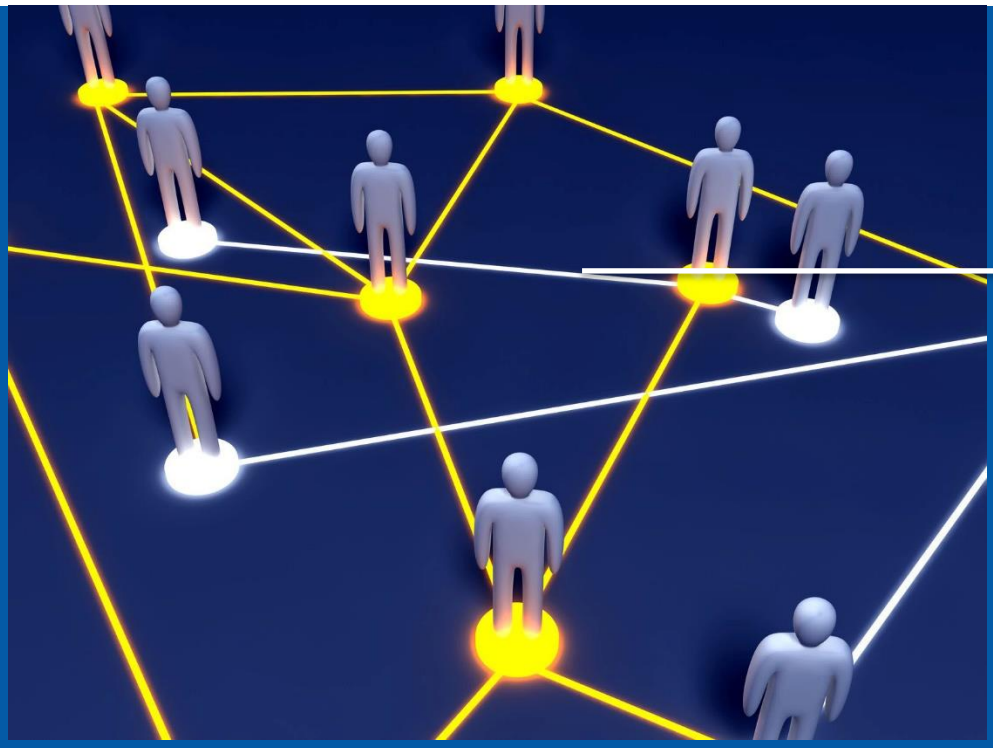
ROBERT KOCH INSTITUT



VERTRAUENSSTELLE IMPLANTATEREGISTER DEUTSCHLAND (IRD)

# Schnittstellenbeschreibung für teilnehmende Gesundheitseinrichtungen

# Änderungshistorie

| Version | Datum | Grund der Änderung, besondere Hinweise | Bearbeitung |
|---|---|---|---|
| 1.0 | 28.10.2022 | Initialversion | RKI Referat VIG (Vertrauensstelleird@rki.de) |
| 1,0a | 05.06.2023 | Anpassung der Verlinkungen auf den Download-Bereich VST IRD | RKI Referat VIG (Vertrauensstelleird@rki.de) |

# Inhalt

# Einleitung

Das Dokument beschreibt die öffentliche Schnittstelle der Vertrauensstelle des Implantateregisters Deutschland (IRD) beim Robert Koch-Institut (RKI). Diese Schnittstelle ist von den meldenden Gesundheitseinrichtungen entsprechend § 2 Abs. 5 IRegG im Rahmen der Verfahren zur Meldung an das IRD zu nutzen.

Von der Vertrauensstelle IRD werden jeweils die aktuell veröffentlichte Version der Schnittstelle sowie die beiden vorhergehenden Versionen unterstützt.

Zum erweiterten Schutz der personenidentifizierenden Daten sind diese grundsätzlich für die Übertragung zu verschlüsseln. Das betrifft sowohl den Aufruf einer Schnittstelle der Vertrauensstelle, als auch die zugehörige Antwort der Vertrauensstelle, zusätzlich zur verschlüsselten Übertragung per TLS. Dabei sind die Schlüssel der Kommunikationspartner aus der PKI der Telematikinfrastruktur (TI) der gematik zu nutzen.
Hinweis: In der aktuellen Version der API wird diese Anforderung aus Implementierungsgründen noch nicht vollständig umgesetzt, sondern ist für die folgenden Versionen der API geplant.

Für Fragen und Hinweise zur Schnittstelle ist die Vertrauensstelle IRD per E-Mail an **Vertrauensstelle-VIG@rki.de** erreichbar.

