Einführung einer personenbezogenen ID im Programm Polizei 20/20

– P20-UID –

Version 2.0| Stand **02.06.2022**

GEMEINSAM. DIGITAL. VERNETZT.

Dokumenteninformation				
Programm	Polizei 20/20			
Programmleiter	Holger Gadorosi			
Projektleiter/Verantwortlicher	Norbert Linde			
Dokumententitel	Einführung einer personenbezogenen ID im Programm Polizei 20/20			
Version	2.0			
Erstellt am **Erstellt von**	17.06.2021 PG IAM (OE)			
Zuletzt bearbeitet am **Zuletzt bearbeitet von**	02.06.2022 PG IAM			
Status	In Bearbeitung	Vorgelegt	Freigegeben **X**	Verworfen

Freigabe Hauptversion 1.0 durch Freigabeverantwortlichen bzw. zuständiges Gremium
Freigegeben am: 28.06.2022
Freigegeben von: 39. BLProgT, TOP 5.4

Versionshistorie			
Version	**Datum**	**Erstellt durch**	**Inhaltliche Kurzbeschreibung der Neuerungen**
0.1	16.06.2021	Jens Haug, Christian Müller, Holger Puttkammer	Ersterstellung des Dokumentes
0.2	29.06.2021	UAG P20-UID	Erster Grobentwurf; Einbindung KTT Hr. Donner
0.3	27.07.2021	WS PG IAM	Fortschreibung
0.4/041	12.08.2021	WS PG IAM	Fortschreibung
0.42	24.08.2021	UAG P20-UID	Fortschreibung aus QS
0.9	12.10.2021	PG IAM	Einarbeitung Rückmeldung CCF
0.91	22.10.2021	PG IAM	Einarbeitung Rückmeldung aus WS mit den P2020-Projekten
1.0	10.01.2022		Freigegeben von: 34. BLProgT, TOP 5.2
1.1	04.02.2022	PG IAM	Fortschreibung nach Rückmeldungen Umlaufverfahren und Bereich „Recht und Datenschutz“
1.2	14.03.2022	PG IAM	Einfügen von gültigen Werten je UID-Segment im Anhang

1.3	11.05.2022	PG IAM	Überarbeitung des Registrierungsprozesses nach Rückmeldung BKA
1.4	25.05.2020	PG IAM	Version zur Übergabe SKT
1.4	02.06.2022	24.SKT	Klarstellung in Ziffer 4.2.2 (4. Absatz neu)

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. 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 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 Konzept beschreibt dazu:

- Rahmenbedingungen
- Anforderungen an eine P20-UID
- Gestaltung und die Generierung der P20-UID
- Anforderungen an Teilnehmer hinsichtlich der Ausstattung der Identitäten mit der P20-UID sowie die Anforderungen an Anwendungen zur Verwendung der P20-UID.

Die P20-UID soll ein zusätzliches Merkmal zur Kommunikation mit der Plattform sein. Dies bedeutet, dass sie, abseits der Ertüchtigung der TN-Benutzerverwaltungen keine Auswirkungen auf die TN-internen Systeme hat.

Die P20-UID ist nicht als interaktiver Login-Name für die Anmeldung konzipiert.

Innerhalb des Dokumentes wird gelegentlich das generische Maskulinum verwendet. Dies soll jedoch alle Geschlechter umfassen.

2. 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
  [Anmerkung: Abweichung zum generellen Glossar der PG IAM; hier ohne „juristische Person“ und „Objekte“].
  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.

3. Ausgangssituation und Zielsetzung

3.1. Ausgangssituation

Das Programm Polizei 20/20 benötigt für die integre Kommunikation zwischen den Schnittstellen der Teilnehmer, der PSP und dem Datenhaus für die Protokollierung und bereitgestellten Services einen bundesweit eindeutigen technischen Identifikator für digitale, personenbezogene Identitäten.

Die „Expertengruppe IAM 2018“ legte u.a. in ihrem Zwischenbericht 2018 fest, dass die derzeit bei den Teilnehmern (und Partner [*1)) verwendeten Benutzerkennungen für den Zugriff auf P20/20-Anwendungen verwendet werden sollten und definierte für ihren Einsatz in der Identitätsföderation u.a. die folgende Vorgaben:

- *Bei allen Teilnehmern wird über den jeweiligen Identity Provider (z.B. ADFS) eine eineindeutige Benutzerkennung, der sog. User Principal Name (kennung@bundesland.de, UPN), bereitgestellt.*
- *Dieser UPN darf sich nicht ändern und auch nicht wiederverwendet werden.*
- *Über den UPN muss die Landeskennung erkennbar sein (überschneidungsfrei).*

*1) Hinweis: die EG IAM 2018“ hatte damals sog. „Partner“ (z.B. Staatsanwalten) noch nicht im Blickfeld.

Der „USER Principal Name“ wurde deswegen im IMP als personenidentifizierendes Attribut zur Kennzeichnung des Sachbearbeiters der „beteiligten Stelle“ hinterlegt.

Als eindeutiger Identifikator für das Programm Polizei 20/20 kommt er allerdings aus folgenden Gründen nicht in Betracht:

- Größere infrastrukturelle, produktbezogene oder konzeptionelle Veränderungen können veränderte Nutzungen des UPN notwendig machen. Die langfristige zukünftige Flexibilität für alle Beteiligten erhöht sich erheblich, wenn hier ein Identifikator verwendet wird, der keinerlei Abhängigkeiten zur derzeitig eingesetzten Technik besitzt.
- In den Protokoll- oder Verfahrensdaten des Polizei 20/20-Programms müssen die gesetzlichen Datenschutzanforderungen für die Daten der Mitarbeitenden umgesetzt werden. Die dabei mögliche Verwendung einer Polizei 20/20 ID, die im Vergleich zum derzeitigen Bestand an UPN keine personenbezogenen Daten in der ID enthält, bietet dabei ausreichend Schutz. Der derzeitige Bestand an UPN´s bei einigen Teilnehmern erfüllt diese Anforderungen hingegen nicht. Sie verwenden Kennungen, in denen Namensbestandteile, Geburtsdaten oder anderweitige personenbeziehbare Daten enthalten sind. In den projektübergreifenden, nichtfunktionalen Anforderungen des Programm P20/20 wird eine Verwendung von personenbezogenen Daten in technischen Protokollen ausgeschlossen.

