GEMEINSAM. DIGITAL. VERNETZT.
P20 POLIZEI 20/20

IT-Kooperation

Lastenheft zur BV-Anbindung an ein P20-TN-LDAP

Version 00.02.02

Projekt-/ Produktbe-zeichnung	SNIT ITK-BV-TN-LDAP	
Projektleiter	*C. Pahl*	
Verantwortlich	*S.Tumovec*	
Erstellt am	21.12.2022	
Zuletzt geändert	7. Mai 2024 13:26	
Bearbeitungszustand		in Bearbeitung
	x	Vorgelegt
		fertig gestellt
Dokumentablage	[ANF-1031] Anbindung BV an ein P20-LDAP	

Änderungshistorie:

Nr.	Version	Datum	Autor	Änderung	Zustand
01	00.00.01	21.12.2022	T. Hohmann	Entwurf	erledigt
02	00.00.02	22.12.2022	S. Tumovec	AF.BV.P20-AW.00 „Übertragung eines P20-Benutzers mit Nutzerinfomationen in TN-P20-LDAP“	erledigt
03	00.00.03-04	30.12.2022	S. Tumovec	Umstrukturierung, Normierung und Überarbeitung aller AF	erledigt
04	00.00.05	13.01.2023	S. Tumovec	Prüfung vor Weitergabe an ITK	erledigt
05	00.00.06	13.02.2023	T. Hohmann	Überarbeitung und Weitergabe an ITK	erledigt
06	00.00.06	06.04.2023	U. Dallmann N. Nissen	Kommentierung	erledigt
07	00.01.01	07.03.2023	S. Tumovec	Formale Dokumentanpassungen – u.a. Kopfzeile	erledigt
08	00.01.02	21.-28. 04.2023	S. Tumovec	Neustrukturierung und Einarbeitung der Hinweise aus Nr. 06	erledigt
09	00.01.03	02.05.2023	T. Hohmann	Überarbeitung und Weitergabe an ITK	erledigt
10	00.01.04	22.06.2023	S. Tumovec	Einarbeitung der Kommentierung von U. Dallmann zu 00.01.03 - Anzahl verpflichtender Attribute in AF.BV.P20-AW.00 reduziert - Anpassung der CSV-Datei zur Festlegung der Rollenverschachtelungen in Anlage 5 incl. Beschreibung der Spalten - Neu-Erstellung AF.BV.Admin-Tool.00 „Löschen aller Benutzerberechtigungen im TN-P20-LDAP“ - Konkretisierung der Übergabe von „Dienstgrad“ bzw. Amtsbezeichnung in LDAP-Personenobjekten	erledigt
11	00.01.05	10.11.2023	S.Tumovec	Korrektur der Darstellung einer MemberOf-Beziehung in der Darstellung der generischen LDAP-Hierarchie im Abschnitt 1.4 (S. 8)	erledigt
12	00.02.01	23.04.2024	S. Tumovec	Komplexitätsreduzierung der FIAM-Transformation von TN-P20-LDAP zur Anwendungsseite (PLX) erfordert Anpassungen 1. Anpassung der Darstellung der Generic-LDAP-Struktur für die TN-Seite 2. Einfügen einer Beispiel-Datenbestückung entsprechend der Strukturanpassung unter Pkt.1 3. Einarbeitung der geänderten Strukturen in die betroffenen Anwendungsfälle	zur Aufwandschätzung vorgelegt

				4. Umbau/Umorientierung der technischen Abbildung der Beziehung zwischen Rollen und Funktionsrechten (neu: Rolle ist member in Funktionsrechten) 5. Auswertung der Spalte „Objekttyp“ der csv-Datei zum Laden von Rollen und Rechten einer P20-Anwendung. → Mitführung des Typs in den BV-Rollen/Rechten	
13	00.02.02	30.04.2024	S. Tumovec	Korrektur der Beispiel-CSV-Datei in Bezug auf den Objekttyp „Marker“. Versehentlich war dort vorher „Vertretung“ dargestellt.	zur Aufwandschätzung vorgelegt

Prüfungen:

Datum	Geprüfte Version	Prüfer	Anmerkung	Neuer Produktzustand

Inhalt

Tabellen

1 Einleitung

Im Rahmen der geplanten Anbindung der iVBS-Systeme an den Basisdienst P20-F-IAM wird die Berechtigungssystematik der PLX-basierten Systeme ebenso angepasst werden, wie auch die der beiden anderen iVBS-Alternativen, @rtus und IGVP-FE. Das Zielbild dieser Anpassungen hinsichtlich Autorisierung und Authentifizierung wird gegenwärtig durch die P20-PG-IAM projektiert. Zentraler Benutzer- und Berechtigungsspeicher wird dann die Komponente F-IAM (Föderatives Identitäts- und Berechtigungsmanagement) sein. Die teilnehmereigenen Benutzerverwaltungen und Verzeichnisdienste dienen ab dann nur noch dem lokalen Erfassen, Zwischenspeichern und Weiterleiten der Benutzer- und Berechtigungsinformationen an die zentrale P20-Komponente F-IAM.

