P20 POLIZEI 20/20

P20 UID Generator Service

Identity Governance Service

Version 1.0.0

P20 GEMEINSAM. DIGITAL. VERNETZT.

P20 UID Generator Service

Veröffentlicht 17.06.2023

von Sophie Strecke, Dieter Steding und Sylvert Bernet

Programm	Polizei 20/20
Programmleiter	Holger Gadorosi
Projektleiter/Verantwortlicher	Norbert Linde
Dokumententitel	P20 UID Generator Service
Version	1.0
Erstellt am **Erstellt von**	08.06.2022 Dieter Steding
Zuletzt bearbeitet am **Zuletzt bearbeitet von**	29.08.2022 Dieter Steding

Versionshistorie

Version	Datum	Autor	Verweis
1.0	29.08.2022		Kein vorheriges Dokument

Inhaltsverzeichnis

Vorwort 1
Zweck dieses Dokuments 1
Notationskonventionen 1
Typografische Konventionen 1
Symbol Konventionen 1
Einleitung 3
Referenzarchitekture 4
Architekturkomponenten 4
Authentifizierung für die REST-API 5
Autorisieren einer Anfrage 6
Bezug eines Access-Token 6
Anfrageparameter 6
Antwortparameter 7
Übersicht über die Ressourcen 9
HTTP Verben 9
REST Ressourcen 9
REST Endpunkte 10
Anhang 12
Glossar 12
Zulässige Werte je P20-UID-Segment 14
1.Segement (Kategorie Partner Type / Teilnehmer Type 14
2.Segment (Staatenzuordnung) 14
3.Segment (Bund / Land / International) 14
4.Segment (Partner- bzw. TeilnehmerID) 15
5.Segment Identitätstyp 16

Vorwort

Zweck dieses Dokuments

Dieses Dokument beschreibt die Nutzung der durch den UID-Generator bereitgestellten Serviceschnittstellen und richtet sich an Administratoren von Ressourcen und Teams für die Integration von Zielsysteme.

Notationskonventionen

Die Schlüsselwörter *MUSS*, *DARF NICHT*, *ERFORDERLICH*, *SOLL*, **SOLL NICHT**, **SOLL**, **SOLLTE NICHT**, *EMPFOHLEN*, *KANN* und *OPTIONAL* in diesem Dokument sind wie in beschrieben zu interpretieren *[RFC2119]* Diese Schlüsselwörter werden groß geschrieben, wenn sie verwendet werden, um Anforderungen an das Protokoll oder Anwendungsfunktionen und -verhalten, die sich auf die Interoperabilität und Sicherheit von Implementierungen auswirken, eindeutig anzugeben. Wenn diese Wörter nicht großgeschrieben werden, sind sie in ihrem natürlichen Sprachsinn gemeint.

Typografische Konventionen

In diesem Dokument werden die folgenden typografische Konventionen verwendet.

Konvention	Bedeutung
fett	Fettschrift kennzeichnet Elemente der grafischen Benutzeroberfläche, die einer Aktion zugeordnet sind, oder Begriffe, die im Text oder im Glossar definiert sind.
kursiv	Kursivschrift kennzeichnet Buchtitel, Hervorhebungen oder Platzhaltervariablen, für die Sie bestimmte Werte angeben.
`monospace`	Monospace-Schrift kennzeichnet Befehle innerhalb eines Absatzes, URLs, Code in Beispielen, Text, der auf dem Bildschirm angezeigt wird, oder Text, den Sie eingeben.

Symbol Konventionen

In diesem Dokument werden die folgenden Konventionen für Symbole verwendet.

Symbol	Bedeutung
[ ]	Enthält optionale Argumente und Befehlsoptionen.
{ | }	Enthält eine Reihe von Auswahlm öglichkeiten für eine erforderliche Befehlsoption.
${ }	Referenziert eine Variable.
-	Verbindet gleichzeitig mehrere Tastenanschläge.
+	Verbindet mehrere aufeinanderfolgende Tastenanschläge.

Symbol	Bedeutung
>	Zeigt die Auswahl eines Menüpunkts in der grafischen Benutzeroberfläche an.

