

Basisdienst personenbezogenen ID im Programm Polizei 20/20

P20-P20-UID

Version 0.1| Stand 24.05.2022

V

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Dokumenteninformation** | | | | | | | | | | |
| **Programm** | | | Polizei 20/20 | | | | | | | |
| **Programmleiter** | | | Holger Gadorosi | | | | | | | |
| **Projektleiter/Verantwortlicher** | | | <Norbert Linde> | | | | | | | |
| **Dokumententitel** | | | Basisdienst personenbezogenen ID im Programm Polizei 20/20 | | | | | | | |
| **Version** | | | 0.1 | | | | | | | |
| **Erstellt am**  **Erstellt von** | | | <24.05.2022>  <PG IAM> | | | | | | | |
| **Zuletzt bearbeitet am**  **Zuletzt bearbeitet von** | | | <24.05.2022>  PG IAM | | | | | | | |
| **Status** | | | In Bearbeitung  <**X**> | | Vorgelegt  <> | | | Freigegeben  <> | | Verworfen  <> |
| **Vorprüfung des Dokumentes** | | | | | | | | | | |
| **Fachliche Prüfung** (Fachlichkeit) | | | | | | | Vorgelegt <> | | Freigegeben <> | |
| **Technische Prüfung** (Technik) | | | | | | | Vorgelegt <> | | Freigegeben <> | |
| **Methodische Prüfung** (Projektkoordination) | | | | | | | Vorgelegt <> | | Freigegeben <> | |
| <Bitte tragen Sie hier weitere mitzeichnungspflichtige Prüfinstanzen je nach Thematik und festgelegtem Erstellungsprozess ein, z.B. AG Recht, AG Vergabe.> | | | | | | | Vorgelegt <> | | Freigegeben <> | |
| **Freigabe Hauptversion 1.0 durch Freigabeverantwortlichen bzw. zuständiges Gremium** | | | | | | | | | | |
| **Freigegeben am** (TT.MM.JJJJ): | | | | | | | | | | |
| **Freigegeben von** (Nachname, Vorname, OE): | | | | | | | | | | |
| **Unterschrift** (Unterschrift in gescannter Kopie): | | | | | | | | | | |
| **Versionshistorie** | | | | | | | | | | |
| **Version** | **Datum** | **Erstellt durch** | | **Inhaltliche Kurzbeschreibung der Neuerungen** | | | | | | |
| 0.1 | 24.05.2025 | Sophie Strecke, Dieter Steding | | Ersterstellung des Dokumentes | | | | | | |
|  |  |  | |  | | | | | | |
|  |  |  | |  | | | | | | |
|  |  |  | |  | | | | | | |
|  |  |  | |  | | | | | | |
|  |  |  | |  | | | | | | |
|  |  |  | |  | | | | | | |
|  |  |  | |  | | | | | | |
|  |  |  | |  | | | | | | |
|  |  |  | |  | | | | | | |
| **Referenzierte Dokumente** | | | | | | | | | | |
| **Referenzdokument** | | | | **Version** | | **Autor** | | | | **Datum** |
| <A> | | | | <Link> | | <Vorname Nachname, Organisationseinheit> | | | | <TT.MM.JJJJ> |

Inhaltsverzeichnis

[Abkürzungsverzeichnis 5](#__RefHeading___Toc15734_2043478891)

[Abbildungsverzeichnis 6](#__RefHeading___Toc15736_2043478891)

[Tabellenverzeichnis 6](#__RefHeading___Toc15738_2043478891)

[1. Einleitung 7](#__RefHeading___Toc15740_2043478891)

[2. Begrifflichkeiten 8](#__RefHeading___Toc15742_2043478891)

[3. Aufbau, Generierung und Registrierung der P20-UID 9](#__RefHeading___Toc15744_2043478891)

[3.1. Aufbau der P20-UID 9](#__RefHeading___Toc15746_2043478891)

[3.2. Generierung und Registrierung der P20-UID 11](#__RefHeading___Toc15748_2043478891)

[3.2.1. TN-seitige Beantragung zur Generierung / Registrierung einer P20-UID 12](#__RefHeading___Toc15750_2043478891)

