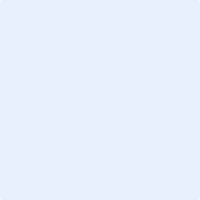
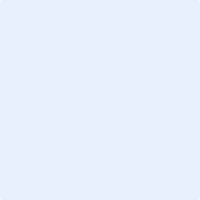
* 

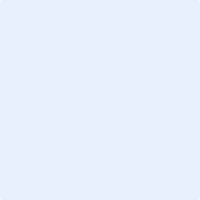
LDAP-Legacy+

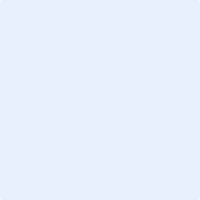
Version 0.1| Stand 14.12.2023

V









|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Dokumenteninformation** | | | | | | | | |
| **Programm** | | | Polizei 20/20 | | | | | |
| **Programmleiter** | | | Holger Gadorosi | | | | | |
| **Projektleiter/Verantwortlicher** | | | Norbert Linde | | | | | |
| **Dokumententitel** | | | Identity Management Fachkonzept | | | | | |
| **Version** | | | 0.1 | | | | | |
| **Erstellt am**  **Erstellt von** | | | 14.12.2023  PG IAM | | | | | |
| **Zuletzt bearbeitet am**  **Zuletzt bearbeitet von** | | | 14.12.2023  PG IAM | | | | | |
| **Status** | | | In Bearbeitung | | | | | |
| **Vorprüfung des Dokumentes** | | | | | | | | |
| **Fachliche Prüfung** (Fachlichkeit) | | | | | | Vorgelegt <> | Freigegeben <> | |
| **Technische Prüfung** (Technik) | | | | | | Vorgelegt <> | Freigegeben <> | |
| **Methodische Prüfung** (PMO) | | | | | | 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 durch** (Gremiensitzung, TOP Nr.): | | | | | | | | |
| **Versionshistorie** | | | | | | | | |
| **Version** | **Datum** | **Erstellt durch** | | **Inhaltliche Kurzbeschreibung der Neuerungen** | | | | |
| 0.1 | 14.12.2023 | PG IAM | | Neu erstellt | | | | |
|  |  |  | |  | | | | |
| **Referenzierte Dokumente** | | | | | | | | |
| **Referenzdokument** | | | | **Version** | **Autor** | | | **Datum** |
| Transformation IAM - Grobkonzept | | | | V2.0 | PG IAM | | | 24.11.2022 |

Inhaltsverzeichnis

[Abbildungsverzeichnis 4](#__RefHeading___Toc3548_874349787)

[1. Einleitung 5](#__RefHeading___Toc3550_874349787)

Abbildungsverzeichnis

# Einleitung

Für die Steuerung des Zugriffs auf innerhalb und außerhalb des Programms Polizei 20/20 zur Verfügung gestellten Ressourcen (Anwendungen, Daten) wird auf Seiten bestimmter Teilnehmer eine Verzeichnisdienst bereitgestellt, der dieDaten für diese Steuerung bereitstellt.

Die Struktur und Ausprägung diese Verzeichnisdienstes stellt eine Vereinfachung des im Transformationskonzept als LDAP-Generic definierten Verzeichnisdienstes dar. Im Unterschied zu einer als LDAP Generic definierten Ausprägung wird in der Ausprägung als LDAP-Legacy+ auf die Steuerung von Funktionsrechten, Rollen und Intermediates verzichtet. Die Verwaltung derartiger Berechtigungsobjekte im Kontext eines Benutzerkontos obliegt der jeweiligen betroffenen Anwendung.

# Schnittstellendefinitionen

Dieses Kapitel befasst sich mit der konkreten Beschreibung der angebotenen Schnittstellen. Der Fokus liegt hierbei vor allem auf der Beschreibung von Schnittstellen für die Umsetzung von IDM-Prozessen.

## LDAP-Schnittstelle für Teilnehmer

Dieses Kapitel konkretisiert die Informationen zur Verwendung der Schnittstelle „LDAP“ für Teilnehmer ausgehend von der TN-BV/IAM zum Basisdienst IAM.

### Struktur des LDAP-Servers

* ou=P20-Benutzer  
    
  Der Bereich der LDAP-Struktur, in dem Benutzerkonten angelegt werden, die vom Basisdienst IAM für den Zugriff auf P20-Anwendungen berechtigt werden sollen.
* ou=P20-Anwendungen  
    
  Der Bereich der LDAP-Struktur, in dem für jede vom TN genutzte P20-Anwendung ein eigener Bereich in der Struktur erstellt wird (hier: ou=AW1, ou=AW2, ou=AW3).
* ou=[Anwendungsname]  
    
  Innerhalb des Bereichs „P20-Anwendungen“ wird für jede vom TN genutzte P20-Anwendung ein eigener Bereich in der Struktur erstellt. In diesem Beispiel stehen AW1, AW2, AW3 für je eine Anwendung. Zur besseren Lesbarkeit werden Anwendungsnamen in der Umsetzung möglichst sprechend gewählt (z.B. iVBS, Jira, usw.). Eine Liste von gültigen Anwendungsnamen wird durch die PG IAM bis Mitte 2023 veröffentlicht und mit jeder Anbindung weiterer P20-Anwendungen/-Dienste fortgeschrieben.
* cn=Zugriff  
    
  Eine Gruppe, die sich in der generischen LDAP-Struktur für jede Anwendung befindet. Eine Gruppenmitgliedschaft („DN“ des Benutzerkontos aus ou=P20-Benutzer ist „member“ in „cn=Zugriff“) führt dazu, dass der Basisdienst IAM ein Benutzerkonto in der assoziierten Anwendung provisioniert. Das Entfernen der Gruppenmitgliedschaft von einem Benutzerkonto führt zu einer Deprovisionierung des Benutzers aus der assoziierten Anwendung.