Einleitung

Für den Zugriff auf die vom Programm Polizei 20/20 zur Verfügung gestellten Ressourcen (Anwendungen, Daten) wird die Anreicherung der dafür vorgesehenen bestehenden Benutzerkonto mit einer zusätzlichen P20/20-ID (im Folgenden P20-UID) nach einheitlicher Logik vorgenommen.

Dieser "*Unique Identifier*" (die P20-UID) ist im Informationsmodell Polizei (IMP) abgebildet. Sie ist bei der Kommunikation zwischen den Ländern, der PSP, dem Datenhaus über die P20/20-Schnittstellen zu übertragen. Die P20-UID macht den Verantwortlichen einer Abfrage oder einer Datenänderung dienstübergreifend zweifelsfrei kenntlich. Die P20-UID enthält keine personenbeziehbare Daten. Eine Zuordnung zur Person kann nur unter Beteiligung des Teilnehmers erfolgen.

Die P20-UID dient der Identifizierung sowie der fachlichen / datenschutzrechtlichen Protokollierung. Aus ihr sollen unter anderem das Herkunftsland, der (INPOL)-Teilnehmer oder Partner-Institutionen, die auf P20/20-Dienste zugreifen, direkt ableitbar sein.

Dies Dokument beschreibt die zentral bereitgestellte Verwaltungsfunktionen des Generators und seine offengelegten Schnittstellen.

Referenzarchitekture

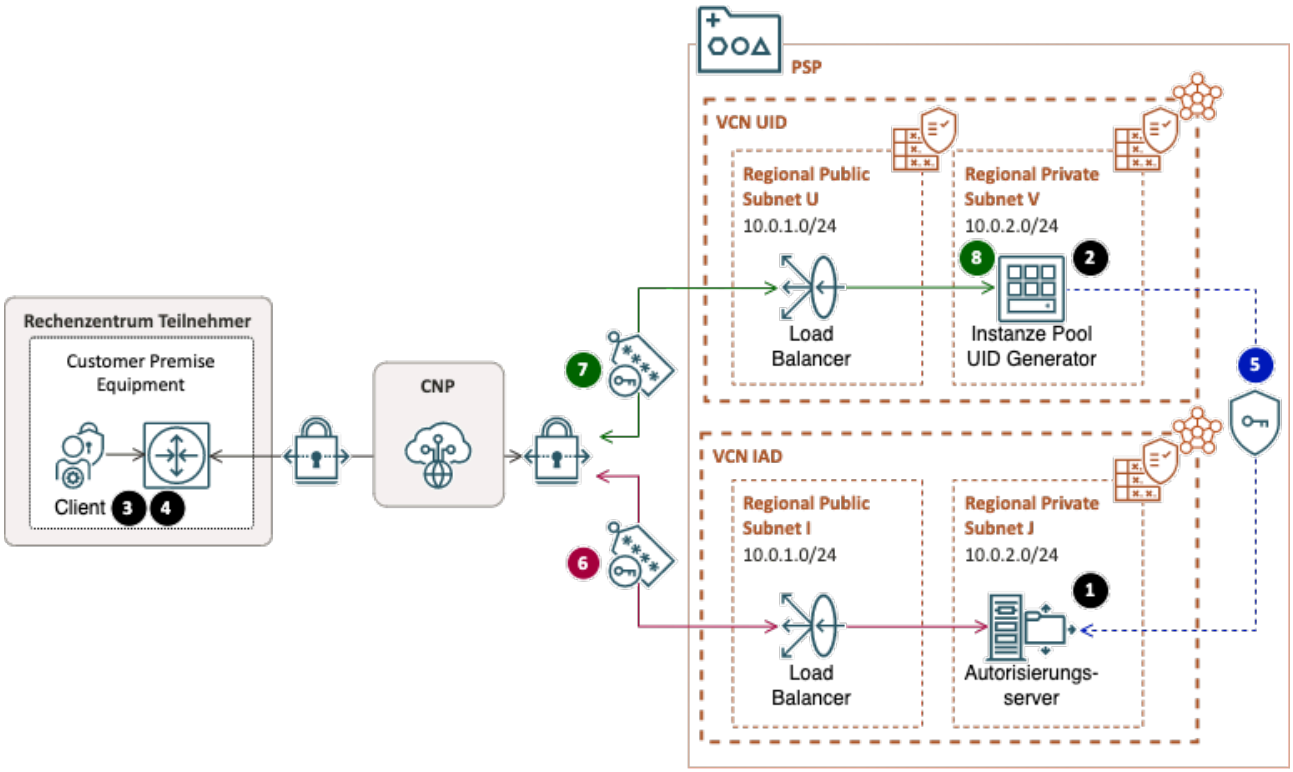
Die Referenzarchitektur veranschaulicht die auf der PSP für den UID-Generator bereitgestellten Architekturkomponenten.