[3.2.2. TN-seitige Generierung der P20-UID und zentrale Registrierung 12](#__RefHeading___Toc15752_2043478891)

[4. Gesamtsystemarchitektur 15](#__RefHeading___Toc15754_2043478891)

[4.1. Anforderungen an die Teilnehmer 15](#__RefHeading___Toc15756_2043478891)

[5. Anhang 15](#__RefHeading___Toc15758_2043478891)

[5.1. Glossar 15](#__RefHeading___Toc15760_2043478891)

[5.2. Zulässige Werte je P20-UID-Segment 16](#__RefHeading___Toc15762_2043478891)

Abkürzungsverzeichnis

|  |  |
| --- | --- |
| BKA | Bundeskriminalamt |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Abbildungsverzeichnis

[Abbildung 1 TN-seitige Beantragung zur Generierung und Registrierung einer P20-P20-UID 12](#Abbildung!1|sequence)

[Abbildung 2 TN-seitige Generierung und zentrale Registrierung einer P20-P20-UID 13](#Abbildung!2|sequence)

Tabellenverzeichnis

[*Tabelle 1 – Detaillierter Aufbau der P20-UID* 10](#Tabelle!2|sequence)

[Tabelle 2 – Beispiele P20-UIDsgemäß der P20-UID Systematik 11](#Tabelle!3|sequence)

[Tabelle 3 – Glossar 15](#Tabelle!5|sequence)

[Tabelle 4 Segment 1 „Kategorie Partner“ / Teilnehmer – derzeit zulässige Werte 16](#Tabelle!6|sequence)

[Tabelle 5 Segment 2 „Staat“– derzeit zulässige Werte 16](#Tabelle!7|sequence)

[Tabelle 6 Segment 3 „Bund/Land/International“– derzeit zulässige Werte 17](#Tabelle!8|sequence)

[Tabelle 7 Segment 4 „Partner- bzw. TeilnehmerID“– derzeit zulässige Werte 18](#Tabelle!9|sequence)

# Einleitung

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

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.

Das vorliegende beschreibt den zentral bereitgestellten Dienst des Generators und seine exponierten Schnittstellen.

# Begrifflichkeiten

* **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.
* **Partner:** Als Partner werden innerhalb dieses Dokumentes die Behörden betrachtet, die eventuell zukünftig im Rahmen ihrer hoheitlichen Aufgaben und/oder einer polizeilichen Zusammenarbeit auf Dienste des Programmes 20/20 zugreifen, aber nicht zu den eigentlichen Teilnehmern von Polizei 20/20 gehören.
* **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.

* **Benutzerkonto: Ein Benutzerkonto, kurz Nutzerkonto oder Account, ist eine Zugangsberechtigung zu einem zugangsbeschränkten IT-System.**

**Daher** wäre es ebenfalls möglich, einem technischen Gerät (z.B. Kennzeichenlesegerät, IoT-Device) ein Benutzerkonto zuzuteilen.

# Aufbau, Generierung und Registrierung der P20-UID

Dieses Kapitel beschreibt den Aufbau sowie die Ausgestaltung zur Generierung der P20-UID.

## Aufbau der P20-UID

Die P20-UID umfasst ingesamt sechs Segmente. Die ersten vier Segmente kennzeichnen den Teilnehmer / Partner, die letzten beiden die jeweilige Identität beim Teilnehmer / Partner. Die Segmente werden über Feldtrenner (-) voneinander abgekoppelt.

* Kategorisierung TN oder Partner
* Informationen zur Staatenzuordnung, des zu der Identität gehörenden Partners oder Teilnehmers
* Informationen zur Bundeslandzuordung des Teilnehmers (Bund oder Internationale Behörden werden aufgeführt)
* Die Partner- bzw. Teilnehmer-ID (2-11 Zeichen)
* Informationen zum Identitätstyp (z.B. Interner Sachbearbeiter, Externer Sachbearbeiter, Administrative Identität),
* sowie einen 5-11-stelligen-Bereich zur freien Vergabe beim Teilnehmer, der die eindeutige Zuordnung der ID zum Benutzerkonto und damit zur Identität beim Teilnehmer sicherstellt.