3.1.1. Berücksichtigung von Zugriffen auf das P20-Services und -Anwendungen aus „Partnerorganisationen“

Zum jetzigen Zeitpunkt steht noch nicht fest, aus welchen nicht-teilnehmerbezogenen Institutionen Mitarbeiter auf P20-Anwendungen über personenbeziehbare Identitäten eventuell zugreifen werden.

Entsprechende Anwendungsfälle sind derzeit im Programm fachlich nicht beschrieben, könnten aber zukünftig entstehen, z. B. für:

- Mitarbeitende aus bundesbezogenen- oder landesbezogenen Justizbehörden (z.B. Staatsanwaltschaften)
- Im Rahmen internationaler polizeilicher Zusammenarbeit mit Polizisten anderer Staaten bzw. internationaler Polizeiorganisationen
- Mitarbeitende von kommunalen oder kreisbezogenen Institutionen
- Mitarbeitende r aus anderweitigen Behörden mit hoheitlichen Aufgabenbereichen

3.2. Zielsetzung

Jede Identität einer Person, die für den direkten oder indirekten Zugriff auf P20-Services und dem Datenhaus vorgesehen ist, soll mit einem eindeutigen, nicht veränderbaren, nach vorgegebenem Schema und Regeln aufgebauten Identifikator-Attribut ausgestattet werden. Dieses wird für die Kommunikation zwischen den Schnittstellen der Länder, PSP / Datenhaus, den Anwendungen und Diensten sowie deren Protokollierung herangezogen. Somit wird der Erstellende oder Lesende eines Informationssachverhalts zweifelsfrei service-übergreifend kenntlich gemacht. Diese ID ersetzt den derzeitig verwandten UPN im IMP als Referenz auf den Sachbearbeitenden der beteiligten Stelle. Die zu gestaltende P20-UID ist

- Zukunftssicher
- Entspricht den Datenschutz- und Sicherheitsanforderungen des Programms
- Bietet auch die Möglichkeit, Identitäten von Partnern mit eindeutigen IDs auszustatten.

3.3. Stakeholder

Folgende Stakeholder sind identifiziert:

Stakeholder	Rolle
IAM-Verantwortliche der TN	Bei den TN erfolgt die Anbindung der IAM-Lösung sowie die Einführung einer P20-User ID
Datenschutz	Die rechtliche und / oder datenschutzrechtliche Prüfung ist von der AG Recht und / oder AG Datenschutz zu erbringen
Basisdienst Protokollierung	Vorgaben zur ID-Verwendung nach datenschutzrechtlichen Vorgaben
KTT (Kernteam Technik)	Schnittstelle Technik zur Fachlichkeit und Strategie (IT-Sicherheit)
P20 TN -Allgemein	Bedarfsträger um TN-eigene (Dritt-)Anwendungen an Teilanwendungen des Datenhauses von P20/20 anzubinden
XPolizei/NG	Umsetzungsinstitution für Anforderungen an das XPolizei-Modell
SK-T/SK-F (Steuerkreis Technik/Fachlichkeit)	Konzeptabnahme als Vorinstanz zur BLProgT

P20 Projektverantwortliche Polizeiliche Sachbearbeitung / Verbund / Mobilität /	Anforderungen an Anwendungen zur Verwendung der P20-UID
PAM	Management der IT-Gesamtarchitektur (NFAs) / Standard XPolizei
UA IUK	Unterausschuss Information und Kommunikation insb. K-AS

Tabelle 1 – Stakeholder

3.4. Organisatorischer und technischer Rahmen

3.4.1. Festlegung zur Verwendung von Benutzerkennungen aus den Verzeichnisdiensten der Teilnehmer

Die Teilnehmerumfragen aus den Jahren 2018 und 20/20 (Expertengruppe IAM 2018, Polizei 20/20 IAM) stellen dar, dass auf Teilnehmerseite die Benutzerkonten-Bereitstellung über die teilnehmerbezogenen Verzeichnisdienste erfolgt. Bis auf einen Teilnehmer wird dabei der Verzeichnisdienst "Microsoft Active Directory“ (AD) (in verschiedenen Versionsständen) verwendet.

Folgende Festlegungen wurden von der Expertengruppe IAM 2018 getroffen und von der PG IAM 20/20 übernommen:

- *die Benutzerkonten aus den ADs werden zum Zugriff auf die bereitgestellten Dienste der Plattform verwendet*
- *Die Authentifizierung und die Pflege der Benutzer erfolgt beim jeweiligen Teilnehmer. Entsprechende Prozesse für den LifeCycle einer Identität sowie die Genehmigungsprozesse für z.B. Rollenzuweisungen liegen daher weiter in der Verantwortung des jeweiligen Teilnehmers. Dort wird sichergestellt, dass die Identität vorhanden ist und authentifiziert werden kann. Der jeweilige Teilnehmer stellt auch sicher, dass Organisationszugehörigkeiten sowie die Übertragung von Businessrollen eines Benutzers jeweils erfolgen.*

3.4.2. Heterogene Benutzerkonten-Konventionen

Die Pflege der Identitäten in den Verzeichnisdiensten der Teilnehmer erfolgt nach eigenen unterschiedlich ausgeprägten Konzepten. Hier gab es in der Vergangenheit keine gemeinsam konzipierten Vorgaben. Die gewachsenen Namenskonventionen und Attributsverwendungen für Benutzerkennungen sind deswegen bei jedem Teilnehmer individuell.

3.4.3. Verwendung der TN-bezogen Benutzerkontennamen in TN-bezogenen Drittverfahren

Die Umfrage der PG IAM Programm 20/20 ergab, dass sehr häufig die Benutzerkontennamen auch als Identfizierer in etlichen Drittverfahren der Teilnehmer verwendet werden. Änderungen der Konventionen dieser Benutzerkonten-Namen verursachen bei den einzelnen Teilnehmern äußerst komplexe und aufwändige Projekte mit sehr großem Abstimmungsaufwand. Diese Problematik wird dadurch vermieden, dass die P20-UID als neues Attribut eingeführt wird.