Dazu sind seitens der jetzigen ITK-BV Anpassungen erforderlich, die ein Schreiben von Benutzer- und Berechtigungsinformationen auf einem gemeinsamen Übergabe-/Übernahmepunkt, in einem separaten Benutzer- und Berechtigungsverzeichnis, welches nicht das AD ist, ermöglichen. Im Dokument wird dieser Übergabepunkt als TN-P20-LDAP-Verzeichnis bezeichnet.

Im bestätigten Konzept „Transformation IAM Grobkonzept v1.2“ ist diese normierte Sicht auf einheitliche und vom Ziel-iVBS unabhängige verzeichnisbasierte Übergabestrukturen festgehalten und Grundlage der in diesem Dokument zusammengestellten Anwendungsfälle für die Beschreibung der Funktionalität der zu erstellenden Schnittstelle „SNIT ITK-BV-TN-LDAP“.

1.1 Authentifizierung

Die Mechanismen der Authentifizierung sind nicht Gegenstand des Schnittstellenumfangs, wenngleich die Erzeugung der P20-UID in der ITK-BV und die nachfolgende Provisionierung über die „SNIT ITK-BV-TN-LDAP“ in das TN-P20-LDAP-Verzeichnis eine grundlegende Voraussetzung einer späteren Authentifizierung des Nutzers auf dem iVBS-Client gegenüber dem entfernten iVBS-Backend ist.

1.2 Autorisierung

Die nachfolgend dargestellte interne Strukturierung und die Bestückung des TN-P20-LDAP-Verzeichnis stellt den ersten von mehreren Schritten der Provisionierung von Autorisierungsinformationen des TN in Richtung iVBS-Backend beim zentralen Dienstleister (Dataport, andere) dar. Die Ausleitung (Anlage, Änderung, Löschen) von Berechtigungstripeln (Benutzer, Rolle, Dienststelle) aus der ITK-BV der TN in das TN-P20-LDAP-Verzeichnis ist Gegenstand der in den folgenden Abschnitten angeführten Anwendungsfälle.

1.3 Definition von Begrifflichkeiten

Die Unterscheidung zwischen Rollen und Rechten ist im allgemeinen Sprachgebrauch häufig nicht klar genug abgegrenzt. Aus Sicht der Zielsysteme liefert die BV manchmal eher eine (allgemeine) Rolle und ein anderes Mal ein (spezifisches) Recht.

Entscheidend ist, dass die BV heute nur eine Ebene besitzt.