Innerhalb der PSP VCN's gibt es zwei Arten von Subnetzen:

- public (Öffentliches Subnet)
- private (privates Subnet und Daten-Subnet)

In den öffentlichen Subnetzen bereitgestellte Ressourcen erhalten eine öffentliche IP-Adresse und sind im CNP öffentlich sichtbar. Die Load Balancer, die den Serviceinstanzen vorgelagert sind, werden hier bereitgestellt.

In den privaten Subnetzen bereitgestellte Ressourcen erhalten nur eine private IP-Adresse und sind daher im CNP nicht öffentlich sichtbar, was die Sicherheit dieser Ressourcen verbessert. Die Serviceinstanzen werden in privaten Subnetzen bereitgestellt.



Architekturkomponenten

#	Komponente	Beschreibung
1	Autorisierungsserver	Dies ist der Server, der die Schnittstelle bereitstellt, über die der Benutzer die Anfrage zur Authentifizierung genehmigt oder ablehnt. In kleineren Implementierungen kann dies derselbe Server wie der API-Server sein, bei größeren Bereitstellungen wird dieser jedoch häufig als separate Komponente erstellt.

#	Komponente	Beschreibung
2	Resource Server	Der Ressourcen-Server ist der API-Server, der für den Zugriff auf die durch die Ressourcen bereitgestellten Informationen verwendet wird.
3	Client	Der Client ist die Anwendung, die versucht, Zugriff auf das Konto des Benutzers zu erhalten. Bevor sie dies tun kann, muss sie die Zustimmung des Benutzers einholen. Ein *"Vertraulicher Client"* ist eine Anwendung, die vom Autorisierungsserver Anmeldeinformationen erhält und diese wiederum verwendet, um sich selbst beim Autorisierungsserver zu authentifizieren, wenn sie beispielsweise Zugriffstoken anfordert. Die Anmeldeinformationen können ein einfaches Kennwort oder eine sicherere Option wie ein privater Schlüssel sein, der zum Signieren eines JWT verwendet wird, sein. Der Vorteil der Verwendung einer Client-Authentifizierung jeglicher Art besteht darin, dass der Autorisierungsserver weiß, dass alle mit diesen Anmeldeinformationen gestellten Anforderungen von einem legitimierten Client stammen und ein Identitätswechsel des Client somit nicht möglich ist.
4	Resource Owner	Der Ressourcen-Eigentümer ist die Person, die Zugriff auf einen Teil ihres Benutzerkontos gewährt.
5	Trust	Über einen Austausch von Schlüsseln wird eine Vertrauensstellung des Ressourcen-Server zum Autorisierungsserver konfiguriert.

Authentifizierung für die REST-API

6 Alle Anfragen an Ressourcen in der REST-API *MÜSSEN* im Namen eines Ressourcen-Eigentümer erfolgen. Bevor eine Anfrage verarbeitet wird, authentisiert die API die Anfrage, um den Ressourcen-Eigentümer zu ermitteln. Die API verwendet zu diesem Zweck das OAuth 2.0-Protokoll und der Prozess basiert auf Access-Token, wie unten beschrieben.

7 Alle REST-API-Aufrufe **MÜSSEN** autorisiert sein. Anstatt bei jedem REST-API-Aufruf die vollständigen Anmeldeinformationen zu übergeben, verwendet REST einen Access-Token. Der Access-Token ist für einen konfigurierbaren Zeitraum gültig und fungiert wie ein temporäres Passwort.