3.4.4. Mehrere Benutzerkonten für eine natürliche Person

Für unterschiedliche Aufgabengebiete eines Mitarbeitenden werden aktuell auch unterschiedliche Benutzerkonten in den Verzeichnisdiensten verwandt. Oftmals werden auf Vorgabe der IT-Sicherheit zur Administration von Umgebungen / Fachanwendungen dedizierte Benutzerkonten verwendet.

3.4.5. Berücksichtigung des Transformationsprozesses

Das Transformationskonzept beschreibt u.a. das strategische Vorgehen zur Transformation der Programm-Vorhaben im Sachbearbeitungs- sowie im Verbundbereich. Es ist dabei sicherzustellen, dass auch schon in der Transformation befindliche Verfahren / Anwendungen eine einheitliche P20-UID für die Identitäten der Mitarbeitenden verwenden, um bei der Kommunikation über die Schnittstellen der Länder, dem PSP / Datenhaus den Erstellenden oder Leseenden eines Informationssachverhaltes zweifelsfrei kenntlich zu machen.

3.4.6. Umsetzung in XPolizeiNG

Innerhalb des IMP wird ab der Version 2.5 ein **Unique Identifier** (P20-UID) für personenbezogene Identitäten (z.B. den Benutzerkennungen in den Verzeichnisdiensten der Teilnehmer) aufgenommen. Er ersetzt den bisherigen Identifier (User Principal Name) im XPolizei-Standard.

4. Anforderungen

Nachfolgend werden die Anforderungen an eine P20-UID dargestellt. Die Anforderungen fließen in die übergreifenden Anforderungsliste IAM ein. Die Notation der Anforderungen ergibt sich aus der Anforderungsliste.

4.1. Datenschutz

4.1.1. Pseudonymisierung von Mitarbeiterdaten

IAM DS_13: Die P20-UID soll keine personenbezogenen oder personenbeziehbaren Daten von Mitarbeitenden enthalten.

IAM_F_DS_14: Bei jedem Protokollierungsprozess, bei dem der Benutzer erfasst werden soll, ist immer die P20-UID als einziges Attribut zur Zuordnung von Identitäten zu verwenden.

Gemäß § 3 BDSG sollen öffentliche und nicht öffentliche Stellen, die mit personenbezogenen Daten umgehen, immer unter der Maßgabe arbeiten, nur so viele Daten zu speichern, zu nutzen oder zu verarbeiten, wie für den jeweiligen Zweck von Nöten sind. Diese sollen zudem – soweit möglich – anonymisiert oder pseudonymisiert werden. Bei der Pseudonymisierung wird das Originaldatum durch einen anderen Wert ersetzt, wobei die Zuordnung zwischen Original und Ersatz abgespeichert wird. Wenn zu einem späteren Zeitpunkt das Originaldatum benötigt wird, kann es anhand der abgespeicherten Zuordnung abgerufen und rekonstruiert werden. Eine projektübergreifende Anforderung des Programmes ist, sofern möglich, die Pseudonymisierung von Mitarbeiterdaten auch in Protokollierungsdaten zu verwenden. Dabei wird die Verwendung von Namen, Namensbestandteilen oder anderweitigen sensiblen mitarbeiterbezogenen Daten (Steuernummern-IDs, Geburtsdaten) ausgeschlossen.
Auch folgender Auszug aus dem Bundesdatenschutzgesetz stellt die Anforderung dar, dass die einschlägigen technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen sind. Bei der Verarbeitung von personenbezogenen Daten soll hier bspw. eine Pseudonymisierung der Daten - wenn möglich - vorgenommen werden.

§64 BDSG (neu) – Anforderungen an die Sicherheit der Datenverarbeitung

(1) Der Verantwortliche und der Auftrags[daten]verarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

(2) Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt wird und

2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann.

Gemäß diesen gesetzlichen Vorgaben verpflichten sich das Programm Polizei 20/20 bzw. seine Dienstleister zur Einhaltung dieser Gesetzeslagen. Namensbestandteile bzw. sonstige personensensible Daten von Mitarbeitenden sind bei der technischen Protokollierung nicht zu verwenden. Stattdessen werden IDs verwendet werden, die diese Informationen nicht enthalten. Auch bei der vorgeschriebenen datenschutzrechtlichen Protokollierung, die durch den entsprechenden Basisdienst bereitgestellt wird, wird diese ID verwendet werden, um die Identität der Person zweifelsfrei zuzuordnen, die über P20-relevante Anwendungen entweder personenbezogene Daten abgefragt oder offengelegt hat, oder die Empfänger der Daten ist. Hier soll eine „einheitlich" anwendungsübergreifende programmweit genutzte Personen-ID genutzt werden.

4.1.2. Direkte Zuordnung von pseudonymisierten Mitarbeiter-ID`s zu Teilnehmern und Partnern

IAM_DS_15: Um eine Zuordnung der P20-UID zur zuständigen Einrichtung vornehmen zu können, muss eine Teilnehmer- bzw. Partner-Zuordnung aus der P20-UID ableitbar sein.

IAM_F_DS_16: Der für einen Anwendenden verantwortliche Teilnehmer muss eine eindeutige Zuordnung der P20-UID zu dem Nutzer ermöglichen.

Die Verwendung der datenschutzrechtlichen Protokollierung ist im §76 BDSG festgelegt.

Zudem schreibt der §81 Abs. 1 BKAG eine elektronische Auswertbarkeit für die Datenschutzbeauftragten vor. Daraus ergibt sich, wer zu welchem Zweck Einsicht in die datenschutzrechtliche Protokollierung nehmen darf. Entsprechend dürfen Protokolldaten nur den zuständigen Datenschutzbehörden und –beauftragten sowie den zuständigen Verantwortlichen zur Kontrolle der Datenschutzvorgaben (Eigenüberwachung) zugängig gemacht werden. Sind die Protokolldaten im Rahmen der Strafverfolgung erforderlich, könnten sie über die vorgenannten Personen/Einrichtungen herangezogen werden.