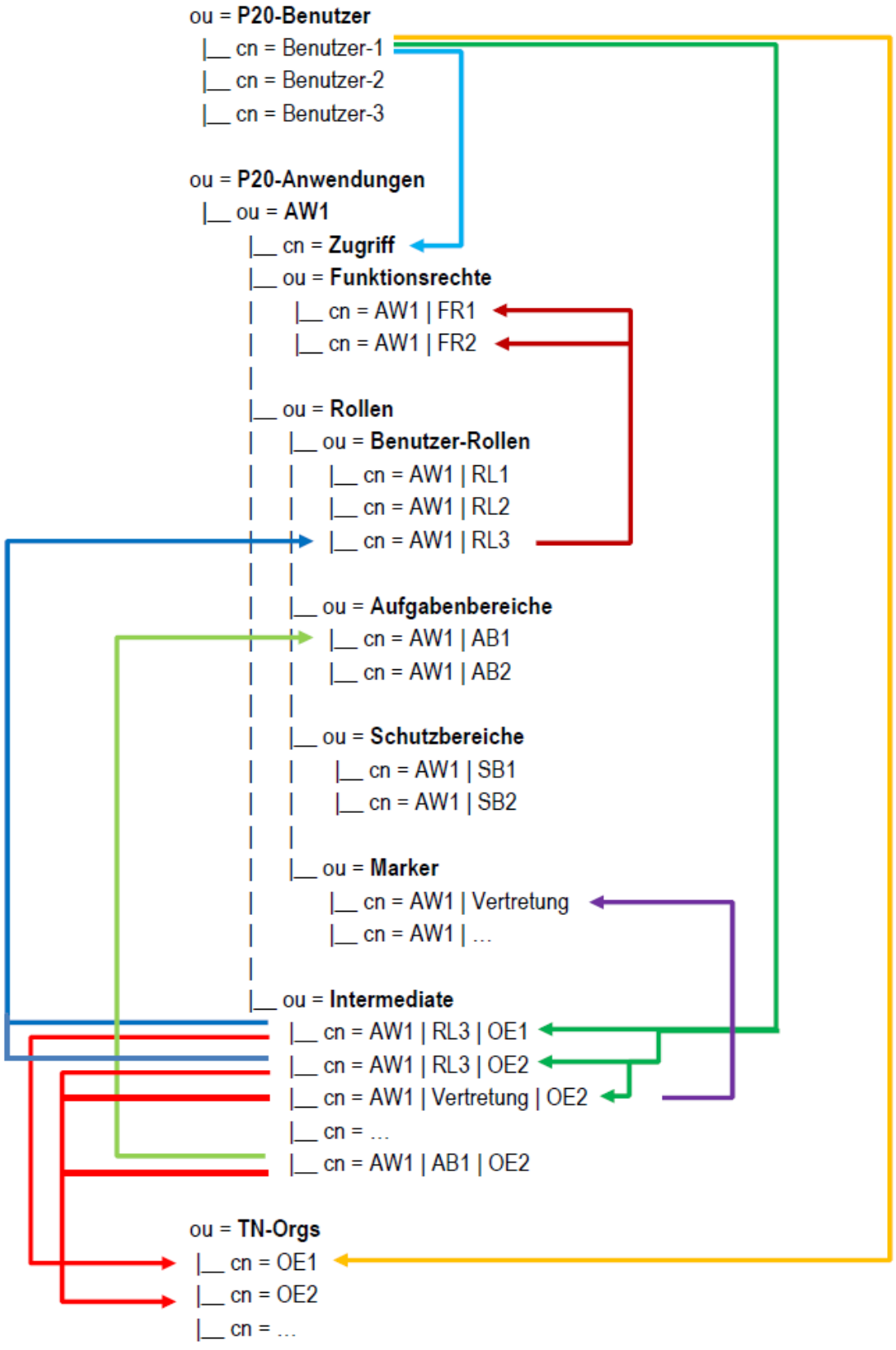
Überwiegend entspricht dies eher einer Rolle, weil die resultierenden spezifischen Anwendungsrechte oftmals deutlich mehr sind. Eine Rolle kann bspw. diverse Anwendungsrechte beinhalten, die untereinander in komplexen Beziehungen stehen bzw. Abhängigkeiten untereinander besitzen können.

Wird einem Anwender in der BV ein Recht vergeben oder entzogen, dann wirkt sich dies nur auf die Mitgliedschaften der im folgenden beschriebenen Rollen-Gruppen aus. So ist es auch in den nachfolgenden Anwendungsfällen beschrieben. Ein BV-Recht ist demnach am ehesten mit einer Rolle vergleichbar.

Die Zuordnung von Rollen zu Funktionsrechten (=> „Rollenzuschnitt“) ist spezifisch für die jeweilige Anwendung und wird durch die normalen Anwendungsfälle der BV nicht verändert. Diese werden nur in den Anwendungsfällen eines Neu-Aufbaus beschrieben. Dort kommen entsprechende Informationen z.B. aus einer csv-Datei, aber nicht aus der BV selbst. Im Rahmen zukünftiger Erweiterungen mag sich das ändern, aber für den hier beschriebenen ersten Schritt, hat die BV selbst darüber keine Informationen.

Begriff	**Bedeutung**
Rolle	Eine Rolle (in einem Zielsystem) besteht aus mind. 1 Recht oder Funktionsrecht (im Sinne des Zielsystems) Es ist jedoch auch möglich, dass eine Rolle gar kein Funktionsrecht beinhaltet. Bspw. leitet PLX in diesem Fall eine anwendungsspezifische Eigenschaft des Nutzers ab. So werden dort z.B. sogenannte „Aufgabenbereiche“ und „Schutzbereiche“ und „Marker“ über Rollenvergabe dem Benutzer zugeordnet.
Recht/Funktionsrecht	Ein Basis-Recht (z.B. Leseberechtigung, Schreibberechtigung) in einem Zielsystem
BV-Recht	In der BV können Berechtigungen für Zielsysteme vergeben werden. Diese Berechtigung kann im Zielsystem eine Rolle oder ein Recht sein.
BV-Rechtegruppe	In der BV können zur Übersichtlichkeit (oder für bestimmte Regeln wie gegenseitigem Ausschluss von Berechtigungen) Rechtegruppen vergeben werden. Eine Rechtegruppe kann (aber muss nicht) identisch zu einem Zielsystem sein. Mehrere BV-Rechtegruppen können einer P20-Anwendung zugeordnet werden. Jede BV-Rechtegruppe ist genau einer oder keiner P20-Anwendung zugeordnet.

