfolgt mit einer jährlichen Rechnungstellung im *RJ* auf Basis von vereinbarten Planwerten für dieses Jahr mit einer Korrektur der Differenz zur tatsächlichen Nutzung im Folgejahr.

Die Korrektur im Folgejahr erfolgt für:

- Die Meldungsgebühren auf Basis der Anzahl der abgesendeten Meldungen (Anzahl erstellter Message IDs und Datenvolumen pro adressierte Empfänger) der Periode 01.10.*VJ* – 30.09.*RJ* (Vorjahr $VJ=RJ-1$).
- Die Teilnehmergebühren auf Basis der Anzahl aktiver, physischer und logischer Teilnehmer am Stichtag 30.09.*RJ*.

6.4 Service Level

Für die sedex-Services gelten die folgenden Service-Level.

6.4.1 sedex-Support

Element	Service Level
Supportzeit	Montag bis Freitag jeweils 8.30 bis 12 Uhr und 13.30 bis 16 Uhr

6.4.2 sedex-Plattform

Element	Service Level								
Servicezeit	Montag bis Sonntag jeweils von 0 bis 24 Uhr								
Wartung	Sonntag 8 bis 22 Uhr für Major Changes, systemübergreifende Wartung								
Verfügbarkeit pro Quartal	<table> <tr> <td>maximale Ausfallzeit pro Ausfall:</td><td>8 Stunden</td></tr> <tr> <td>maximale Anzahl Ausfälle:</td><td>3</td></tr> <tr> <td>maximale Wiederherstellungszeit:</td><td>8 Stunden</td></tr> <tr> <td>maximale Datenverlustzeit:</td><td>2 Stunden</td></tr> </table>	maximale Ausfallzeit pro Ausfall:	8 Stunden	maximale Anzahl Ausfälle:	3	maximale Wiederherstellungszeit:	8 Stunden	maximale Datenverlustzeit:	2 Stunden
maximale Ausfallzeit pro Ausfall:	8 Stunden								
maximale Anzahl Ausfälle:	3								
maximale Wiederherstellungszeit:	8 Stunden								
maximale Datenverlustzeit:	2 Stunden								
Schutzniveau	Grundsatz: erlaubt die Bearbeitung von nicht öffentlich zugänglichen Personen-daten und Datensammlungen gemäss Datenschutzgesetz DSG.								

6.4.3 Zertifikats-Plattform

Element	Service Level	
Servicezeit	Montag bis Freitag jeweils von 7 bis 18 Uhr	
Wartung	Mittwoch 18 Uhr bis Donnerstag 6 Uhr	
Verfügbarkeit pro Quartal	maximale Ausfallzeit pro Ausfall:	12 Stunden
	maximale Anzahl Ausfälle:	3
	maximale Wiederherstellungszeit:	12 Stunden
	maximale Datenverlustzeit:	4 Stunden
Schutzniveau	Grundschutz: erlaubt die Bearbeitung von nicht öffentlich zugänglichen Personen- daten und Datensammlungen gemäss Datenschutzgesetz DSG.	

6.4.4 sedex-Kundenplattform

Element	Service Level	
Servicezeit	Montag bis Sonntag jeweils von 0 bis 24 Uhr	
Wartung	Nach Absprache	
Verfügbarkeit pro Quartal	maximale Ausfallzeit pro Ausfall:	2 Arbeitstage
	maximale Anzahl Ausfälle:	3
	maximale Wiederherstellungszeit:	Best Effort
	maximale Datenverlustzeit:	Best Effort
Schutzniveau	Grundschutz: erlaubt die Bearbeitung von nicht öffentlich zugänglichen Personen- daten und Datensammlungen gemäss Datenschutzgesetz DSG.	

7 Help Center

7.1 sedex-Support

Der sedex-Support unterstützt bei:

- Fragen bezüglich der sedex-Teilnehmerzertifikate,
- der Konfiguration der sedex-Teilnehmer,
- Fragen zur Installation und dem Betrieb des sedex-Clients,
- der Definition der Geschäftsfälle und sedex-Meldungstypen,
- der Bereitstellung von Nutzungsberichten und Transaktionsprotokollen und
- weiteren sedex spezifischen Problemen.

Ausgeschlossen sind Leistungen bezüglich Fachapplikationen, Peripheriegeräten, Informatik- und Kommunikationsinfrastrukturen der Endbenutzer sowie alle in diesem Servicekatalog nicht explizit aufgeführten Leistungen.

Der sedex-Support kann über folgende Kanäle kontaktiert werden:

- E-Mail: sedexsupport@bfs.admin.ch
- Telefon: 0800 866 700

7.2 Technical user documentation for the sedex-Client

In unserer [Anwenderdokumentation \(docs.sedex.admin.ch\)](https://docs.sedex.admin.ch) finden Sie neben den aktuellen sedex-Clients und Release Notes auch umfassende technische Erläuterungen zu den verschiedenen Betriebsformen eines sedex Clients und zur Integration von sedex in eine Fachapplikation. Diese Dokumentation wendet sich an IT-Spezialisten, welche sedex-Clients betreiben oder sedex in ihre Fachapplikation integrieren, und ist nur in Englisch verfügbar.

7.3 sedex NewsMail

Mit der sedex NewsMail informieren wir Sie über die folgenden sedex-Themen:

- Veröffentlichungen neuer Versionen des sedex-Clients
- Service-Meldungen (Benachrichtigungen über zukünftige Wartungen und Unterbrechungen von sedex)
- Allgemeine Informationen zu sedex

Anmeldung: [sedex NewsMail abonnieren](#)

7.4 sedex directories

In [sedex directories \(www.sedex.swiss\)](http://www.sedex.swiss) finden Sie die Verzeichnisse der [sedex-Teilnehmer](#), [sedex-Meldungstypen](#) und [sedex-Domänen](#). Die Verzeichnisse werden täglich aktualisiert.