Um hier eine direkte Zuordnung der ID zu entsprechenden Einrichtung bzw. den einzubindenden Datenschutzbehörden- und dem Beauftragten vornehmen zu können, sollte eine Teilnehmer- bzw. Partner-Zuordnung aus der P20-UID ableitbar sein.

4.2. IT-Sicherheit

4.2.1. Eindeutige Zuordnung von Identitäten zu Personen

IAM_DS_15: Um eine Zuordnung der P20-UID zur zuständigen Einrichtung vornehmen zu können, muss eine Teilnehmer- bzw. Partner-Zuordnung aus der P20-UID ableitbar sein.

IAM_F_DS_16: Der für einen Nutzer verantwortliche Teilnehmer muss eine eindeutige Zuordnung der P20-UID zu dem Nutzer ermöglichen.

Das BSI sieht in seinen IT-Grundschutz-Bausteinen den Baustein ORP.4 (Organisation und Personal Identitäts- und Berechtigungsmanagement) vor, dass das IAM gewährleistet, dass den Benutzern nur die Berechtigungen gegeben werden, die zur Aufgabenerfüllung notwendig sind (ORP.4.A2, „least privileges“, „need to know“). Dabei muss jede Benutzerkennung eindeutig einem Benutzer zugeordnet werden können (ORP.4.A1). Zudem sollte kontrolliert werden, dass nicht mehrere Benutzer mit der gleichen Kennung arbeiten, bzw. dass sich die Benutzer regelmäßig abmelden (ORP.4.A14). Die P20-UID sollte diese Anforderungen unterstützen, indem sie neben dem eindeutigen Benutzer auch weitere Informationen beinhaltet, die auf den TN rückschliessen lassen und es so ermöglichen, Erkenntnisse aus den Protokollauswertungen bzgl. Nicht-Abmeldungen bzw. Doppel-Anmeldungen zu verfolgen.

Zudem sollte eine P20-UID für den LifeCycle einer Identität an diese gekoppelt werden und nach deren Löschung auch nicht wieder neu vergeben werden.

4.2.2. Kategorisierung von Identitäten

Für unterschiedliche Aufgabengebiete eines Mitarbeitenden können unterschiedliche Benutzerkonten in den Verzeichnisdiensten verwandt werden. Oftmals werden auf Vorgabe der IT-Sicherheit zur Administration von Umgebungen / Fachanwendungen dedizierte Benutzerkonten verwendet.

Mitarbeitende erhalten für die Sachbearbeitung und die Bürokommunikation „normale“ Anwender-Konten, für die administrative Tätigkeiten Administrationskonten.

Jedes Benutzerkonto eines Anwenders sollte eine eigene P20-UID erhalten. Dies bedingt eine Kategorisierung von Identitätstypen (s.u. Tabelle 5).

Die Entscheidung wieviele UIDs eine Person haben kann (z.B. Administrator, Sachbearbeiter) obliegt dem TN und ist i.d.R. abhängig von den TN-eigenen Prozessen der Benutzerverwaltung.

Die P20-UID umfasst insgesamt 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. Das erhöht die zukünftige Anpassfähigkeit. Anbei die Auflistung der Segmente:

1. Kategorisierung TN oder Partner
2. Informationen zur Staatenzuordnung, des zu der Identität gehörenden Partners oder Teilnehmers
3. Informationen zur Bundeslandzuordung des Teilnehmers (Bund oder Internationale Behörden werden aufgeführt)

4. Die Partner- bzw. Teilnehmer-ID (2-11 Zeichen)
5. Informationen zum Identitätstyp (z.B. Interner Sachbearbeiter, Administrative Identität)
6. 5 bis 11 stelliger-Bereich zur freien Vergabe beim Teilnehmer, der die eindeutige Zuordnung der ID zum Benutzerkonto und damit zur Identität beim Teilnehmer sicherstellt

Eine detaillierte Auflistung der zugeordneten Stellen, der dazugehörigen Beschreibung kann der „Tabelle 2 Detaillierter Aufbau der P20-UID“ entnommen werden. Exemplarische P20-UID-Abbildungen sind in „Tabelle 3 – 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 und sich an XPolizei-Katalogwerte anlehnt.

Die derzeit zulässigen Werte der ersten fünf Segmente werden im Anhang unter „7.2 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	Staatenzuordung 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.

Segment	Anzahl Zeichen	**Attribut**	**Beschreibung**	**Zulässige Werte**
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 2 – Detaillierter Aufbau der P20-UID

) in der P20-UID.

4.3. Zukunftssicherheit

4.3.1. Technische Unabhängigkeit der P20-UID

IAM_ZS_01: Die P20-UID soll als eigenständiges, neues, Attribut abgebildet werden.

Größere infrastrukturelle, produktbezogene oder konzeptionelle Veränderungen auf Teilnehmerseite (z.B. bei einem Wechsel des Verzeichnisdienstes) sollten sich nicht auf die P20-UID auswirken. Die langfristige zukünftige Flexibilität für alle Beteiligten erhöht sich erheblich, wenn hier für Polizei 20/20 ein Identifikator verwendet wird, der keine Abhängigkeiten zur derzeitig eingesetzten Technik und Organisationsaufbau besitzt.

Die geplante P20-UID ist ein zusätzliches einzuführendes Attribut, welches mit keinem bereits vorhandenen Attribute in IAM-Systemen der Teilnehmer und der anderen involvierten Systeme (wie z.B. Anwendungen, Protokollierung) im Konflikt stehen darf. Bzgl. IAM wird die P20-UID von den Teilnehmern in den Teilnehmer-IAMs nach dem vorliegenden P20-UID-Konzept als Attribut in der Datenhaltung (bspw. AD DS Schemaerweiterung) erstellt und für Benutzer des TN mit Zugriff auf Services der Plattform vergeben.

Die P20-UID wird von den Teilnehmern im Rahmen von Authentifizierungs- und Autorisierungsvorgängen an das F-IAM übermittelt. Die hier verwendete Technik zur Übermittelung wird in der technischen Konzeption des F-IAM festgelegt und ist nicht Bestandteil dieses Dokuments.