1.4 Strukturierung des TN-P20-LDAP-Verzeichnis



Legende / Erklärung:

„Benutzer-1“ ist berechtigt, auf Anwendung „AW1“ zuzugreifen (hellblau)

„Benutzer-1“ ist der TN-Organisation „OE1“ zugehörig (gelb)

„Benutzer-1“ hat folgende Dienststellen-bezogenen Berechtigungen zugewiesen bekommen (dunkelgrün)
- „AW1 | RL3 | OE1“ (auf Dienststelle OE1 eingeschränkt)
- „AW1 | RL3 | OE2“ (auf Dienststelle OE2 eingeschränkt)
- „AW1 | Vertretung | OE2“ (auf Dienststelle OE2 eingeschränkt, was hier konkret bedeutet, dass er dieser Dienststelle vertretungsweise zugeordnet ist)

Die Intermediate-Objekte „AW1 | RL3 | OE1“ und „AW1 | RL3 | OE2“ beziehen sich auf die Benutzer-Rolle „AW1 | RL3“ (dunkelblau)

Das Intermediate-Objekt „AW1 | AB1 | OE2“ bezieht sich auf den Aufgabenbereich „AW1 | AB1“ (hellgrün)

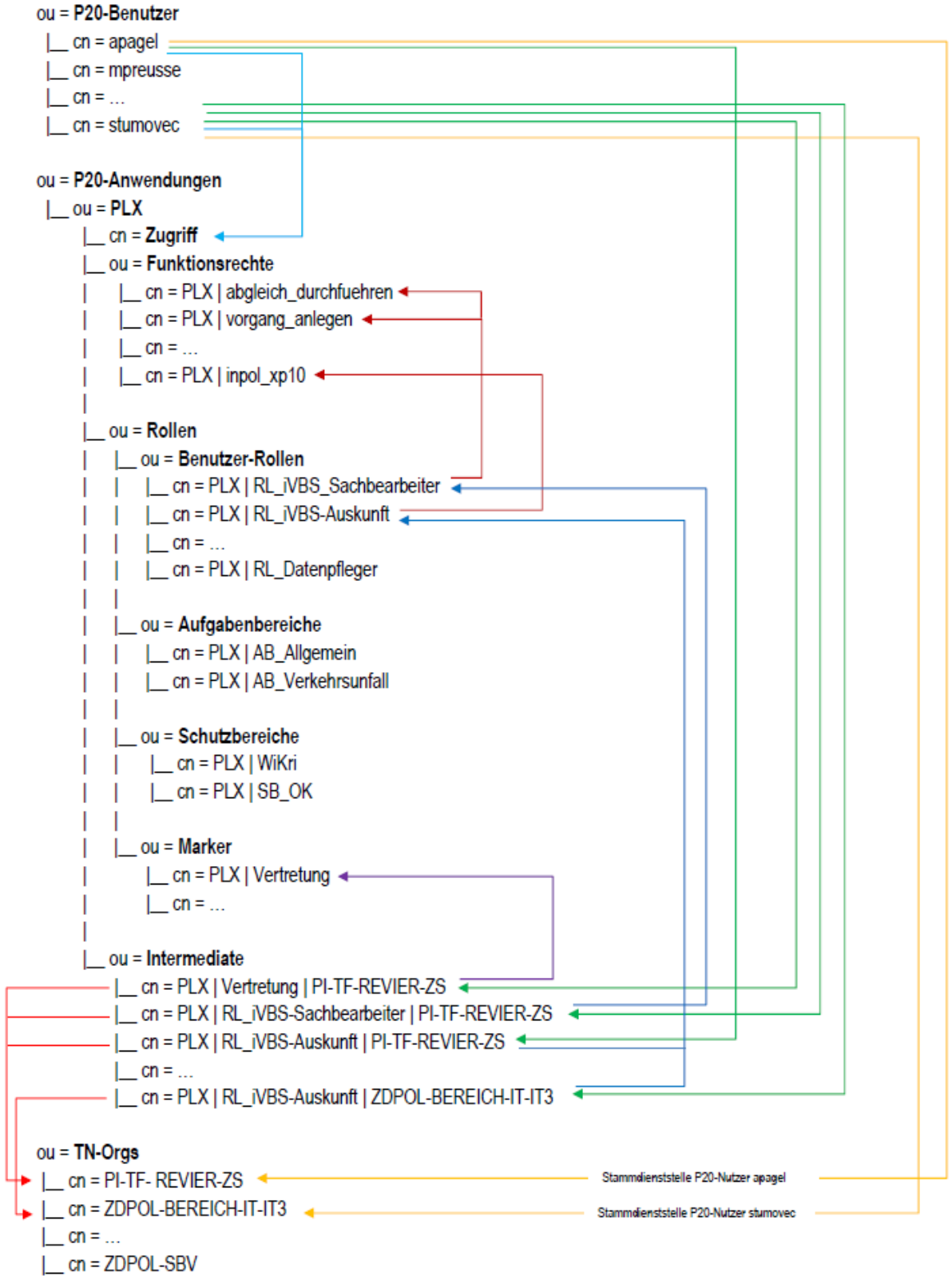
Das Intermediate-Objekt „AW1 | Vertretung | OE2“ bezieht sich auf den Marker „AW1 | Vertretung“ (violett)