Exemplarischen P20-UID-Abbildungen sind in Tabelle 2 – Beispiele P20-UIDs enthalten.

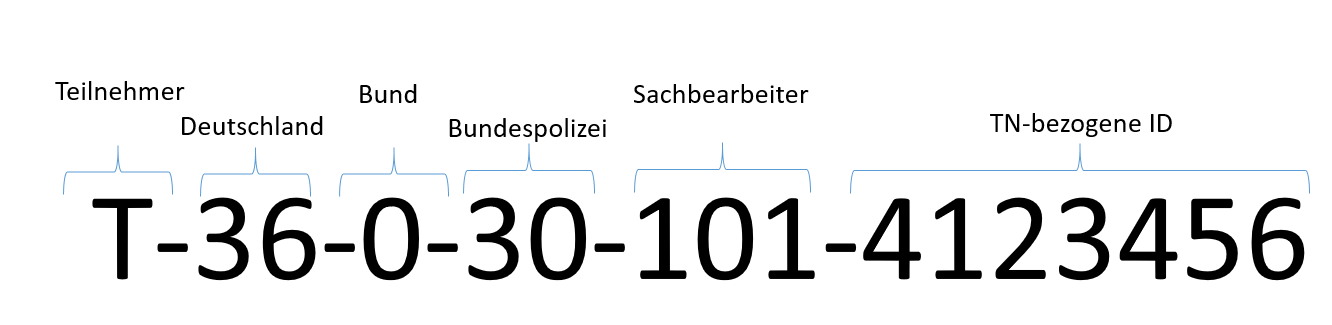
Auch bei der Zuordnung zum Staat, des TN oder Bund-Länderangabe wird die zulässige Wertemenge über eine eigene Code-Liste vorgegeben, die von P20-IAM-Verantwortlichen gepflegt wird, um zukünftig möglichst flexibel auf großflächige Restrukturierungen reagieren zu können. So wird auch eine Entkopplung zu etwaigen Katalog-Veränderungen ermöglicht.

Die derzeit zulässigen Werte der ersten fünf Segmente werden im Anhang unter „5.2. Zulässige Werte je P20-UID-Segment“ aufgeführt.

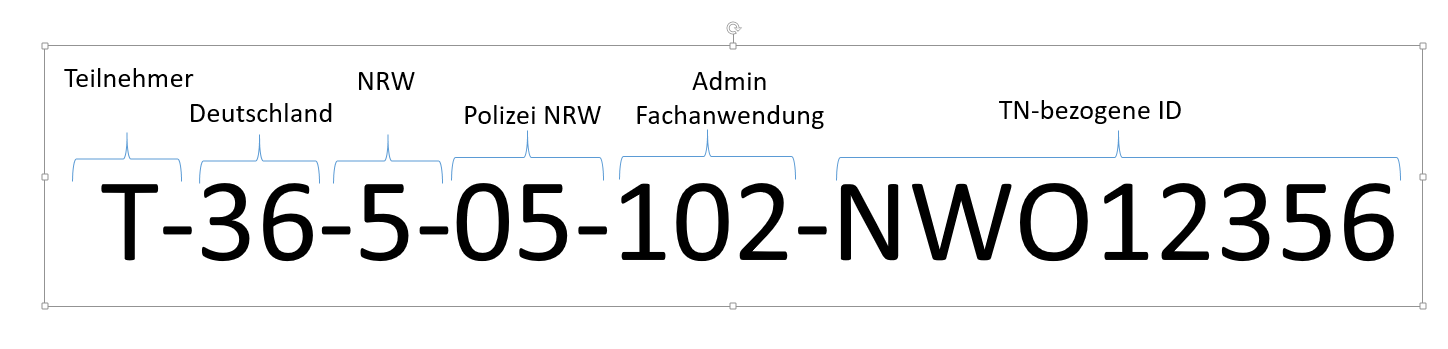
| Segment | Anzahl Zeichen | **Attribut** | **Beschreibung** | **Zulässige Werte** |
| --- | --- | --- | --- | --- |
| 1 | 1 | TN oder Partner | Teilnehmer: T  Partner:P | Codeliste – Vorgabe durch P20 IAM: Code-Liste:  TN= T  Partner:P |
| 2 | 1-3 | Staatenzuordnung | Staatenzuordnung der Partnerbehörde / Teilnehmer der Identität. Bei internationalen Partnern (z.B. Europol / Interpol):0 | Codeliste – Vorgabe durch P20 IAM mit Anlehnung an Xpolizei-Katalogliste 208 (Staaten) |
| 3 | 1-2 | Bundesland | Länderzuordnung | Codeliste – Vorgabe durch P20 IAM mit Anlehnung an Xpolizei-Katalogliste Länder 321, Bundesbehörden:0  Internationale Behörden 99 |
| 4 | 2-11 | Eindeutige TN-ID/Partner ID | Angabe der jeweiligen individuell noch festzulegenden PartnerID, TN-ID | Festlegung durch P20 IAM Betrieb  TN-ID orientiert sich an Katalog 287 Teilnehmerschlüssel. |
| 5 | 3 | Identitätstyp | z.B. TN-Bezogene Anwender-Identität eines internen Anwenders, TN-bezogene Anwender-Identität eines externen Mitarbeiters, TN-Bezogene Administrative Identität eines Mitarbeiters, TN-bezogene | Codeliste – Vorgabe durch P20IAM |
| 6 | 5-11 | Eindeutige ID beim TN | Ein durch den Teilnehmer frei zu vergebener Alphanumerischer Wert. Er muss die Eindeutigkeit dieser ID beim Teilnehmer / Partner verbindlich sicherstellen. | Ein entweder durch den Teilnehmer oder P20 IAM UID-Generator frei zu vergebener alphanumerischer Wert. Er muss die Eindeutigkeit dieser ID beim Teilnehmer / Partner verbindlich sicherstellen.  Wert 0-9 bzw. A-Z |

