

GBDBS-Schnittstellen-Anbindung für die Landesweite Grundstücksuche

Aktenzeichen:

Zielpublikum dieser Information sind Technikerinnen oder Techniker der Kantone, welche die GBDBS-Schnittstelle in den Kantonen pflegen.

Die Kantone stellen den Abruf der rechtswirksamen Daten des Hauptbuchs und der Daten des Personenidentifikationsregisters durch den Grundstücksuchdienst über die GBDBS sicher. Das BJ oder die Techniker des ISC-EJPD werden nicht auf die Kantone zugehen.

Was haben wir vorbereitet?

Wir verbinden uns mit den GBDBS-Schnittstellen der Kantone über ein Art API Gateway des ISC-EJPD (dem Informatik-Leistungserbringer des EJPD). Das Gateway meldet sich beim Kanton mit einem Zertifikat (mTLS – mutual TLS) und weiss folgende Kriterien auf:

- Der CN (Common Name) enthält folgenden Wert (:
 - Produktive Umgebung: **svcgw-ejpd**
- Es wird die komplette Certificate Chain wie folgt geliefert:
 - **Swiss Government Root CA II (Root)**
 - **Swiss Government Regular CA 01 (Intermediate)**
 - **svcgw-ejpd** oder **svcgw-ejpd-i (Serverzertifikat)**
- Das Root Zertifikat kann, bei Bedarf, direkt von der Webseite des BIT heruntergeladen werden: [Swiss Government Root CA II \(admin.ch\)](#)

Was die Kantone abklären müssen?

- Bereitstellung der produktiven GBDBS Schnittstelle über HTTPS.
- Der Server soll die ganze «Certificate Chain» bereitstellen. Also analog zu dem, was das EJPD bereitgestellt hat.
- Der Server soll ein eindeutiges CN im Zertifikat haben und kein «Wildcard» Zertifikat einsetzen. Z.B.
 - «gbdbbs.kanton.ch» im CN ist gut.
 - «*.kanton.ch» ist hingegen nicht gut.
- Der **Swiss Government Root CA II** soll in den Truststore übernommen werden («vertrauen»), falls dies noch nicht geschehen ist.
Es ist eine Prüfung auf den CN zu definieren.
 - Das ISC-EJPD Gateway auf die Integrationsumgebung (Pre-Prod) hat ein Zertifikat mit CN: **svcgw-ejpd-i**
 - Das ISC-EJPD Gateway auf die Produktionsumgebung (Prod) hat ein Zertifikat mit CN: **svcgw-ejpd**
 - Die Produktivumgebung des Kantons soll die Verbindung auf beide CNs **svcgw-ejpd-i** und **svcgw-ejpd** erlauben
- Bitte definieren Sie keine Rules betreffend dem CN auf IP-Adressen ebene: Das EJPD hat viele Gateways, die in Zukunft dynamisch verwaltet werden.
- Bitte bilden Sie die Firewall Rules nicht auf Zertifikate ebene ab. Damit werden Probleme bei Zertifikatserneuerung vermieden.

Was die Kantone bereitstellen müssen?

- Eine URL mit der die GBDBS Service abgerufen werden kann.
 - Für eine leichte Integration wäre eine Verbindung über das **Internet** empfohlen.
 - Eine Verbindung über KOMBV- KTV Netz wäre auch möglich. Diese wird aber mit einer längeren Laufzeit für die Integration gebunden.
- Die komplette Certificate Chain der das EJPD vertrauen soll (In der Regel: Root – Intermediate – Serverzertifikat).
- Die WSDL Datei, wie sie in der Anwendung des Kantons implementiert ist. (Web-service Definition Language)
- Ein paar Testdaten um die Schnittstelle initial zu testen.

Vorgehen:

- Der Kanton meldet sich beim Bund, damit ein Termin für den Anschluss vereinbart werden kann.
- Von Seiten des BJ und ISC-EJPD sind wir aus Kapazitätsgründen auf eine kontinuierliche Anbindung zwischen Juli und Oktober 2023 angewiesen. Bitte melden Sie sich so schnell wie möglich für einen Termin bei uns. Wir werden Rahmen unserer Kapazitäten den Kantonen zuerst helfen, ihren Auftrag rechtzeitig zu erfüllen, die sich zuerst bei uns gemeldet haben.