Die Rolle „AW1 | RL3“ enthält die Funktionsrechte „AW1 | FR1“ und „AW1| FR2“ (dunkelrot)

Das Intermediate-Objekt „AW1 | RL3 | OE1“ bezieht sich auf OE1 (hellrot)

Die Intermediate-Objekte „AW1 | RL3 | OE2“, „AW1 | Vertretung | OE2“ und „AW1 | AB1 | OE2“ beziehen sich auf OE2 (hellrot)

Beispielbestückung TN-P20-LDAP (BB) nach Konsolidierungs WS-Reihe in KW 15-17 (22.04.2024)



Hinweis zum Trennsymbol „|“:

Das bei der TN-spezifischen Namensbildung der Objekte in der Darstellung verwendete Trennsymbol „-“, z.B. bei „AW1-R3-OE1“ ist eine Möglichkeit zur Visualisierung und Abgrenzung der Namensbestandteile. Dieses Trennsymbol ist aus Sicht des Verzeichnisdienstes jedoch nicht vorgegeben und daher frei wählbar - es kann sogar ganz weggelassen werden.

Aus Sicht der Nutzung der SNIT ITK-BV-TN-LDAP, insbesondere aus der Sicht potentieller manueller Problemanalysen, wäre es vorteilhaft ein Trennsymbol zu verwenden, welches nicht Bestandteil der jeweiligen namensbildenden Komponenten selbst ist. So ist bspw. das Symbol „-“ bereits massiv Bestandteil in der Bildung der durch die Kooperationsländer in der BV verwendeten Leitzeichen (z.B. ZDPOL-BEREICH-IT-IT3). Das würde die Lesbarkeit im Rahmen einer Problemanalyse sehr erschweren.

Als Alternative könnte hier ein „|“ anstelle des „-“ verwendet werden. Alle Zeichen in der nachfolgenden Tabelle sollten jedoch nicht verwendet werden, da sie in der Namensbildung mit einem „\“ quotiert werden müssen.

comma	,
Backslash character	\
Pound sign (hash sign)	#
Plus sign	+
Less than symbol	<
Greater than symbol	>
Semicolon	;
Double quote (quotation mark)	"
Equal sign	=
Leading or trailing spaces	

Hinweis zur Längenbegrenzung von Namen in LDAP-Verzeichnissen:

Für die Bezeichnung von LDAP-Objekten (cn und ou) existieren Längenbeschränkungen von jeweils max. 64 Zeichen. Diese Begrenzung muss bei der automatisierten Zusammensetzung kombinierter Bezeichnungen aus Anwendungsname, Rolle und Organisationseinheit besonders bei den Intermediate-Objekt-Bezeichnern beachtet werden und folgender Restriktion entsprechen:
Länge (Bezeichner P20-Rechtegruppe) + 1 +
Länge (Bezeichner BV-Recht) + 1 +
Länge (Leitzeichen) **<= 64**

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.

Als identifizierendes Merkmal wird die eindeutige Benutzerkennung aus der TN-Domäne genutzt. Diese entspricht ebenfalls der eindeutigen Benutzerkennung in der ITK-BV.

Bildungsvorschrift: <***Benutzername/Benutzerkennung***>
Bsp: **Benutzer-1**

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.

Die Liste der Anwendungsnamen im TN-P20-LDAP-Verzeichnis wird durch den Betrieb eingerichtet und nicht durch die SNIT ITK-BV-TN-LDAP geschrieben. Ein Anwendungsname im TN-P20-LDAP-Verzeichnis muss dann in der BV einer BV-Rechtegruppe entsprechen.

