SocietyByte
Wissenschaftsmagazin des BFH-Zentrums Digital Society
https://www.societybyte.swiss

Sedex - der digitale Postbote des Bundes

Autor : Stefan Podolak

Datum : 6. Juni 2019

Mit sedex bieten das Bundesamt für Statistik (BFS) und das Bundesamt für Informatik (BIT) einen sicheren Datenaustausch für Behörden und öffentliche Verwaltungen an. Dabei werden Verschlüsselungen und Sicherheitszertifikate angewendet.

Was ist sedex?

sedex steht für secure data exchange und ist eine Dienstleistung des BFS welche vom Bundesamt für Informatik BIT betrieben wird. Die hochverfügbare Plattform (24/7) wurde im Rahmen der Modernisierung der Volkszählung aufgebaut und ist seit der Inbetriebnahme am 15. Januar 2008 für den sicheren asynchronen Datenaustausch zwischen Organisationseinheiten konzipiert.

Vor diesem Hintergrund waren die ersten sedex Kunden die Einwohnerdienste der Gemeinden, die quartalsweise die Statistiklieferungen ans BFS leisten müssen. Da sensitive Daten ausgetauscht werden, musste die Plattform von Beginn an hohen Anforderungen an die Sicherheit sowie Nachvollziehbarkeit genügen. Dazu setzt sedex moderne

Verschlüsselungsverfahren sowie Sicherheitszertifikate der Swiss Government PKI ein. Seit 2009 kennt die Governance von sedex noch weitere Domänen und interessierte Organisationen können unter bestimmten Voraussetzungen den Service von sedex mitbenutzen.

Im ersten Quartal 2019 wurde sedex von über 6’600 Organisationseinheiten genutzt, die sich auf über 70 Domänen verteilen. Von Januar 2008 bis Ende April 2019 wurden ca. 17.6 Millionen Meldungen via sedex übermittelt.

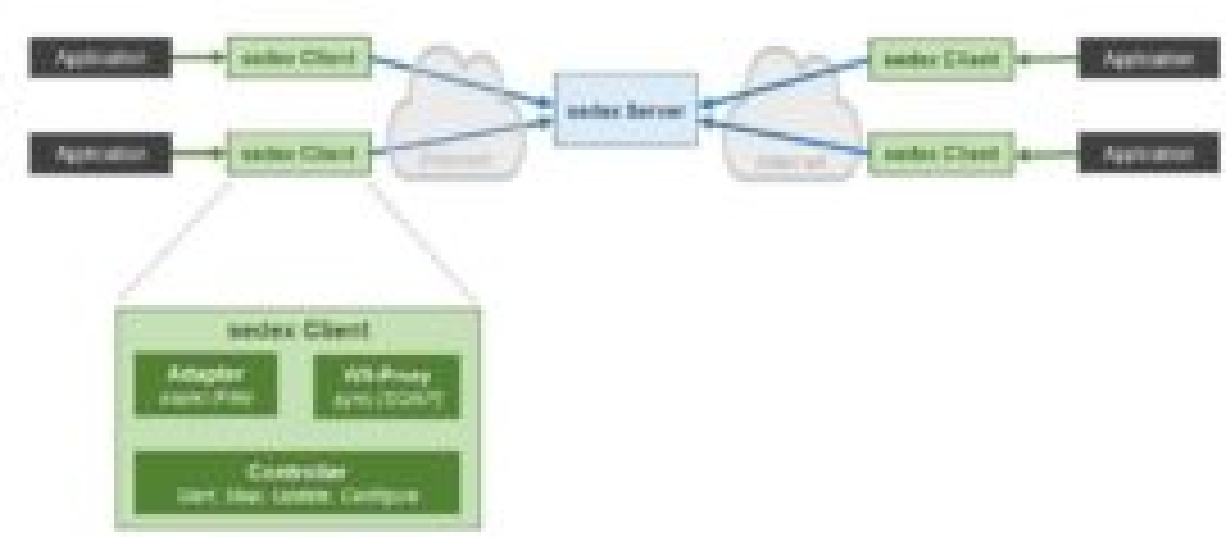
Wer sind die Kunden von sedex?