Nach erfolgreicher Autorisierung entscheidet eine Berechtigungsprüfung darüber, ob der Ressourcen-Eigentümer die angeforderte Aktion ausführen darf. Diese Prüfung verwendet die vorhandenen Berechtigungen, die dem Ressourceneigentümer gewährt wurden.

Autorisieren einer Anfrage

Jede Anfrage **MUSS** autorisiert werden, indem im Anfrage Header `Authorization` einen Access-Token übergeben wird. Ersetzen Sie im folgenden Beispiel *<your-token>* durch einen Verweis auf Ihren Access-Token:

Beispiel

```
curl --request GET \
     --url "https://<service-host>:<service-port>/igs/uid/v1" \
     --header "Authorization: Bearer <your-token>"
```

> **Hinweis**
>
> In den meisten Fällen können `Authorization: Bearer` oder `Authorization: token` verwendet werden, um ein Access-Token zu übergeben. Wennjedoch ein JSON-Web-Token (JWT) übergeben wird, **MUSS** `Authorization: Bearer` als Header verwendet werden.

Wenn versucht wird, eine Ressource ohne oder mit einem Access-Token zu verwenden, das nicht über ausreichende Berechtigungen verfügt, erhalten Sie die Antwort `401 Unauthorized` oder `403 Forbidden`.

Bezug eines Access-Token

Der Prozess basiert auf dem Ablauf *Resource Owner Password Credentials*.

Der Ablauf *Resource Owner Password Credentials* erfordert, dass ein Client die Anmeldeinformationen des Ressourcen-Eigentümer kennt. Um den Benutzernamen und das Passwort gegen ein Access-Token auszutauschen, senden Sie eine HTTPS-POST-Anfrage mit den entsprechenden Parametern an den Basis-URI des Access-Token-Endpunkts des Autorisierungsserver. Die http-Verbindungen werden dabei nicht akzeptiert; verwenden Sie stattdessen https.

Der implementierte Ablauf basiert auf einem *"Vertraulichen Client"* und erfordert daher eine `client_id` **UND** ein `client_secret`. Auch wenn die `client_id` öffentlich ist, wird empfohlen, sie derartig zu gegerieren, dass sie von Dritten nicht erraten werden kann. Daher verwenden viele Implementierungen so etwas wie eine 32-stellige Hex-Zeichenfolge. Das `client_secret` ist das nur der Client-Anwendung bekannte Kennwort. Es sollte ausreichend zufällig sein, um nicht erraten zu werden. Daher sollte nicht auf gängige UUID-Bibliotheken zurückgegriffen werden, da diese häufig den Zeitstempel oder die MAC-Adresse des Servers berücksichtigen, der für die Generierung verwendet wird.

Anfrageparameter

Parameter	Erforderlic	Beschreibung
client_id	ja	Die öffentliche Kennung eines Client, die zum Zeitpunkt der Client-Registrierung erhalten wurde.

Parameter	Erforderlic	Beschreibung
client_secret	ja	Ein Geheimnis, das nur dem Client und dem Autorisierungsserver bekannt ist.
grant_type	ja	Geben Sie `password` als Wert für diesen Parameter an.
username	ja	Der Anmeldename des zu verwendenden Benutzerkontos.
password	ja	Das Kennwort für das zu verwendende Benutzerkonto.

Antwortparameter

Parameter	Beschreibung
access_token	Der OAuth 2.0 Access-Token.
token_type	Der Typ des zurückgegebenen Access-Tokens. Zu diesem Zeitpunkt ist dies immer `Bearer`.
expires_in	Die verbleibende Lebensdauer eines Access-Token.
refresh_token	Der Refresh-Token wird zurückgegeben, wenn eine Clientanwendung dafür registriert ist. Mit diesem Token kann der Access-Token erneuert werden, wenn er abgelaufen ist.

Hinweis

Wenn Fehler bei der Überprüfung auftreten, wird HTTP-Status 400 mit der JSON-Antwort zurückgegeben, die die Elemente `error` und `error_description` enthält.