Bildungsvorschrift: <***Anwendungsname***>
Bsp: **AW1**

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.

ou=Funktionsrechte

Dieser Bereich wird für die Berechtigungsverwaltung benötigt. Hier muss durch jeden TN eine Gruppe je Funktionsrecht der assoziierten Anwendung erstellt werden. Dies kann, wenn gewünscht, manuell basierend auf dem Berechtigungskonzept der Anwendung geschehen oder innerhalb der TN-BV/IAM automatisiert werden. Eine stets aktuelle Liste von Anwendungen und den jeweiligen Funktionsrechten soll zukünftig über einen API-Request vom Zentralen Rollenkonfigurator (ZeRo) abgerufen werden können.
Eine Relevanz für die Anpassungen im BV-Kern besteht hier nicht, da die Funktionsrechte nicht durch den BV-Kern verwaltet werden.

Bildungsvorschrift: <***Anwendungsname***>|<***Funktionsrecht***>
Bsp: AW1 | FR1

ou=Rollen

Im Unterschied zur bisherigen (ANF-1031 Lastenheft_BV_LDAP_PLX_00.**01.05**) „flachen“ Auflistung der Rollen unterhalb der ou=Rollen ist eine typisierte Abbildung von Rollen notwendig, die sich unmittelbar auf die Strukturierung der Teil-Hierarchie im LDAP-Verzeichnis ab ou=Rollen auswirkt.

ou = **Rollen**
|__ ou = **Benutzer-Rollen**
| |__ cn = AW1 | RL1
|
|__ ou = **Aufgabenbereiche**
| |__ cn = AW1 | AB1
|
|__ ou = **Schutzbereiche**
| |__ cn = AW1 | SB1
|
|__ ou = **Marker**
| |__ cn = AW1 | Vertretung
|

ou=Benutzer-Rollen

In diesem Bereich der für jede Anwendung generischen LDAP-Struktur wird es den TN ermöglicht eigenständig, ohne Konsultation des Basisdienstes IAM oder der assoziierten Anwendung, neue Rollendefinitionen zu hinterlegen. Durch das Erstellen einer neuen Gruppe innerhalb dieses Bereichs wird eine neue Rolle geschaffen. Durch das Zuweisen dieser neuen Gruppe als „member“ in einer vorhandenen Gruppe in ou=Funktionsrechte erhält die neue Rolle das mit dieser Gruppe assoziierte Funktionsrecht. Wird nun ein Benutzerkonto Mitglied („member“) in der neu erstellten Gruppe/Rolle, erhält er automatisch das verlinkte Funktionsrecht in der Anwendung.
Die Zuordnung von Funktionsrechten zu Rollen wird nicht im BV-Kern gepflegt. Jedoch beschreibt die AF.BV.ADMIN-TOOL.04 die gewünschte Funktionalität, mit der in einem BV-Admin-Tool diese initiale Anlage, geliefert in einer CSV-Datei, vorgenommen werden kann.
Die in der BV gespeicherte „Bezeichnung“ eines Rechtes wird bei der Namensbildung des Objektes im LDAP-Verzeichnis als <Rolle> (s. u.) verwendet.

Bildungsvorschrift: <***Anwendungsname***>|<***Benutzer-Rolle***>
Bsp: AW1 | RL1

ou=Aufgabenbereiche
ou=Schutzbereiche

Aufgabenbereiche und Schutzbereiche sind aus Sicht der BV ebenfalls Rollen/Rechte, die innerhalb einer Dienststelle an Mitarbeiter dieser Dienststelle oder an Mitarbeiter einer anderen Dienststelle als Fremdberechtigung vergeben werden können.

„Aufgabenbereiche“, „Schutzbereiche“ und „Marker“ werden im Unterschied zu Benutzer-Rollen keinen Funktionsberechtigungen zugeordnet.

Der in *5.4 Anlage 5 CSV-Datei zur Definition der Rollen-Funktionsrechte-Verschachtelung* in der csv-Datei die mitgelieferte Spalte **Objekttyp** muss nun durch das BV-Admin-Tool beim Einlesen interpretiert werden. Bislang diente sie nur als Hilfsspalte zur Verwaltung der Erstellung und Änderung der csv-Datei durch den Administrator.

Dieser Objekttyp muss nun als typisierendes Merkmal an der Rolle in der BV vermerkt werden und dient beim Export über die SNIT-LDAP zur Unterscheidung der jeweiligen Ablage im LDAP-Verzeichnis.

Folgende Bezeichner für Objekttypen in der csv-Datei sind zulässig:

1. „Funktionsberechtigungen“ → Rollentyp: „Benutzer-Rolle“
2. „Aufgabenbereich“ → Rollentyp: „Aufgabenbereich“
3. „Schutzbereich“ → Rollentyp: „Schutzbereich“
4. „Vertretung“ → Rollentyp: „Vertretung“

ou=Marker

Marker beinhaltet „Markierungen“, die Intermediate-Objekte besonderer Bedeutung markieren. Ein aktuell benötigter Marker ist „cn=AW1 | Vertretung“. Die Anlage dieses Markers erfolgt analog der Anlage von Aufgaben- und Schutzbereichen entsprechend der Auswertung des Objekttyps beim Einlesen eines Datensatzes aus der csv-Datei.