4.3.2. Organisatorische Unabhängigkeit der P20-UID innerhalb der Institionen und des TN

Organisatorische Änderungen sollen keine Auswirkungen auf die P20-UID haben. Die P20-UID ist in dieser Hinsicht unveränderlich.

Beispiele für organisatorische Änderungen sind:

- Umbenennungen von Mitarbeitenden (z.B. durch Heirat)
- Wechsel der Organisationseinheit innerhalb eines Teilnehmers

4.3.3. Ausreichende Anzahl an Zeichen zur Ausstattung der Identitäten für Teilnehmer / und Partner-Zuordnung

Den Teilnehmern müssen zur Ausstattung der Identitäten mit P20-UIDs ausreichende Anzahl an Zeichen Verfügung gestellt werden. Die Länge der einzelner UID-Bereiche sollte auch im Nachhinein noch veränderbar sein.

4.3.4. Mögliche Einbindung von Identitäten von Partnern

Die zu gestaltende P20-UID sollte die Möglichkeit bieten, Identitäten von Partner-Institutionen, die auf P20/20-Services zugreifen sollen, mit Partnerinformationen (Kategorien + IDs dieser Partner) abzubilden.

4.3.5. Ausreichende Anzahl von Zeichen zur Einbindung und Kategorisierung von Partner-Institutionen

Es sollte eine ausreichende Anzahl an Zeichen zur Einbindung und Kategorisierung von Partner-Institutionen berücksichtigt werden.

4.4. Gestaltungsfreiheit für Teilnehmer

Bei einigen Teilnehmern sind schon jetzt teilnehmerweite anwendungsübergreifende identitätsbezogene IDs im Einsatz, die den derzeitigen Anforderungen des Datenschutzes und der IT-Sicherheit hinsichtlich der Pseudonymisierung und der eindeutigen Zuordnung zur Identität genügen und in P20- und Verbund-relevanten Verfahren derzeit eingesetzt werden. Den Teilnehmern sollte die Möglichkeit gegeben werden, diese in einem spezifizierten, teilnehmerbezogenen Teil der P20-UID zu verwenden, um Transformationsprozesse von Verfahren und Diensten auf die P20-Plattform zu vereinfachen. Eine durch das Projekt IAM durchgeführte Teilnehmer-Umfrage ermittelte hier einen Bedarf von derzeit mindestens 8 Zeichen.

4.5. Vermeidung von Komplexitäten

IAM_VK_01: In der P20-UID müssen ausschließlich alphanumerische Zeichen vergeben werden
IAM_VK_02: Bei der Verarbeitung der P20-UIDs muss immer das gleiche Encoding verwendet werden.

In der P20-UID sollen zur Vermeidung von Komplexitäten ausschließlich alphanumerische Zeichen (Wertemengen 0-9 und A-Z, also ausschließlich Großbuchstaben) vergeben werden. Bei der Verarbeitung der P20-UIDs muss immer das gleiche Encoding verwendet werden.

4.6. Einheitlicher stringenter Aufbau

Durch einen einheitlichen stringenten Aufbau der ID sollen die Entwicklung von Skripten, Applikationen, Reports, und Protokollen und deren Auswertungen einfach gestaltet werden.

4.7. Einzigartigkeit der P20-UID

IAM_EI_01: Jede P20-UID muss zu jeder Zeit und an jedem Ort eindeutig sein.

IAM_EI_02: Die Eindeutigkeit der ID muss auf der PSP 20/20 verifizierbar sein.

IAM_EI_03: Der korrekte Aufbau der ID muss auf der PSP 20/20 verifizierbar sein.

4.8. Flexibilität bei der Generierung von P20-UIDs

Um sich optimal in bestehende Geschäftsprozesse zu integrieren, sollen den Teilnehmern unterschiedliche Optionen zur Generierung von P20-UIDs geboten werden. Entweder soll die Generierung eigenständig beim TN erfolgen, oder aber durch einen zentralisierten Generierungs-Service, durch den die TN mit P20-UIDs ausgestattet werden sollen.

5. Aufbau, Generierung und Registrierung der P20-UID

Dieses Kapitel beschreibt den Aufbau sowie die Ausgestaltung und die angedachte Vorgehensweise zur Generierung der P20-UID. Diese erfüllt die im Kapitel 4 gestellten Anforderungen an die P20-UID.

5.1. Aufbau der P20-UID

Die P20-UID umfasst insgesamt 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. Das erhöht die zukünftige Anpassfähigkeit. Anbei die Auflistung der Segmente:

7. Kategorisierung TN oder Partner
8. Informationen zur Staatenzuordnung, des zu der Identität gehörenden Partners oder Teilnehmers
9. Informationen zur Bundeslandzuordung des Teilnehmers (Bund oder Internationale Behörden werden aufgeführt)
10. Die Partner- bzw. Teilnehmer-ID (2-11 Zeichen)
11. Informationen zum Identitätstyp (z.B. Interner Sachbearbeiter, Administrative Identität)
12. 5 bis 11 stelliger-Bereich zur freien Vergabe beim Teilnehmer, der die eindeutige Zuordnung der ID zum Benutzerkonto und damit zur Identität beim Teilnehmer sicherstellt

Eine detaillierte Auflistung der zugeordneten Stellen, der dazugehörigen Beschreibung kann der „Tabelle 2 Detaillierter Aufbau der P20-UID“ entnommen werden. Exemplarische P20-UID-Abbildungen sind in „Tabelle 3 – 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 und sich an XPolizei-Katalogwerte anlehnt.

Die derzeit zulässigen Werte der ersten fünf Segmente werden im Anhang unter „7.2 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	Staatenzuordung 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 2 – 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.

Abbildung 1 Exemplarische Abbildung der P20-UID eines Mitarbeiters der Bundespolizei

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.