Beispiel Anfrage

Im Folgenden finden Sie ein Beispiel einer Anfrage zur Austellung eines Access-Tokens. Für eine bessere Lesbarkeit wurden Leerzeichen beibehalten.

```
curl --location 'https://<authorization-host>:<authorization-port>/oauth2/rest/token' \
     --header 'Accept: application/json' \
     --header 'x-oauth-identity-domain-name: SecureDomain2' \
     --header 'Content-Type: application/x-www-form-urlencoded' \
     --header 'Authorization: Basic YmI3NzViMTItYmJkNC00MjNiLTgzZD...' \
     --data-urlencode 'grant_type=password' \
     --data-urlencode 'username=user1' \
     --data-urlencode 'pass@123'
```

Identity Domain

Aus Sicherheitsgründen ist der Autorisierungsserver in Identitätsdomänen segmentiert.

Der Header `x-oauth-identity-domain-name` ist erforderlich, wenn der Client nicht in der Standarddomäne registriert ist.

Beispiel Antwort

Eine vom Autorisierungsserver erhaltene Antwort sieht folgendermaßen aus:

```
{ "access_token": "eyJraWQiOiJTZWN1cmVEb21haW4yIiwieDV0IjoiSjFsVmdQ..."
, "token_type": "Bearer"
, "expires_in": 7200
, "refresh_token": "LnE8w3KlOu5SN%2B0LEfVicg%3D%3D%7EUGKP%2BRWrPO..."
}
```

Übersicht über die Ressourcen

Dieses Kapitel hilft Ihnen, sich mit den UID-Generator-REST-Endpunkten vertraut zu machen. Dadurch können Sie die benötigten Informationen schnell finden und die erforderlichen Aufgaben problemlos erledigen.

Die UID-Generator-REST-Ressourcen bieten Funktionen für die Mehrheit der Verwaltungsaufgaben. Der Zugriff auf die UID-Generator-REST-Ressourcen erfolgt durch direkte Anmeldung bei der Anwendung (See Authentifizierung für die REST-API).

Was das REST-API-Design betrifft:

- HTTP hat Verben (Aktionen oder Methoden): GET, POST, PUT, PATCH und DELETE sind am häufigsten anzutreffen.
- REST ist **ressourcenorientiert** und eine Ressource wird durch einen **URI** dargestellt.
- Ein **Endpunkt** ist die Kombination aus einem Verb und einem URI.

HTTP Verben

Nachfolgend sind die Verben, die eine kompatible REST-Implementierung (wie UID Generator) spricht, zusammengefasst:

HTTP Verb	Beschreibung
GET	Ruft eine oder mehrere Ressourcen ab (z. B. UIDs/Teilnehmer).
POST	Erstellt neue Ressourcen, führt SuchvorgÜnge aus.
PUT	Ändert Ressourcen durch Hinzufügen und Ersetzen von Attributen
DELETE	Löscht eine Ressource.

REST Ressourcen

Die folgende Tabelle fasst die verfügbaren Ressourcen des UID-Generator zusammen:

Ressource	Beschreibung
Eindeutige Kennungen	Die Ressource für eindeutige Kennungen umfasst das Generieren, Registrieren und Löschen eindeutiger Kennungen.
Teilnehmer oder Partner	Die Ressource zur Typverwaltung von Teilnehmer oder Partnern umfasst das Suchen, Erstellen, Aktualisieren und Löschen von Teilnehmertypen.
Staatenzuordnung	Die Ressource zum Verwalten von Staatenzuordnungen im UID-Generator umfasst das Suchen, Erstellen, Aktualisieren und Löschen von Staatenzuordnungen.

Ressource	Beschreibung
Länderzuordnung	Die Ressource zum Verwalten von Länderzuordnungen im UID-Generator umfasst das Suchen, Erstellen, Aktualisieren und Löschen von Länderzuordnungen.
Teilnehmer-/ Partner-ID	Die Ressource zum Verwalten von Teilnehmer-/Partner-ID's im UID-Generator umfasst das Suchen, Erstellen, Aktualisieren und Löschen von Teilnehmer-/ Partner-ID's.
Accounttyp	Die Ressource zum Verwalten von Accounttypen im UID-Generator umfasst das Suchen, Erstellen, Aktualisieren und Löschen von Accounttypen.