Raccordement de l'interface IPD-RF pour la recherche d'immeubles à l'échelle nationale

N° de dossier :

La présente information est destinée aux techniciens des cantons responsables de l'interface IPD-RE.

Les cantons assurent l'accès aux données du grand livre ayant des effets juridiques et aux données du registre des identifiants de personnes depuis le service de recherche d'immeubles via l'interface IPD-RF. L'OFJ et les techniciens du CSI-DFJP ne seront pas proactifs en la matière.

Les préparatifs effectués par le DFJP

Nous nous connectons avec l'interface IPD-RF des cantons par le biais d'une passerelle API du CSI-DFJP (le prestataire de services informatiques du DFJP). La passerelle utilise un certificat *mutual TLS* (mTLS) pour communiquer avec le canton. Les caractéristiques sont les suivantes :

- Le nom commun (*common name* ; CN) lié au certificat a la valeur suivante :
 - environnement productif : **svcgw-ejpd**
- La chaîne complète de certificats a les valeurs suivantes :
 - **Swiss Government Root CA II (certificat racine)**
 - **Swiss Government Regular CA 01 (certificat intermédiaire)**
 - **svcgw-ejpd ou svcgw-ejpd-i (certificat de serveur)**

Au besoin, le certificat racine peut être téléchargé depuis le site de l'OFIT : [Swiss Government Root CA II \(admin.ch\)](https://www.admin.ch/gov/fr/infocentre/accueil)

Les préparatifs à effectuer par les cantons

- Les cantons doivent disposer d'une URL sous forme d'adresse HTTPS pour consulter l'interface IPD-RF en mode production.
- Le serveur du canton doit mettre à disposition la chaîne complète de certificats, comme le fait le DFJP.
- Le serveur du canton doit disposer d'un CN univoque dans son certificat et ne pas s'appuyer sur un certificat «wildcard». Par exemple :
 - un CN ayant la forme «ipd-rf.canton.ch» est admissible ;
 - un CN ayant la forme «*.canton.ch» n'est pas admissible.
- Le **Swiss Government Root CA II** doit être placé dans le *truststore*.
Le serveur du canton doit accepter le CN du certificat de la passerelle du CSI-DFJP :
 - dans l'environnement d'intégration (pre-prod), dans lequel le CN est : **svcgw-ejpd-i** et
 - dans l'environnement productif (prod), dans lequel le CN est : **svcgw-ejpd**.Il est à noter que, dans l'environnement productif, la connexion avec les deux CN (**svcgw-ejpd-i** et **svcgw-ejpd**) doit être possible.
- Les cantons ne définissent pas de règles de vérification du CN au niveau de l'adresse IP. Le DFJP dispose de nombreuses passerelles qui seront à l'avenir gérées de manière dynamique.
- Les règles du pare-feu ne doivent pas se répercuter sur les certificats afin d'éviter des problèmes lors du renouvellement de ceux-ci.

Les éléments que les cantons doivent mettre à disposition

- une URL permettant de consulter l'IPD-RF :
 - pour faciliter l'intégration, une connexion via **Internet** est recommandée ;
 - une connexion via le réseau KOMBV- KTV est également possible, mais le temps d'intégration est plus long ;
- une chaîne complète de certificats auxquels le DFJP doit pouvoir se fier (en règle générale : certificat racine – certificat intermédiaire – certificat de serveur) ;
- le fichier WSDL (Webservice Definition Language) tel qu'il est implémenté dans l'application du canton ;
- quelques données-test en vue de tester l'interface.

Procédé :

- Le canton conclut un rendez-vous avec la Confédération en vue du raccordement au service de recherche d'immeubles.
- Pour des raisons de ressources, l'OFJ et le CSI-DFJP doivent pouvoir réaliser les raccordements en continu entre juillet et octobre 2023. Nous vous saurions gré de conclure un rendez-vous avec nous dans les meilleurs délais. Nous nous chargerons des raccordements dans l'ordre d'arrivée des demandes.