Abbildung 2 Exemplarische Abbildung der P20-UID eines Mitarbeiters der Polizei NRW

Im Folgenden werden exemplarische Aufbauten einer P20-UID 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 3 – Beispiele P20-UIDsgemäß der P20-UID Systematik

5.2. Generierung der P20-UID

Die eigenständige Generierung der P20-UID kann in der Benutzerverwaltung der TN erfolgen und dem entsprechenden Benutzerobjekt im TN-IDM zugeordnet werden. Alternativ kann ein durch die P20-IAM bereitgestellter UID-Generierungsservice zur Erzeugung genutzt werden. Auch hier die erfolgt die Zuordnung der UID zum Benutzerobjekt im TN-IDM-System. Grundsätzlich sollte sich ein TN dauerhaft für eine der genannten Generierungs-Varianten entscheiden.

Im Kapitel „6.1 Anforderungen an die Teilnehmer“ wird weitergehend auf diesen Prozess eingegangen.

Die generierte P20-UID muss folgende Eigenschaften besitzen:

- Die P20-UID wurde bis dato nicht vergeben, ist also einmalig.
- Die P20-UID ist syntaktisch richtig aufgebaut.
- Die Werte der TN- oder Partnerbezogenen Segmente stimmen mit den für diesen TN vorgesehenen Werten überein.
- Die vergebenen Werte in den einzelnen Segmenten sind zulässige Werte, also in den Codelisten für das jeweilige Segment enthalten.

5.3. 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 an zentraler Stelle registriert werden. Die registrierte P20-UID eines Benutzerkontos ist die Voraussetzung, um auf P20-Services zugreifen zu können.

Die zentrale Registrierung einer P20-UID erfolgt über die erstmalige Anlage des Benutzerkontos im Benutzerspeicher des F-IAM. Der Basisdienst IAM sieht gemäß Transformationsgrobkonzept IAM eine Provisonierung von Benutzerdaten aus den TN-IAMs in den Benutzerspeicher des F-IAM zur benötigten Versorgung von bestimmten P20-Anwendungen vor. In diesem Zusammenhang wurde im Rahmen des Fachkonzeptes „Vereinbarung zum Austausch von Attributen“ eine Erst-Erhebung zur Ermittlung der benötigten Daten der P20-Fachanwendungen vorgenommen, die zukünftig im Dokument „Anforderungen an die Teilnehmer“ dargestellt werden.

Wird dabei erstmalig ein Benutzer im Benutzerspeicher des F-IAM angelegt, wird die dabei übergebene P20-UID implizit registriert, sofern sie alle dafür notwendigen Voraussetzungen erfüllt.

Für eine Neu-Anlage im Benutzerspeicher stellt die ordnungsgemäß übergebene P20-UID eine zwingende Voraussetzung zur Benutzeranlage dar. Das folgende Sequenzdiagram stellt diesen Vorgang unter Verwendung des P20-SCIM-Interfaces exemplarisch dar.

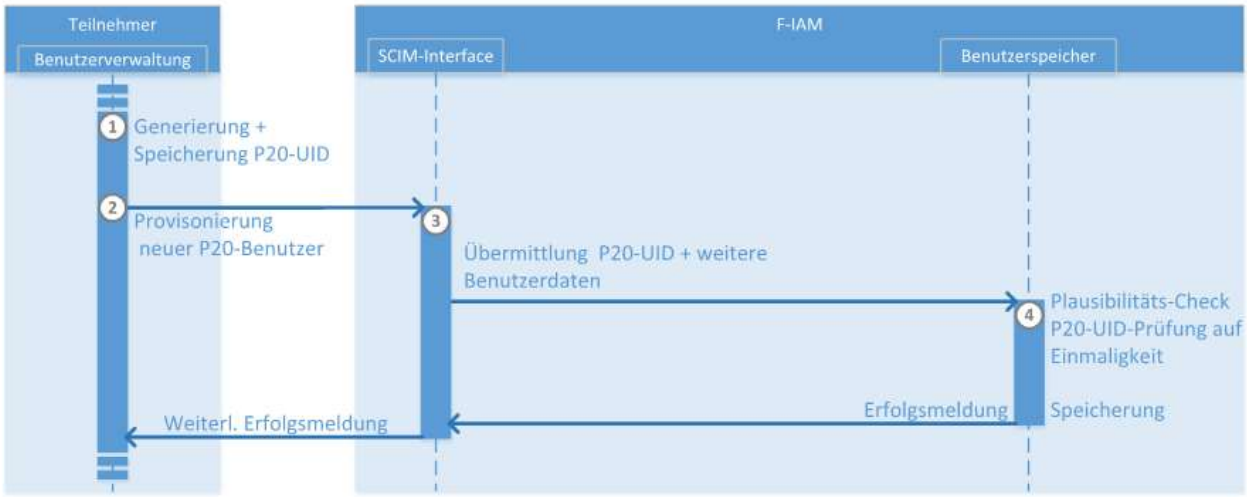

Abbildung 3 Generierung und Registrierung einer P20-UID beim Provisionieren eines neuen P20-Benutzers

1. Generierung der P20-UID in der TN-Benutzerverwaltung:
   Die TN Umgebung (bspw. IAM-System beim TN) generiert und speichert die P20-UID unter Einhaltung der vorgegebenen Regelwerke und dem festgelegten Format.
2. Provisionierungsanfrage an das F-IAM P20- SCIM-Interface
3. Die Schnittstelle des F-IAM nimmt die Anfrage der TN-Benutzerverwaltung entgegen und leitet sie an den P20-Benutzerspeicher weiter.
4. Der F-IAM Benutzerspeicher prüft auf Eindeutigkeit der übergebenen P20-UID, ihre Plausibilität und die Plausibilität der weiteren Benutzerdaten. Im Positivfall wird die P20-UID im Benutzerspeicher registriert und dauerhaft gespeichert.

Sollte die TN-Benutzerverwaltung die Rückmeldung erhalten, dass die Plausibilitäts- und Eindeutigkeitsprüfung der P20-UID fehlgeschlagen ist, ist die generierte P20-UID in der TN-Benutzerverwaltung zu entfernen. P20-UIDs werden im Benutzerspeicher des F-IAM nicht gelöscht, auch wenn die zur UID gehörige Person den Polizeidienst verlässt und das dazugehörige Benutzerkonto im TN-IAM nicht mehr existent ist. So wird ihre Einmaligkeit auch zukünftig sichergestellt. Da die P20-UIDs keine personenbezogenen oder beziehbaren Daten enthalten, ist eine datenschutzrechtliche Löschfrist nicht zu beachten. Die Prozesse zur Generierung und Registrierung der P20-UIDs werden detailliert in dem Konzept „IDM-Prozesse“ beschrieben. Dabei werden auch die Prozessverantwortlichkeiten beim Teilnehmer und en Betreibern des F-IAM genau spezifiziert.