REST Endpunkte

Die folgende Tabelle fasst die verfügbaren Endpunkte in der UID-Generator-Implementierung des REST-Dienstes zusammen:

Endpunkt	Ressource	HTTP Verben	Beschreibung
/uid	Eindeutige Kennungen	GET, POST, PUT, DELETE	Eindeutige Kennungen abrufen, generieren, registrieren und löschen.
/participantTyp	Teilnehmertypen	GET, POST, PUT, DELETE	Teilnehmertypen abrufen, hinzufügen, ändern und löschen.
/country	Staatenzuordnung	GET, POST, PUT, DELETE	Staatenzuordnungen abrufen, hinzufügen, ändern und löschen.
/state	Bundeslandzuordnung	GET, POST, PUT, DELETE	Staatenzuordnungen abrufen, hinzufügen, ändern und löschen.
/participant	Teilnehmer	GET, POST, PUT, DELETE	Teilnehmer abrufen, hinzufügen, ändern und löschen
/type	Accounttyp	GET, POST, PUT, DELETE	Identitätstypen abrufen, hinzufügen, ändern und löschen

Hinweis

Den tatsächlichen Endpunkt-URLs wird entsprechend die Stamm-URL der REST-API vorangestellt. Beispielsweise sollte die Endpunkt-URL der Staatenzuordnung, die Sie in Ihren Anwendungen verwenden möchten, wie folgt sein:

```
https://<service-host>:<service-port>/igs/uid/v1/country
```

Wichtig

Alle Nutzlasten, die per POST oder PUT an Endpunkte gesendeten werden, sollten mit `Content Type: application/json` und unter Verwendung der UTF-8-Kodierung bereitgestellt werden. Ebenso wird die Ausgabe vom Server in UTF-8 gesendet.

Anhang

Glossar

Begriff / Abkürzung	Beschreibung
API	Application Programming Interface Ein Dienst stellt solche Schnittstellen bereit, damit andere die durch den Dienst ermöglichten Features und Funktionen nutzen können. API's beschreiben, wie ein Verbraucher Anfragen an den Dienst stellt und was er im Gegenzug erhält.
Authentifizierung	Prüfung und Bestätigung einer Identität Überprüfen einer Identität durch Überprüfung eines Identitätsnachweises, den die Identität zu erbringen hat (z.B. Überprüfung des Personalausweises durch Gesichtskontrolle und Überprüfung der Ausweisnummer).
Authentisierung	Behauptung einer Identität Nachweisen einer Identität durch die Identität selbst (z.B. Vorlegen eines Personalausweises durch den Inhaber)
Autorisierung	Gewähren des Zugang Einräumen von Rechten anhand einer bereits festgestellten (authentifizierten) Identität und Rolle (z.B. jeder authentifizierte EU-Bürger ist autorisiert, in die Schweiz einzureisen).
Benutzerkonto	Ein Benutzerkonto (engl. Account), kurz Nutzerkonto, ist eine Zugangsberechtigung zu einem zugangsbeschränkten IT-System. Die Struktur eines Benutzerkontos variiert je IT-System. Mittels eines Benutzerkontos können natürliche Identitäten als auch technische Accounts (andere IT-Systeme) auf ein IT-System zugreifen.
CNP	
Encoding	Eine Zeichenkodierung erlaubt die eindeutige Zuordnung von Schriftzeichen (i. A. Buchstaben oder Ziffern) und Symbolen innerhalb eines Zeichensatzes.
Identität	Als Identität wird eine in einem bestimmten Verwendungskontext eindeutige, wiedererkennbare Beschreibung einer natürlichen Person bezeichnet. Die Identität besteht aus Attributen, die die Person eindeutig charakterisieren.
Identity Provider	Ein Identitätsanbieter (IdP) ist ein System, das digitale Identitäten erstellt, speichert und verwaltet. Der IdP kann den Benutzer entweder direkt