Die Herstellung einer Beziehung zwischen einem Intermediate-Objekt-Objekt, welches in einer speziellen BV-Rolle eine Vertretungs-Berechtigung in einer Fremddienststelle markiert, erfolgt durch „cn=AW1 | Vertretung | OE1 → ou=Marker cn= AW1 | Vertretung“.
Darüber lassen sich dann für die Anwendung u.a. leicht alle Vertreter innerhalb einer Dienststelle bestimmen. Ebenso einfach können zu einem Mitarbeiter alle zulässigen Vertretungsdienststellen bestimmt werden (zum Login-Zeitpunkt eines Benutzers in die Anwendung)

<u>Anmerkung zur Nutzung des ZeRo (Zentraler Rollenkonfigurator):</u>

Seitens PG-IAM wird ZeRo ein Plus-Feature (spätere Ausbaustufe) bereitgestellt werden, mit dessen Hilfe der Rollenzuschnitt (Zuordnung von Funktionsrechten zu Rollen) erfolgen kann. Dieses steht jedoch erst mittelfristig zur Verfügung, so dass die BV unabhängig von ZeRo agieren muss. Zudem wäre es auch positiv, wenn durch diese Unabhängigkeit auch in andere Landesanwendungen, die keine unmittelbare P20-Relevaz haben, Berechtigungsdaten erzeugt und provisioniert werden könnten.

ou=Intermediate

In diesem Bereich der für jede Anwendung generischen LDAP-Struktur können Rollen (aus ou=Rollen) auf bestimmte Organisationseinheiten eingeschränkt werden. Dieser Bereich wird also benötigt für sog. „OE-bezogene Berechtigungen“. Basierend auf den aktuell vorliegenden Anforderungen an den Basisdienst IAM können Rollen ausschließlich durch OE-Bezug eingeschränkt werden.

Nicht jede Anwendung erfordert es, OE-bezogene Berechtigungen zu verwenden. Typisch ist dieses Berechtigungsmodell allerdings für die Vorgangsbearbeitungs-Systeme der Polizei und folglich auch für die zentral bereitgestellten iVBS. Hieraus ergibt sich kein gesonderter Anpassungsbedarf des BV-Kerns. Zielsysteme, die diesen OE-Bezug nicht benötigen, müssen ihn ignorieren bzw. damit umgehen können.

Um eine vorhandene Rolle auf eine Organisationseinheit einzuschränken, muss eine neue Gruppe in ou=Intermediate erstellt werden (z.B. Rolle1|Dienststelle1). Diese neue Gruppe muss nun „member“ sein in einer Gruppe aus ou=TN-Orgs, welche wiederum mit einer beliebigen Organisationseinheit des TN assoziiert wird. Zusätzlich muss die neue Gruppe aus ou=Intermediate „member“ sein in der Gruppe aus ou=Rollen, welche mit der einzuschränkenden Rolle assoziiert wird.

Die nun geschaffene Verschachtelung erlaubt es ein „Berechtigungstripel“ bestehend aus Benutzer, Berechtigung und OE-Bezug in einem Verzeichnisdienst abzubilden.

Die Strukturierung sollte auch hier durch die Einhaltung einer strikten Namenskonvention unterstützt werden:

Bildungsvorschrift: <***Anwendungsname***>|<***Rolle***>|<***Organisationseinheit***>
Bsp: **AW1 | RL1 | OE1**

ou=TN-Orgs

In diesem Bereich der generischen LDAP-Struktur können durch den TN Gruppen erstellt werden, die wiederum mit Organisationseinheiten (OEs) des TN assoziiert werden. Diese Gruppen dienen der Einschränkung von Berechtigungen auf OEs sowie der Zuordnung von Benutzern zu sogenannten „Stammdienststellen“.

Dabei werden jedoch nur Attribute in einer flachen Objektstruktur übertragen, d.h. es ist möglich über den Basisdienst IAM Informationen wie einen Namen für OEs zu übermitteln. Basierend auf den der PG IAM vorliegenden Anforderungen wird die Objektstruktur, also die Hierarchie der OEs zueinander, vom Basisdienst IAM weder berücksichtigt noch transportiert (siehe auch Anmerkung unten).