Der Kundenkreis von sedex ist über sogenannte Domänen geregelt und spannt sich von der kommunalen, über die kantonale Verwaltungsebene bis hin zu diversen Bundesämtern. Man befindet sich immer dann im Einsatzgebiet von sedex, wenn die angewendeten Prozesse einen regelmässigen und gesetzlich geregelten Datenaustausch erfordern, einen stabilen Benutzerkreis darstellen, hohe Sicherheitsanforderungen brauchen und einen Nachvollziehbarkeit der Meldungen notwendig ist. So zählt sedex heute neben den Einwohnerregistern der Gemeinden mit den Statistiklieferungen auch die Betreibungsämter, das Zivilstandsregister, das eidgenössische Gebäude und Wohnungsregister, die Vereinigung der Spitäler H+, eOperations Suisse, SSK, Verein HPI Suisse ePolice, Gemeinsame Einrichtung KVG und viele mehr zu seinen Kunden.

Diese profitieren unter anderem davon, dass sie keine eigene Infrastruktur für den Datentransport aufbauen müssen, die Thematik der Sicherheit durch zwei Bundesämter geregelt und kontrolliert wird, und sie keine eigene Benutzerverwaltung und Supportorganisation aufbauen müssen.

Wie funktioniert sedex?

Der sedex Client (eine Java Applikation) besteht im Wesentlichen aus 3 Komponenten, dem Adapter, dem Webservice Proxy und dem Controller, welche dazu dienen innert Sekunden Meldungen zwischen den sedex Teilnehmer auszutauschen.



Die Hauptaufgabe des Service ist der asynchrone Datenaustausch von einzelnen Meldungen zwischen zwei in der Meldung identifizierten sedex Teilnehmern. Eine Meldung besteht aus einer beliebigen Datendatei (data_) und einem sedex Umschlag (envelope envl_). Die Datendatei kann einem beliebigen Dateiformat entsprechen. Zum Beispiel pdf, docx, zip, jpg, tar, xml usw. Die fachlichen Inhalte oder Konventionen (z.B. Verwendung von Standards) werden von den Domänen geregelt. Der Umschlag ist eine standardisierte XML-Datei gemäss dem eCH Standard eCH-0090.

Die Fachanwendung des Absenders schreibt zunächst die Datendatei in die outbox des sedex Client, danach den zugehörigen Umschlag. Die Datendatei wird mittels dem System public key / private key von Governikus für den Transport verschlüsselt.
Der sedex Client des Absenders verbindet sich anschliessend mit der sedex Plattform und übermittelt die Daten über eine gesicherte Verbindung. Der sedex Client des auf dem Umschlag angegebenen Empfängers holt die Daten auf der sedex Plattform ab und entschlüsselt sie in seiner Infrastruktur. Die Lösung ist technisch so konzipiert, dass nur der Empfänger in der Lage ist, diese Daten zu entschlüsseln. Der Umschlag sowie die Datendatei liegen danach in der inbox des sedex Client. Von dort kann die Fachanwendung des Empfängers die Daten einlesen.

Positive Quittung nach Erhalt

Nach erfolgreicher Zustellung wird dem Absender eine positive Quittung ausgestellt und die Daten auf der sedex Plattform vernichtet. Kann die Zustellung aus irgendwelchen Gründen nicht erfolgen, erhält der Absender eine negative Quittung mit der entsprechenden Begründung. Alle Transaktionen werden protokolliert und die Nachvollziehbarkeit ist zu jedem Zeitpunkt gewährleistet.

Mit dem sedex Client kann auch eine synchrone Datenkommunikation abgewickelt werden. Es

wird eine verschlüsselte Datenkommunikation zwischen Konsument und Anbieter eines Web Service sichergestellt, ohne Einfluss auf die Inhalte zu nehmen. Der Mehrwert liegt darin, den sedex Teilnehmern, welche Web Services konsumieren wollen, eine vereinfachte und einheitliche Implementierung dieser Services anzubieten.

Die Fachanwendung baut eine Verbindung mit dem sedex Client auf. Dies geschieht innerhalb der geschützten Infrastruktur des Teilnehmers. Der sedex Client „weiss“, anhand des Aufrufs, wo der gewünschte Web Service im Internet erreichbar ist und baut einen gesicherten Tunnel dorthin auf.

Der Web Service Konsument kann sich darauf verlassen, dass der tatsächlich gewünschte Web Service Anbieter Auskunft gibt (und nicht ein fingierter). Der Web Service Anbieter (z.B. UPI der zentralen Ausgleichskasse) kann prüfen, ob die Anfrage tatsächlich vom vermeintlichen Konsument erfolgt. Der Web Service Anbieter kann zudem das Berechtigungssystem von sedex einbinden, um die Benutzerverwaltung der Web Service Konsumenten zu vereinfachen.

Der Vorteil und der Erfolg von sedex liegt in der Einfachheit des Systems und der hohen Sicherheit, die es gewährleistet. Das System ist sicher, nachvollziehbar und verlässlich und zählt deshalb immer wie mehr Kunden zu seinem Kreis.