*Tabelle 1 – Detaillierter Aufbau der P20-UID*

Die folgende P20-UID stellt die exemplarisch die UID eines Mitarbeiters dar, der in der Bundespolizei für P20 sachbearbeitend tätig ist.



Die folgende P20-UID stellt die exemplarisch die UID eines Mitarbeiters dar, der bei der Polizei NRW in einem oder mehreren Fachverfahren als Administrator tätig ist.



Im folgenden werden exemplarische Aufbauten einer P20UID mit unterschiedlichen Varianten exemplarisch dargestellt**.**

| Identitätsbeschreibung | UID |
| --- | --- |
| Anwenderkonto Interner Mitarbeiter Sachbearbeitung Bundespolizei | T-36-0-18-101-4123456 |
| Anwenderkonto Mitarbeiter Sachbearbeitung NRW | T-36-5-05-101-NW056731 |
| Administrationskonto für Fachanwendungen eines Mitarbeiters NRW | T-36-5-05-102-NWO56731 |
| Anwenderkonto Mitarbeiter Sachbearbeitung einer internationalen Partnerbehörde (nur exemplarische Darstellung) | P-0-99-*A17567*-101-XYZ1234591 |

Tabelle 2 – Beispiele P20-UIDsgemäß der P20-UID Systematik

## Generierung und Registrierung der P20-UID

Zur Sicherstellung der eindeutigen und einmaligen Vergabe einer P20-UID zur Nutzung im Kontext P20 und dem dortigen F-IAM muss diese nach ihrer Generierung an zentraler Stelle registriert werden. Die registrierte P20-UID eines Benutzerkontos ist die Voraussetzung, um auf P20-Services zugreifen zu können.

Der P20-UID-Store ist dabei der Speicherort für alle jemals vergebenen registrierten P20-UIDs. P20-UIDs werden dort niemals gelöscht, um die Einmaligkeit sicherzustellen. Weder bei der Registrierung noch bei der Generierung werden dabei von den Teilnehmern personenbezogen Daten zur P20-UID an den P20-UID-Store übermittelt.

Es werden unterschiedliche Varianten zur Generierung und Registrierung ermöglicht, um sich flexibel in bestehende Geschäftsprozesse der TN hinsichtlich der Benutzerprovisionierung integrieren zu können.