Begriff / Abkürzung	Beschreibung
	authentifizieren oder Authentifizierungsdienste für Drittanbieter (Apps, Websites oder andere digitale Dienste) bereitstellen.
IdP	Siehe Identity Provider
IMP	Informationsmodell der Polizei Das Informationsmodell Polizei ist definiert als ein konzeptionelles Datenmodell, das geeignet ist, Bund- Länder-übergreifende Datenaustausch- und Geschäftsprozesse zu unterstützen. Es enthält die hierfür notwendigen Informationsobjekte (Entitäten), deren Detailinformationen (Attribute) sowie strukturell und inhaltlich abgestimmte Kataloge (Abstimmung in einem fortlaufenden parallelen Prozess).
JSON	JavaScript Object Notation Ein leichtgewichtiges Format zum Datenaustausch.
P20-UID	User Identity (Eindeutiger Idenitifizierer einer Identität im P200-Umfeld)
Partner	Als Partner werden im Rahmen dieses Dokumentes die BehÖrden betrachtet, die zukünftig im Rahmen ihrer hoheitlichen Aufgaben und/ oder einer polizeilichen Zusammenarbeit auf Dienste des Programmes Polizei 20/20 zugreifen, aber nicht zu den eigentlichen Teilnehmern von Polizei 20/20 gehÖren.
PSP	Polizei-Service-Platform Umfassende Infrastruktur, die die Basis für die Bereitstellung von Anwendungen sowie fachlichen und technischen Services darstellt. Die PSP ist ein logischer Blick auf die Bereitstellung von Infrastrukturen und Plattformen durch verschiedene Dienstleister (BKA-IT, Länder-DL oder auch private DL).
REST	Representational State Transfer
Teilnehmer	Als Teilnehmer werden die Polizeien bezeichnet, die direkt am Programm Polizei 20/20 teilnehmen, d.h. alle Polizeien der Länder und des Bundes (BKA, Bundespolizei, Bundestagspolizei sowie der Zoll) gemäß BKAG §29.
URI	Uniform Resource Identifier Ein Uniform Resource Identifier (URI) ist ein Identifikator und besteht aus einer Zeichenfolge, die zur Identifizierung einer abstrakten oder physischen Ressource dient. URIs können verwendet werden, um alles zu identifizieren, einschließlich realer Objekte wie Personen und Orte, Konzepte oder Informationsressourcen wie Webseiten und Bücher.

Begriff / Abkürzung	Beschreibung
VCN	Virtual Cloud Network

Zulässige Werte je P20-UID-Segment

1.Segement (Kategorie Partner Type / Teilnehmer Type

Wert	Beschreibung
P	Partner
T	Teilnehmer

2.Segment (Staatenzuordnung)

Wert	Beschreibung
36	Deutschland

3.Segment (Bund / Land / International)

Wert	Beschreibung
0	Bund
1	Schleswig-Holstein
2	Hamburg
3	Niedersachsen
4	Bremen
5	Nordrhein-Westfalen
6	Hessen
7	Rheinland-Pfalz
8	Baden-Württemberg
9	Bayern
10	Saarland
11	Berlin
12	Brandenburg

Wert	Beschreibung
13	Mecklenburg-Vorpommern
14	Sachsen
15	Sachsen-Anhalt
16	Thüringen

4.Segment (Partner- bzw. TeilnehmerID)

Wert	Beschreibung
01	Polizei Schleswig-Holstein
02	Polizei Hamburg
03	Polizei Niedersachsen
04	Polizei Bremen
05	Polizei Nordrhein-Westfalen
06	Polizei Hessen
07	Polizei Rheinland-Pfalz
08	Polizei Baden-Württemberg
09	Polizei Bayern
10	Polizei Saarland
11	Polizei Berlin
12	Polizei Brandenburg
13	Polizei Mecklenburg-Vorpommern
14	Polizei Sachsen
15	Polizei Sachsen-Anhalt
16	Polizei Thüringen
20	Bundeskriminalamt
30	Bundespolizei

Wert	Beschreibung
31	Zollkriminalamt
36	Polizei beim Deutschen Bundestag

5.Segment Identitätstyp

Wert	Beschreibung
101	Anwenderkonto - Mitarbeiter
111	Administrationskonto f?r Fachanwendungen