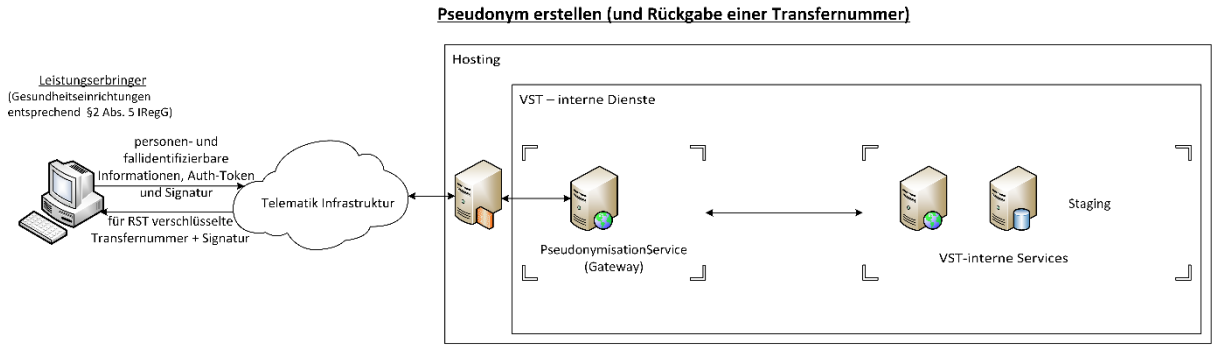
# Schnittstellen

## Pseudonym generieren (neue Meldung/ Änderungsmeldung)

Die Beschreibung der Schnittstelle im Format OpenAPI steht unter der URL
https://xml.ir-d.de/rst/download/vst/v1.0/OpenApi-PseudonymGenerierung.json
bereit.

`POST /psngen/api/v1/pseudonym/generate`
Generierung von Pseudonymen für die übergebenen Daten und Rückgabe einer Transfernummer.

Die Transfernummer muss von der Gesundheitseinrichtung als Information bei der Übermittlung der medizinischen Daten an die Registerstelle mitgesendet werden. Die Registerstelle ruft mit dieser Transfernummer die generierten Pseudonyme von der Vertrauensstelle ab.
Die Gesundheitseinrichtung kann die generierten Pseudonyme **nicht** von der Vertrauensstelle abrufen.




**Request (Beispiel)**

```
ContentType: application/json
ContentEncoding: utf-8

{
    "IdVersicherter": "L751666445",
    "IdDatensatz": "2020-1234",
    "IdKrankenversicherung": "108079808",
    "Signature": "0xffff....",
    "SubjectPublicKeyInfo": "0xababa...."
}
```

**Parameter**

Inhaltliche Pflichtangaben begründen sich aus § 17 Abs. 1 IRegG (diese ist unter der Adresse https://www.gesetze-im-internet.de/iregg/__17.html zu finden).

- IdVersicherter: Unveränderlicher Teil der Krankenversicherungsnummer bzw. ein alternativer eindeutiger Identifikator im Falle von privaten Krankenversicherungsunternehmen und sonstigen Kostenträgern. Diese Angabe ist Pflicht.
- IdDatensatz: Interne Kennung des Datensatzes des Leistungserbringers. Diese Angabe ist Pflicht.

- IdKrankenversicherung: Kennung der Krankenkasse der Patientin/ des Patienten (IK-Nummer). Diese Angabe ist Pflicht.
- Signature: Signatur des SHA256-Hash des Datenpaketes, die mit dem privaten Schlüssel des Einsenders gebildet wird (TI-PKI). Die Signatur muss als DER-Sequenz abgebildet sein. Diese Angabe ist Pflicht.
- SubjectPublicKeyInfo: Der öffentliche Teil des verwendeten Signaturschlüssels. Dieser kann entweder von einer Organisation (SMC-B) oder einer Person stammen (Heilberufeausweis, HBA). Diese Angabe ist Pflicht. Dabei sind die Schlüssel der Kommunikationspartner aus der PKI der Telematikinfrastruktur (TI) der gematik zu nutzen (TI-PKI).