6.Gesamtsystemarchitektur

6.1. Anforderungen an die Teilnehmer

Die P20-UID ist ein für jeden auf P20-Services zugreifenden Benutzer-Account generierter und eindeutiger Schlüssel.

Folgende Regelungen sind Voraussetzung und müssen vom TN eingehalten werden:

- Jede P20-UID darf in seiner Existenz nur einer Person (Eindeutigkeit) nur einmalig zugeordnet werden
- Die Generierung und Registrierung der P20-UID wird ausschließlich durch autorisierte Mitarbeitende der jeweiligen Behörde veranlasst.
- Eine P20-UID wird für einen Mitarbeiter nur generiert, sofern diese auf P20 relevante Dienste und Anwendungen zugreifen sollen.

Zur Generierung der P20-UIDs für Benutzerkonten müssen nachvollziehbare, revisionssichere Funktionen im TN-IAM bereitgestellt werden. Dabei kann das TN-IAM entweder auf einen zentral bereitgestellten Web-Service zurückgreifen oder aber ihre Benutzerverwaltungen erweitern, um P20-UIDs eigenständig zu erzeugen.

Die zentrale Registrierung einer P20-UID erfolgt über die erstmalige Anlage des Benutzerkontos im Benutzerspeicher des F-IAMs. Dazu müssen entsprechende Provisonierungsprozesse zwischen TN-IAM und F-IAM nach einem vorgegebenen Standard etabliert werden. Eine detaillierte Beschreibung dieser Prozesse und Standards erfolgt in einem Konzept „P20 IDM-Prozesse“ und ist nicht Bestandteil des hiesigen Dokumentes.

Zudem muss das TN-IAM dazu befähigt werden, dem Anmelde-Token (des TN-IAM beim F-IAM) die P20-UID als Attribut hinzuzufügen. Eine detaillierte Beschreibung der dar dafür bereitzustellenden Funktionen wird im Dokument „P20-IAM Vorgaben an die Teilnehmer“ beschrieben und ist ebenso nicht Bestandteil des hiesigen Dokumentes.

6.2. Anforderungen an die Anwendungen

6.2.1. Anwendungen des TN mit Schnittstelle zum Datenhaus

Eine zentrale Anforderung für die Datenverarbeitung innerhalb des Programmes Polizei 20/20 ist, das jeder Datenzugriff und jede Datenänderung auf einen authentifizierten und autorisierten Benutzer zurückzuführen ist. D. h., dass Dienste **nicht** substituierend auf Schnittstellen für die Autorisierung eingesetzt werden dürfen. Es ist gefordert, dass über die Schnittstelle die Information transportiert wird, welcher Benutzer diesen Schnittstellenaufruf initiiert hat.

Um dieser Anforderung gerecht zu werden, haben alle TN-Systeme bei jedem Aufruf einer Schnittstelle des Datenhauses die P20-UID mitzusenden. Somit kann durch die P20-UID vom jeweiligen Teilnehmer zu jeder Zeit festgestellt werden, welcher Anwender für den Zugriff bzw. für die Datenänderung verantwortlich ist. Dabei muss nicht zwangsläufig gelten, dass das TN-System in Gänze auf die P20-UIDs umgestellt wird. Es

muss aber – z.B. über das TN-IAM-System – möglich sein, mit der im TN-System verwendeten Benutzerkennung die P20-UID zu ermitteln. Diese ist in der Schnittstelle zum Datenhaus bei jedem Aufruf zu übermitteln.

6.2.2. P20-Anwendungen

Sollen Anwendungen / Dienste in ihrer Eigenschaft als Service Provider anschlussfähig sein, müssen sie die vom P20 vorgegebenen Standards zur Authentifizierung und Autorisierung unterstützen.
Eine Detaillierung findet im Rahmen der Implementierung statt und könnte z.B.

- OAuth 2.0 mit OpenID Connect (OIDC)
- Security Assertion Markup Language 2.0 (SAML 2.0)

sein.

Die P20-UID wird zur Laufzeit an die Anwendung übergeben. Die P20-UID stellt in diesem Zusammenhang ein Pflichtattribut dar. Sie wird über den Identity Provider des Teilnehmers / Partners an die Anwendung übergeben.

Die Anwendung verarbeitet diese Informationen und gewährt dem Benutzer gemäß Rollen- und Rechte-Zuordnungen sowie seiner Organisationszugehörigkeit entsprechenden Zugriff und Sichtweiten innerhalb der Anwendung. Die der Anwendung übergebene P20-UID ist dabei für alle protokollierungsrelevanten Tätigkeiten des Anwenders in den Protokolldaten zu verwenden. Ebenso muss die P20-UID verwendet werden, sofern Zugriffe und Veränderungen im Datenhaus dokumentiert werden müssen.

6.2.3. Interimsvarianten

Auch die in der Transformation befindlichen Anwendungen, die mit der Plattform kommunizieren, müssen die P20-UID verwenden, sobald sie auf die Plattform zugreifen.

Entweder sind die unter Punkt *6.2.1 Anwendungen des TN mit Schnittstelle zum Datenhaus* oder unter Punkt *6.2.2 P20-Anwendungen* dargestellten Methoden zu unterstützen. Diese müssen in der weiteren Transformationskonzeptionierung berücksichtigt werden.