Die Prozesse zur Generierung und Registrierung der P20-UIDs werden in de nachfolgenden Kapiteln beschrieben. Dabei werden auch die Prozessverantwortlichkeiten beim Teilnehmer und den Betreibern des F-IAM genau spezifiziert. Eine sehr grobe Beschreibung kann den folgenden Punkten entnommen werden.

### TN-seitige Beantragung zur Generierung / Registrierung einer P20-UID

Der Teilnehmer sendet seinen Antrag in einem vorgegebenen Format an die Schnittstelle und erhält bei positiver Prüfung und Abarbeitung die P20-P20-UID von der P20-UID-Schnittstelle als Rückgabewert. Hierfür übergibt der Teilnehmer die vorgesehenen Parameter in dem Antrag. Dabei werden keinen personenbeziehbare Daten übertragen.

Die folgende Abbildung skizziert den erfolgreichen Verlauf einer solchen automatisierten Beantragung. Im Fehlerfall erfolgt eine qualifizierte Fehlermeldung.

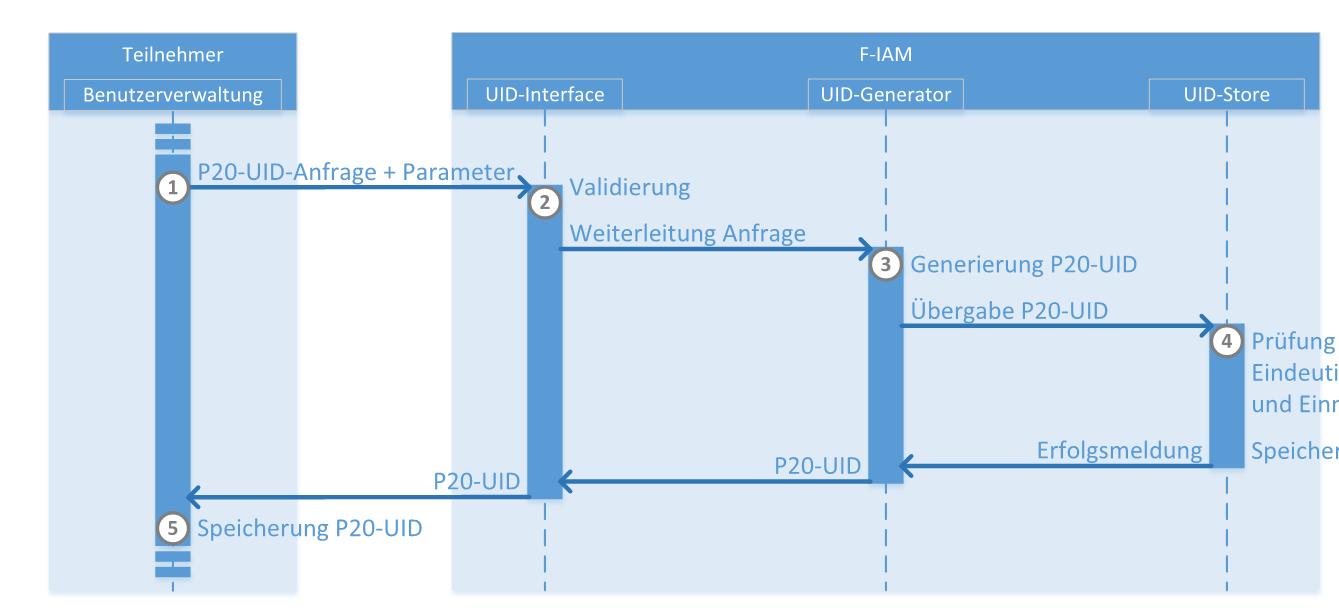


Abbildung 1 TN-seitige Beantragung zur Generierung und Registrierung einer P20-P20-UID

1. Anfrage der TN Umgebung:  
   Die TN Umgebung (bspw. IAM-System beim TN) sendet automatisiert (ggfs. nach erfolgreicher Authentifizierung an der Schnittstelle) den Request zur Registrierung der vorgesehenen P20-UID mit den benötigten Daten im festgelegten Format an das P20-UID-Inferace F-IAM.
2. F-IAM P20-UID Interface:   
   Die Schnittstelle des F-IAM nimmt die Anfrage entgegen, prüft auf syntaktische Richtigkeit der übergebenen Parameter und leitet sie an den P20-UID-Generator weiter.
3. Der P20-UID-Generator generiert die P20-UID und leitet sie an den P20-UID-Store weiter
4. Im P20-UID-Store erfolgt eine Prüfung auf Eindeutigkeit und im Positiv-Fall eine Speicherung. Anschliessend erfolgt ein Rückgabe an TN Umgebung