**SubjectPublicKeyInfo ECDSA (Beispiel)**

```
SEQUENCE (2 elem)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.10045.2.1 ecPublicKey (ANSI X9.62 public key type)
    OBJECT IDENTIFIER 1.2.840.10045.3.1.7 prime256v1 (ANSI X9.62 named elliptic curve)
  BIT STRING (520 bit) 000001001010000001100100110010001100010000100011100000000000
01110000011…
```

**Response**

ContentType: `application/json`

ContentEncoding: `utf-8`

StatusCodes

- bei erfolgreicher Verarbeitung: `OK`, Code `200`
- bei Validierungsverletzungen: `BadRequest`, Code `400` ohne Details zu den Modellverletzungen
- bei Fehlern in der internen Verarbeitung: `InternalServerError`, Code `500`
- bei einer fehlenden oder fehlerhaften Authentifizierung: `Forbidden`, Code `403`

Content (Beispiel)

- bei erfolgreicher Verarbeitung: die für die Registerstelle IRD verschlüsselte Transfernummer und die Signatur (ECDSA, DER-Sequenz). Die Transfernummer ist mit dem öffentlichen Verschlüsselungsschlüssel der Registerstelle IRD verschlüsselt (TI-PKI). Die Signatur ist mit dem Signaturzertifikat der VST gebildet (TI-PKI).

```
{
  "Transfernummer": "0xc45782a8756236a232089ceef5faa331caa747f3cd964daf2aa5dc64...",
  "Signature": "0xffff..."
}
```

- in allen anderen Fällen der Fehlercode ohne detaillierte Information (leerer Body)

**Authentifizierung**

Zur Meldung von Implantaten berechtigte Gesundheitseinrichtungen müssen vor der Übermittlung von Nutzdaten stets authentifiziert sein. Dies erfolgt durch die Authentifizierung an der Geschäftsstelle der Registerstelle.

Die Information der korrekten Authentifizierung wird zusätzlich in Form eines sog. Bearer-Tokens als Authorization-Header mitgesendet. Das JSON Web Token wird durch eine Anmeldung an der Registerstelle zur Verfügung gestellt und wird von der Registerstelle signiert. In dem Token ist unter anderem auch als Claim der eindeutige Identifikator der angemeldeten Gesundheitseinrichtung enthalten (IrdIdGesundheitseinrichtung).

# Auskunftsverlangen

Die Beschreibung der Schnittstelle im Format OpenAPI steht unter
https://xml.ir-d.de/rst/download/vst/v1.0/OpenApi-Auskunftsverlangen.json
bereit.

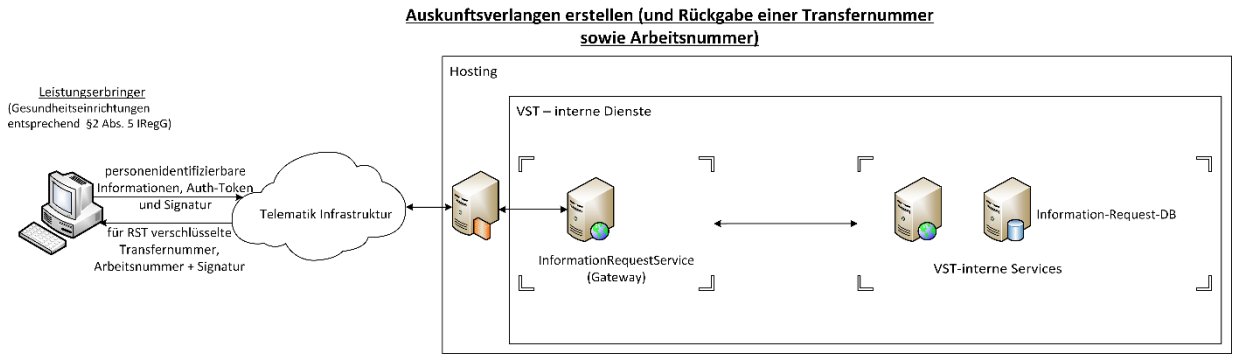
```
POST /rfigen/api/v1/informationrequest/generate
```

Gemäß IRegBV § 22 (https://www.gesetze-im-internet.de/iregbv/__22.html) kann ein Versicherter bei einer teilnehmenden Gesundheitseinrichtung ein Auskunftsverlangen initiieren. Dazu übermittelt die Gesundheitseinrichtung den unveränderlichen Teil der Krankenversicherungsnummer bzw. einen alternativen eindeutigen Identifikator im Falle privater Krankenversicherungsunternehmen und sonstiger Kostenträgern des Versicherten an die VST.

Die VST generiert eine eindeutige Arbeitsnummer (8 Zeichen, hex-codiert) für die Anfrage. Zurückgegeben wird eine Transfernummer, die für die RST verschlüsselt ist, und auch die generierte Arbeitsnummer. Mit der Transfernummer kann die RST das Patientenpseudonym von der VST abrufen.

Beide Datenpakete sind mit einer Signatur versehen (das eingehende von der anfragenden GE und das ausgehende von der VST). Die Registerstelle fragt mit der Transfernummer das Pseudonym des Versicherten an und stellt die Auskunft für den Versicherten zusammen. Es wird immer eine Auskunft direkt an den Versicherten geliefert, selbst wenn keine Daten über den Versicherten im Implantateregister Deutschland gespeichert sind.