8 Monitoring

8.1 sedex Client check

Für die Prüfung der korrekten Funktionsweise eines sedex-Clients stehen verschiedene Werkzeuge zur Verfügung.

8.1.1 sedex Client Pinger

Falls Sie überprüfen wollen, ob Ihr sedex-Teilnehmer grundsätzlich für den Meldungs austausch korrekt installiert ist, kann der sedex-Support mit dem sedex Client Pinger Ihrem Teilnehmer eine Testmeldung senden und die technische Quittung auswerten.

8.1.2 Monitoring-Seite des sedex-Clients

Die lokale Monitoring-Seite des sedex-Clients enthält eine Liste von Schlüssel/Wert-Paaren für die Überwachung von Operationen. Die Monitoring-Seite kann über HTTP oder über das Dateisystem aufgerufen werden.

8.2 sedex System status

Im Auftrag des Bundesamtes für Statistik (BFS) betreibt das Bundesamt für Informatik und Telekommunikation (BIT) die sedex-Plattform und überwacht dessen Betrieb mit verschiedenen Monitoring Systemen. Das Operation Control Center des BIT (OCC) stellt ein Monitoring zur Verfügung, um den Stand und die Verfügbarkeit des Systems zu prüfen (nur vom BV-Netz zugänglich): [00 Dash-boardSHVMain - Berichts-Viewer \(admin.ch\)](#).

9 Sicherheit

9.1 Verschlüsselung

Eine der zentralsten Anforderungen an die Datenübertragung von sedex ist die Sicherheit der übertragenen Daten, d.h. deren Schutz vor Ausspähung und Veränderung. Um die hohen Sicherheitsanforderungen zu gewährleisten, setzt sedex auf Dreifachverschlüsselung auf der Basis bewährter und als state-of-the-art anerkannten Verschlüsselungsverfahren:

1. End-to-End Meldungsverschlüsselung
2. OSCI-Transportverschlüsselung
3. TLS-Kanalverschlüsselung

Somit wird der Inhalt einer sedex-Meldung effektiv dreifach verschlüsselt über das Internet übertragen und ist kryptografisch gleich mehrfach gesichert vor Ausspähung und Veränderung.

Nachfolgend sind die drei Ebenen der kryptografischen Absicherung erläutert.

9.1.1 End-to-End Meldungsverschlüsselung

Die Meldungsübertragung erfolgt in sedex End-to-End verschlüsselt. D.h. es ist auf der Basis asymmetrischer Kryptografieverfahren konzeptionell sichergestellt, dass eine Meldung vom versendenden sedex-Client so verschlüsselt wird, dass einzig der adressierte Empfänger die Meldung wieder entschlüsseln kann.

Dieses Verfahren garantiert, dass die Meldung auf ihrem Weg jederzeit sicher verschlüsselt ist und von niemandem und nichts eingesehen oder verändert werden kann. Selbst auf dem sedex-Server wird die Meldung verschlüsselt zwischengespeichert. Einzig der adressierte Empfänger kann die Meldung vom sedex-Server abholen und die Meldung entschlüsseln.

Zusammenfassend garantiert sedex die End-to-End Verschlüsselung:

1. Vertraulichkeit: Einzig der adressierte Empfänger kann die Meldung entschlüsseln und lesen
2. Unveränderbarkeit: Garantierte Echtheit des Meldungsinhalts
3. Herkunft: Garantierte Echtheit des Absenders

9.1.2 OSCI-Transportverschlüsselung

Für den Transport einer Meldung vom sendenden sedex-Client auf den sedex-Server und vom sedex-Server zum empfangenden sedex-Client verwendet sedex mit dem Produkt Governikus einen zertifizierten Message-Hub nach dem OSCI-Standard. Eine (bereits End-to-End verschlüsselte) sedex-Meldung wird dabei in Form einer oder mehrerer zusätzlich verschlüsselter OSCI-Meldungen übertragen. Hierzu ist jede OSCI-Meldung mittels OSCI-Transportverschlüsselung zusätzlich gesichert.

9.1.3 TLS-Kanalverschlüsselung

Die gesamte Kommunikation zwischen sedex-Clients und dem sedex-Server erfolgt über das mit TLS abgesicherte https-Protokoll.

9.2 Authentisierung

Die Authentisierung der sedex-Teilnehmer erfolgt auf der Basis ihrer sedex-Teilnehmerzertifikate (.X509-Organisationszertifikate Klasse C). Dadurch ist sichergestellt, dass nur identifizierte und zugelassene Organisationen am sedex-Verbund teilnehmen können.

9.3 Autorisierung

sedex verfügt über ein eigenes im System verankertes Berechtigungssystem zur Kontrolle des Meldungsflusses. Pro Meldungstyp können die Autorisierungen jedes Teilnehmers einzeln definiert werden. Vom System wird durchgesetzt, dass von einem Teilnehmer eine Meldung nur dann versendet oder empfangen werden kann, wenn das erforderliche Recht (Privilege) gewährt wurde.

9.4 Datenintegrität

Die verwendeten End-to-End Verschlüsselungs- und Signierv Verfahren auf der Basis bewährter asymmetrischer Kryptografieverfahren garantieren die Geheimhaltung und die Unveränderbarkeit der übertragenen Daten.

10 Gültigkeit

Dieser sedex Servicekatalog gilt ab dem 1. Oktober 2025. Änderungen vorbehalten.