### TN-seitige Generierung der P20-UID und zentrale Registrierung

Bei einigen TN trägt eine eigenständige Generierung der P20-UID zur besseren Einbettung in die schon vorhandenen Geschäftsprozesse zur Benutzerprovisionierung bei. Folgendes Idealbild skizziert hier den leicht geänderten Prozess zur Generierung- und Registrierungsprozess:

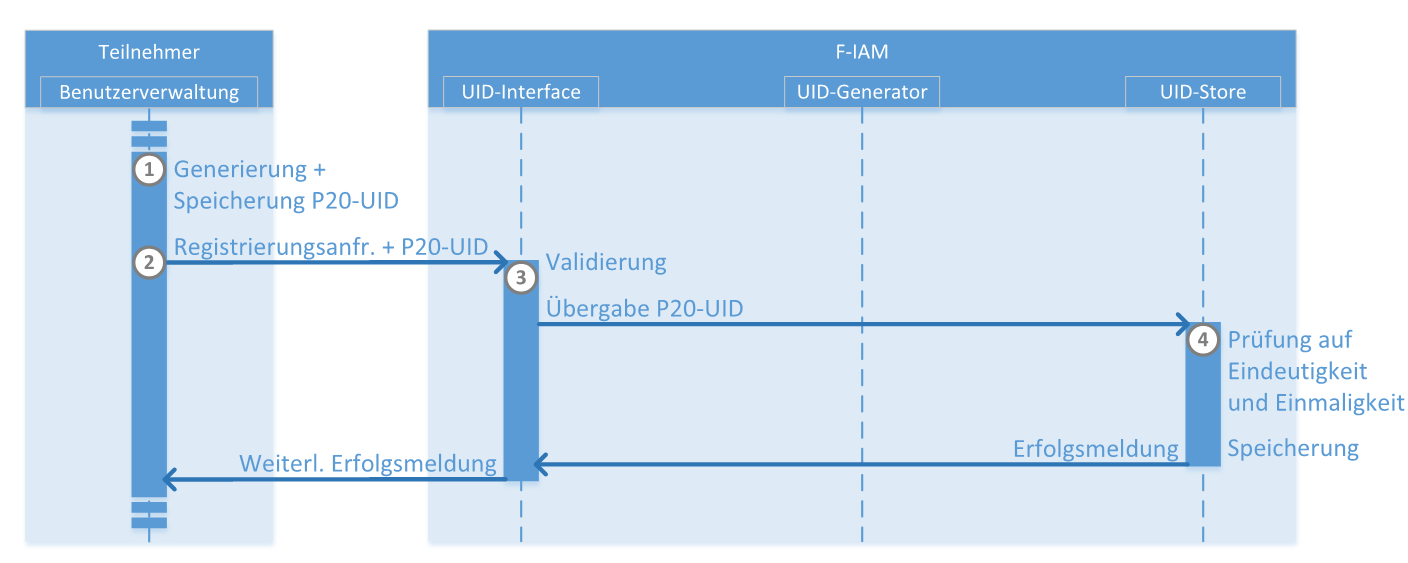
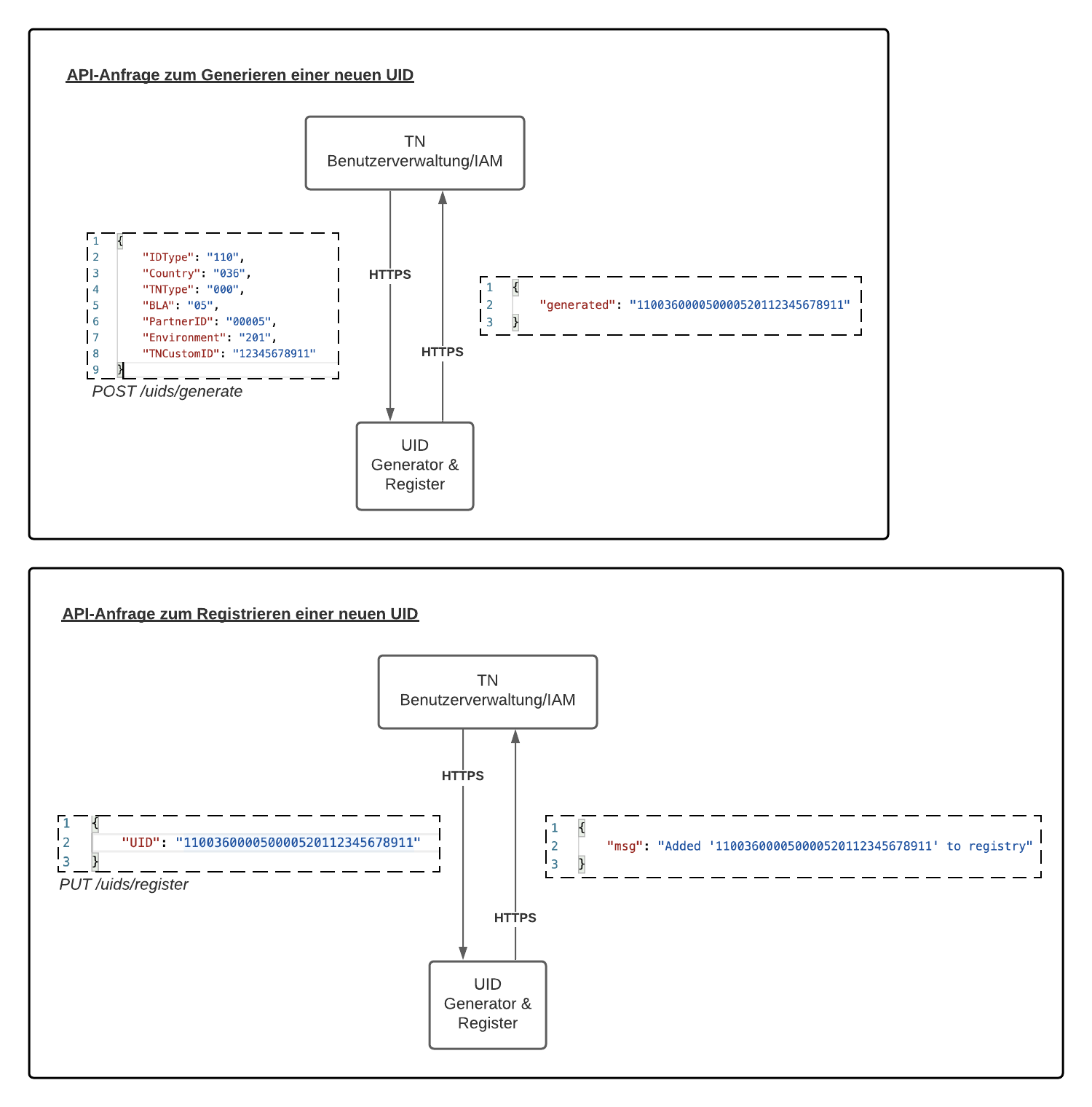


