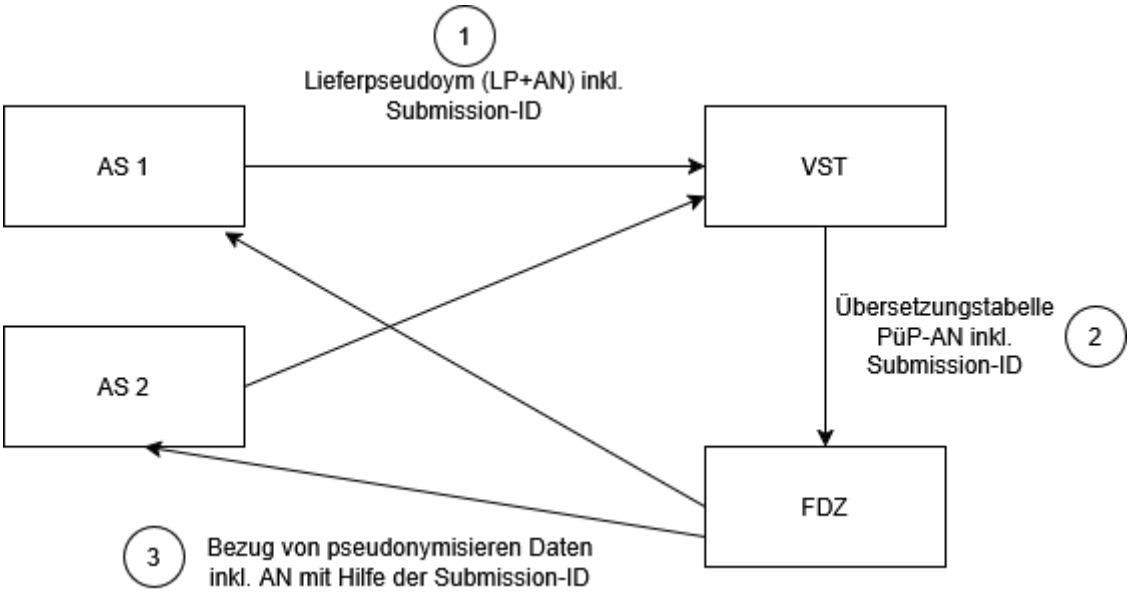
Einleitung

Das FDZ tritt in zwei Rollen auf -- einmal als Server und einmal als ePA-Client.

Wichtigste Anwendungsfälle sind:

- Annahme von Übersetzungstabelle PüP-AN (Submission mit Submission-ID) von der VST (FDZ ist Server)
- Abholen von pseudonymisierten Daten inkl. AN (Submission mit Submission-ID) vom ePA-Aktensystem
  (FDZ ist "normaler" ePA-Client)



Ein AS erzeugt zufällig eine Submission-ID und stellt eine Submission. Dabei werden vom AS Auftragsnummer (AN), Lieferpseudonyme (LP) und pseudoynmisierte Daten erzeugt.

Die Submission-ID (256-Bit-Wert) ist ein wichtiger Zuordnungsschlüsselwert (im Datenbanksinne / Zuordnungsschlüssel).

Das AS sendet eine Abbildungstabelle LP-AN inkl. Submission-ID an die VST. (Link)

Die VST sendet eine Abbildungstabelle PüP-AN inkl. Submission-ID an das FDZ. (Link)

Das FDZ bezieht als "normaler" ePA-Client vom AS die pseudonymisierten Daten (URL kommt dafür aus dem Submission-Daten, siehe weiter unten `call_back_url`). (Link)

Fachdienst/in Rolle	*Client*	*Server*

AS	Lieferung LP+AN-Submission-ID Daten an die VST	Hält pseudoynmisierte Daten inkl. AN + Submission-ID vor für das FDZ
VST	Liefert PüP+AN-Submission-ID ans FDZ	Empfänge PüP+AN-Submission-ID
FDZ	Bezieht pseudonmyisierte Daten inkl. AN + Submission-ID vom AS	Empfäng PüP+AN-Submission-ID

Übersetzungstabelle LP-AN+Submission-ID

Das AS sendet an die VST nach beidseitiger Authentisierung eine Übersetzungstabelle LP-AN+Submission-ID.

Übersetzungstabelle PüP-AN+Submission-ID

Das VST sendet an das FDZ eine Übersetzungstabelle PüP-AN+Submission-ID.

Das ist eine mit der Nomenklatur `Datenausleitung-VST-FDZ-<Submission-ID-Hex>.cbor`

Darin befindet sich folgende Datenstruktur.

```
Submission = [
   {"type": "vst->fdz",
    "created_at": Unix-Zeit,
    "submission_id": Submission-ID,
    "call_back_url": url_aktensystem},
    [PüP1, AN1], [PüP2, AN2] ...
]
```

Die Datenstruktur wird über CBOR binär kodiert.

Das FDZ erhält also bspw. `Datenausleitung-VST-FDZ-81b1b83e2736d45db16674e527890b8adc69ff7275acf11925faf44ae57f7e2f.cbor`

In der Datenstruktur selbst (CBOR-kodiert) sind die Submission-ID, PüP und AN binär kodiert (also jeweils 32 Byte Binärdaten).

Submission vom AS

Aus der `call_back_url` weiß das FDZ, welches AS es mit welcher URL kontaktieren muss. Das FDZ bezieht nach beidseitiger Authentisierung (siehe spätere Abschnitte) die Daten.

Die Daten sind "New-Line-Delimited-JSON (NDJSON)"-Dateien (mit bspw. folgenden Namen: `Datenausleitung-AS-FDZ-<Submission-ID-Hex>.ndjson`).

Vergleiche auch I_Data_Submission_Service.

Datensicherung

Wie in TLS+VAU-Protokoll beschrieben werden die Datentransporte jeweils über zwei übereinander liegende Sicherungsschichten (TLS+VAU-Protokoll) Vertraulichkeits- und Authentitätsgeschützt. Auf TLS-Ebene (HTTPS-Schnittstelle) gibt es nur eine Server-seitige Authentisierung. Auf der darüberliegen VAU-Protokoll-Ebene gibt es eine beidseitige Authentisierung (also sowohl VAU-Protokoll-Server-Authentisierung als auch VAU-Protokoll-Client-Authentisierung) -- Standardvorgehen bei ePA weil meistens ePA-Clients keine X.509-Zertifikate über die "direkte" Authentisierung bei TLS einsetzen können. Die nur Server-seitige TLS-Authentisierung bei der VST erleichtert die Umsetzung (spezielle Einsatzumgebung dort / Perimeter TLS-Gateway).

Revision #21
Created 10 April 2025 11:59:40 by Admin
Updated 10 April 2025 21:39:30 by Admin