Ein Beispiel für eine Arbeitsnummer: `d85782a8756255af`




**Request (Beispiel)**

```
ContentType: application/json
ContentEncoding: utf-8

{
   "IdVersicherter": "L751666445",
   "Signature": "0xffff....",
   "SubjectPublicKeyInfo": "0xababa...."
}
```

**Parameter**

Inhaltliche Pflichtangaben begründen sich aus § 17 Abs. 1 IRegG. Diese sind unter der Adresse

https://www.gesetze-im-internet.de/iregg/__17.html zu finden.

- IdVersicherter: Unveränderlicher Teil der Krankenversicherungsnummer bzw. ein alternativer eindeutiger Identifikator im Falle von privaten Krankenversicherungsunternehmen und sonstigen Kostenträgern. Diese Angabe ist Pflicht.
- Signature: Signatur des SHA256-Hash des Datenpaketes, die mit dem privaten Schlüssel des Einsenders gebildet wird (TI-PKI). Die Signatur muss als DER-Sequenz abgebildet sein. Diese Angabe ist Pflicht.
- SubjectPublicKeyInfo: Der öffentliche Teil des verwendeten Signaturschlüssels. Dieser kann entweder von einer Organisation (SMC-B) oder einer Person stammen (Heilberufeausweis, HBA). Diese Angabe ist Pflicht. Dabei sind die Schlüssel der Kommunikationspartner aus der PKI der Telematikinfrastruktur (TI) der gematik zu nutzen (TI-PKI).

**SubjectPublicKeyInfo ECDSA (Beispiel)**

```
SEQUENCE (2 elem)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.10045.2.1 ecPublicKey (ANSI X9.62 public key type)
    OBJECT IDENTIFIER 1.2.840.10045.3.1.7 prime256v1 (ANSI X9.62 named elliptic curve)
  BIT STRING (520 bit) 000001001010000001100100110010001100010000100011110000000000
01110000011…
```

**Response**

ContentType: `application/json`

ContentEncoding: `utf-8`

StatusCodes

- bei erfolgreicher Verarbeitung: `OK`, Code `200`
- bei Validierungsverletzungen: `BadRequest`, Code `400` ohne Details zu den Modellverletzungen
- bei Fehlern in der internen Verarbeitung: `InternalServerError`, Code `500`
- bei einer fehlenden oder fehlerhaften Authentifizierung: `Forbidden`, Code `403`

Content (Beispiel)

- bei erfolgreicher Verarbeitung: die für die Registerstelle IRD verschlüsselte Transfernummer, die generierte Arbeitsnummer und die Signatur (ECDSA, DER-Sequenz). Die Transfernummer ist mit dem öffentlichen Verschlüsselungsschlüssel der Registerstelle IRD verschlüsselt (TI-PKI). Die Signatur ist mit dem Signaturzertifikat der VST gebildet (TI-PKI).

```
{
      "Transfernummer": "0xc45782a8756236a23eef5faa331caa747f3cd964daf2aa5c6b...",
      "Workingnumber": "d85782a8756255af",
      "Signature": "0xffff..."
}
```

- in allen anderen Fällen der Fehlercode ohne detaillierte Information (leerer Body)

**Authentifizierung**

Zur Meldung von Implantaten berechtigte Gesundheitseinrichtungen müssen vor der Übermittlung von Nutzdaten stets authentifiziert sein. Dies erfolgt durch die Authentifizierung an der Geschäftsstelle der Registerstelle.

Die Information der korrekten Authentifizierung wird zusätzlich in Form eines sog. Bearer-Tokens als Authorization-Header mitgesendet. Das JSON Web Token wird durch eine Anmeldung an der Registerstelle zur Verfügung gestellt und wird von der Registerstelle signiert. In dem Token ist unter anderem auch als Claim der eindeutige Identifikator der angemeldeten Gesundheitseinrichtung enthalten (IrdIdGesundheitseinrichtung).

**Allgemeine Hinweise**

Die gezeigten Beispiele sind für Lesbarkeit gedacht, Bytefolgen sind hexadezimal dargestellt (0xabcdef…). In der Implementierung werden diese Angaben als Roh-Bytes erwartet, die Übermittlung erfolgt automatisch als Base64.

Ein Beispiel für die Signierung der Meldedaten ist unter dem Dokument „PoC-Signierung.pdf“ zu finden. Das Dokument kann hier https://xml.ir-d.de/rst/download/vst/v1.0/PoC-Signierung.pdf heruntergeladen werden.

# Kontakt

Robert Koch-Institut
Nordufer 20
13353 Berlin

E-Mail: Vertrauensstelle-VIG@rki.de