7. Anhang

7.1. Glossar

Begriff / Abkürzung	Beschreibung
Authentifizierung	Prozesschritt-2: Prüfung und Bestätigung einer Identität: „das ist wirklich Paul“ 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	Prozesschritt-1: Behauptung einer Identität: „ich bin Paul“ Nachweisen einer Identität durch die Identität selbst (z.B. Vorlegen eines Personalausweises durch den Inhaber)
Autorisierung	Prozesschritt-3: Gewähren des Zugangs: „das darf Paul“ Einräumen von Rechten anhand einer bereits festgestellten (authentifizierten) Identität und Rolle (z.B. jeder authentifizierte EU-Bürger istautorisiert, in die Schweiz einzureisen)
Benutzerkonto	Ein Benutzerkonto (engl. Account) ist eine Zugangsberechtigung zu einem zugangsbeschränkten IT-System. Die Struktur eines Accounts variiert je IT-System. Mittels eines Accounts können natürliche Identitäten als auch technische Identitäten (andere IT-Systeme) auf ein IT-System zugreifen.
Benutzer-Provisionierung	Die Provisionierung steuert die Autorisierungen und Zugriffsrechte auf einzelne Programm-Ressourcen. Bei der automatisierten Provisionierung werden Benutzerkonten oder Entitäten für mehrere Anwendungen und Systeme gleichzeitig erstellt oder aktualisiert
Bereitstellungsumgebungen	Umgebungen, die für das Einspielen von Projektergebnissen, IT-Produkten und deren Updates in die Produktionsumgebumgebung im Rahmen des Releasemanagement genutzt werden. Sie stellen sicher, dass die Integrität der Produktionsumgebung bei Veränderungen geschützt und die richtigen Komponenten freigegeben werden. Ausnahme: die Schulungsumgebung ist keine Bereitstellungsumgebung
Encoding	Eine Zeichenkodierung erlaubt die eindeutige Zuordnung von Schriftzeichen (i. A. Buchstaben oder Ziffern) und Symbolen innerhalb eines Zeichensatzes.

F-IAM	Zentraler Anteil der IAM-Landschaft für Polizei20/20. Das F-IAM stellt die teilnehmerübergreifene Integration der Zugriffsteuerung für die Anwendungen im Geltungsbereich von P20 sicher.
F-IAM Benutzerspeicher	Der Basisdienst IAM sieht gemäß Transformationsgrobkonzept IAM eine Provisonierung von Benutzerdaten aus den TN-IAMs in den Benutzerspeicher des F-IAM vor. P20-Dienste und –Anwendungen können, wenn benötigt, diese vom Benutzerspeicher bedarfsgerecht beziehen.
Identity Provider	Der Begriff Identitätsanbieter (engl. Identity provider (IDP)) bezeichnet ein zentrales Zugangssystem, z.B. bei einem Teilnehmer im P20/20, für Service-Provider-Dienste (Dienstanbieter), bei dem sich die Nutzer anmelden können. Identity Provider Systeme bieten wichtige Cyber-Sicherheitsdienste fr Service Provider, wie die Authentifizierung eines Nutzers für Single-Sign-On (SSO) und die Autorisierung eines Zugriffs auf die Ressourcen der Identität über spezielle APIs. Dazu authentifiziert der Identity Provider den Nutzer und gibt diese Informationen an die Service Provider weiter. Die Kommunikation zwischen Identity Provider und Service Provider erfolgt über entsprechende Sicherheitsprotokolle, wie z. B. SAML, OpenID oder OAuth.
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).
Interimsvarianten	Bei Interimvarianten handelt es sich um ausgewählte Sachbearbeitungssysteme, die im Programm zentral zur Nutzung durch alle Teilnehmer bereitgestellt werden. Dabei handelt es sich bei um ertüchtigte Bestandssysteme, die XPolizei-NG-konform kommunizieren und die Basisdienste der Plattform nutzen. Ihre Weiterentwicklung und Transformation in das Zielbild des Pro gramms wird vom Gesamtprogramm gesteuert
LifeCycle-Management	Verwaltung des Lebenszyklus einer Identität: Dazu gehören Einrichtung, Modifikation, Suspendierung (Aussetzung) / (Re-)Aktivierung, Löschung / Archivierung.
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 20/20 zugreifen, aber nicht zu den eigentlichen Teilnehmern von Polizei 20/20 gehören.

P20-UID	User Identity (Eindeutiger Idenitifizierer einer Identität im P20/20-Umfeld)
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).
SCIM	Funktionalität/Schnittstelle zur Kommunikation mit dem IAM. Das System für das domänenübergreifende Identitätsmanagement (englisch „System for Cross-Domain Identity“) ist ein Standard zur Automatisierung des Austauschs von Benutzeridentitätsinformationen zwischen Identitätsdomänen oder IT-Systemen.
UPN	User Principle Name: Deutsch Benutzerprinzipalname. Ist ein Attribut, bei dem es sich um einen Internetkommunikationsstandard für Benutzerkonten handelt. Ein UPN besteht aus einem UPN-Präfix (dem Benutzerkontonamen) und einem UPN-Suffix (einem DNS-Domänennamen).

Tabelle 4 – Glossar

7.2. Zulässige Werte je P20-UID-Segment

Zulässige Werte 1.Segement (Kategorie Partner / Teilnehmer	
Wert	Beschreibung
P	Partner
T	Teilnehmer

Tabelle 5 Segment 1 „Kategorie Partner“ / Teilnehmer – derzeit zulässige Werte

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

Tabelle 6 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 7 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 8 Segment 4 „Partner- bzw. TeilnehmerID“– derzeit zulässige Werte

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

7.3. Offene Punkte

Nr.	Beschreibung	Vorgehen zur Klärung
	Technische Konzeptionierung zur Umsetzung beim TN und der zentralen IAM-Plattform	Eine technische Konzeptionierung beim TN kann erst mit der technischen Konzeptionierung des zentralen Services auf der zentralen IAM-Plattform erfolgen. Diese wiederum setzt im Rahmen des Arbeitspaketes „Technische Betrachtung der Anbindungmöglichkeiten der TN“ auf den Anbindungsmöglichkeiten der TN auf.
	Generierung und Registrierung von P20-UIDs von Partner-Identitäten	Das Themenfeld kann nur in Kooperation mit entsprechenden Partnern „designed“ werden
	Prozessbeschreibungen zu Veränderungen in der P20-IAM Codelisten, die die zulässigen Wertemengen je Segment beschreiben	Hier müssen Betrieb des P20 IAM und entsprechende Verantwortlichkeiten im weiteren Verlauf des Projektes konzipiert werden.

Tabelle 9 – Offene Punkte