Abbildung 2 TN-seitige Generierung und zentrale Registrierung einer P20-P20-UID

1. Generierung der P20-UID in der TN-Benutzerverwaltung :  
   Die TN Umgebung (bspw. IAM-System beim TN) generiert und speichert (ggfs. nach erfolgreicher Authentifizierung an der Schnittstelle) die P20-UID unter Einhaltung der vorgegebenen Regelwerke und dem festgelegten Format an das P20-UID-Inferace F-IAM.
2. Registierungsanfrage an das F-IAM P20-UID Interface:   
   Die Schnittstelle des F-IAM nimmt die Anfrage der TN-Benutzervwaltung entgegen und leitet sie an den P20-UID-Store weiter.
3. Der P20-UID-Store prüft auf Plausibilität und Eindeutigkeit der übergebenen P20-UID und registriert im Positivfall die P20-UID.
4. Die Benutzerverwaltung des TN erhält über das F-IAM P20-UID Interface eine Erfolgsmeldung.

Sollte die TN-Benutzerverwaltung über das P20-UID-Interface die Rückmeldung erhalten, dass die Plausibilitäts- und Eindeutigkeitsprüfung fehlgeschlagen ist, ist die generierte P20-UID in der TN-Benutzerverwaltung zu entfernen.



# Gesamtsystemarchitektur

## Anforderungen an die Teilnehmer

Die P20-UID ist ein für jeden auf P20/20-Services zugreifenden Benutzer-Account generierter und eindeutiger Schlüssel. Sie bleibt über den gesamten Lebenszyklus des Benutzer-Accounts hinweg unveränderlich und darf nicht wiederverwendet werden.

Der Basisdienst IAM der Plattform P20/20 stellt Services für die a.) Generierung und b.) Registrierung der P20-UID durch den Teilnehmer zur Verfügung.

Insgesamt müssen die Identity- und Access-Management Systeme beim TN ertüchtigt werden, um die zentrale Generierung zu beauftragten oder der eigenständig generierte P20-UIDs im F-IAM zu registrieren. Zudem müssen sie an der zugeordneten Identität zu speichern. Die P20-UID ist berechtigten Systemen beim TN oder P20/20 zur Verfügung zu stellen.

Jede P20-UID darf in seiner Existenz nur einer Person (Eindeutigkeit) und aus Sicht des P20-UID-Prozesses nur einmalig zugeordnet werden (Einmaligkeit). Die dafür notwendigen Generierungs- und Registrierungsprozesse zwischen den TN IAMs und dem Basisdienst IAM P20/20 sind wesentlich für die Korrektheit und Vertrauenswürdigkeit des Attributs P20-UID für einen Benutzer-Account.

Im polizeilichen Umfeld wird die Generierung und Registrierung der Identität durch autorisierte Mitarbeitende der Behörde veranlasst. Generiert und registriert wird eine P20/20-P20-UID für einen Mitarbeiter/ eine Mitarbeiterin der TN nur dann, wenn ein Zugriff auf die P20/20 Services beziehungsweise die PSP bzw. dem Datenhaus benötigt wird. In diesem Zuge werden für das Benutzerkonto beim Teilnehmer die entsprechenden Prozesse zur Generierung und Registrierung einer P20/20-P20-UID angestoßen. Regelungen bzgl. der Zuweisung und der Nutzung mehrerer Benutzerkonto zu einer Person müssen festgelegt werden.

## 

# Anhang

## Glossar

|  |  |
| --- | --- |
| **Begriff / Abkürzung** | **Beschreibung** |
|  |  |
|  |  |
|  |  |

Tabelle 3 – Glossar

## Zulässige Werte je P20-UID-Segment

|  |  |
| --- | --- |
| **Zulässige Werte 1.Segment (Kategorie Partner / Teilnehmer** | |
| **Wert** | Beschreibung |
| **P** | Partner |
| **T** | Teilnehmer |

Tabelle 4 Segment 1 „Kategorie Partner“ / Teilnehmer – derzeit zulässige Werte

|  |  |
| --- | --- |
| **Zulässige Werte 2.Segment (Staat)** | |
| **Wert** | Beschreibung |
| **36** | Deutschland |

Tabelle 5 Segment 2 „Staat“– derzeit zulässige Werte

|  |  |
| --- | --- |
| **Zulässige Werte 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 |
| **13** | Mecklenburg-Vorpommern |
| **14** | Sachsen |
| **15** | Sachsen-Anhalt |
| **16** | Thüringen |

Tabelle 6 Segment 3 „Bund/Land/International“– derzeit zulässige Werte

|  |  |
| --- | --- |
| **Zulässige Werte 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 |
| **31** | Zollkriminalamt |
| **36** | Polizei beim Deutschen Bundestag |

Tabelle 7 Segment 4 „Partner- bzw. TeilnehmerID“– derzeit zulässige Werte

|  |  |
| --- | --- |
| **Zulässige Werte 5.Segment Identitätstyp** | |
| **Wert** | Beschreibung |
| **101** | Anwenderkonto - Mitarbeiter |
| **111** | Administrationskonto für Fachanwendungen |