Organisationseinheiten werden „bei Bedarf“ durch die SNIT ITK-BV-TN-LDAP angelegt, sobald eine Berechtigungsprovisionierung resp. Zuordnung einer Stammdienststelle für einen Benutzer mit Bezug auf diese OE erfolgt.

Das in der BV gespeicherte „Leitzeichen“ einer Dienststelle wird bei der Namensbildung des Objektes im LDAP-Verzeichnis als <Organisationseinheit> (s. u.) verwendet.

Bildungsvorschrift: ***<Organisationseinheit>***
Bsp.: **OE1**

Anmerkung zur nicht übertragenen Dienststellenhierarchie:

Der vollständige Hierarchiebaum der Dienststellenstruktur muss in der Fachanwendung gehalten werden. Dort liegen dann auch weitere Fachanwendungs-spezifische Dienststellen-Attribute. Dass die Dst-Hierarchie in der BV identisch mit der im PLX-BackEnd ist, dafür muss die jeweilige Fachadministration sorgen.

2 Anwendungsfälle SNIT_ITK-BV-TN-LDAP

Folgend werden die im System BV zusätzlich erforderlichen Funktionalitäten beschrieben, um eine Provisionierung der Benutzer-Dienststellen-Berechtigungs-Informationen für P20-Anwendungen in das TN-P20-LDAP-Verzeichnis zu gewährleisten.

Das in den nachfolgenden Abschnitten in Fehlerfällen referenzierte „Schnittstellen-Logbuch“ sollte im Ermessen der Entwickler hinsichtlich seiner Struktur, Ablage, … etc. diskutiert, festgelegt und als weitere Anlage diesem Dokument beigefügt werden.

2.1 AF.BV.P20-AW.00 „Übertragung eines P20-Benutzers mit Nutzerinformationen in TN-P20-LDAP“

P20-Benutzer und Nutzerinformationen müssen im Fall einer P20-Anwendungsberechtigung in das TN-P20-LDAP-Verzeichnis übertragen werden. Hierbei sind folgende BV-Benutzer-Attribute zu übertragen:

- Benutzerkennung
- Nachname
- Vorname
- E-Mail
- Dienstgrad
- TelefonNr
- OE-Zugehörigkeit
- UPN
- P20-UID

BV Attribut	LDAP(S)	Beispiel	Hinweise
	objectClass → user		fest vorgegeben
Benutzerkennung	cn (2.5.4.3)	stumovec	**verpflichtend (1)** Benutzerkennung - darf sich nie ändern
E-Mail	mail (0.9.2342.19200300 .100.1.3)	Sievert.Tumovec@polizei.brandenburg.de	**verpflichtend (2)**
Dienstgrad	title (2.5.4.12)	RAng	Dienstgrad resp. Amtsbezeichnung
Vorname	givenName (2.5.4.42)	Sievert	**verpflichtend (3)**
Nachname	sn (2.5.4.4)	Tumovec	**verpflichtend (4)**
TelefonNr	telephoneNumber (2.5.4.20)	033702-91-218	optional
Leitzeichen *(der OE)*	division (1.2.840.113556.1.4 .261)	ZDPOL-BEREICH-IT-IT3	optional Leitzeichen der OE des Benutzers (sofern zugeordnet) (Aufrechterhaltung der Abwärtskompatibilität zur gegenwärtigen Anbindung an das BKA-IAM)
Leitzeichen *(des PP)*	department	ZDPOL	optional

	(1.2.840.113556.1.2.141)		Leitzeichen des Präsidiums des Benutzers über Präsidiums-Flag. Das PP-Flag nicht in allen Ländern vorhanden, wodurch das Feld leer sein kann. Dies kann auch passieren, wenn ein Anwender unter keinem PP hängt. (Aufrechterhaltung der Abwärtskompatibilität zur gegenwärtigen Anbindung an das BKA-IAM)
	company (1.2.840.113556.1.2.146)	BB	optional Ein fester aber konfigurierbarer Wert
UPN	userPrincipalName (1.2.840.113556.1.4.656)	stumovec@polizei.bb.local	**verpflichtend (5)** (Aufrechterhaltung der Abwärtskompatibilität zur gegenwärtigen Anbindung an das BKA-IAM)
P20-UID	employeeNumber (1.2.840.113556.1.2.610)	T-36-12-12-101-T0200003390	**Verpflichtend (6)** Verbundweit eindeutiger P20-Identifikator

Die Attribute Benutzerkennung, Nachname, Vorname und E-Mail sind automatisch aus dem AD in die BV übernommene Werte und in der BV unveränderlich. Diese vier Attribute, erweitert um die Attribute P20-UID, TelefonNr und der UPN, aus Gründen der Abwärtskompatibilität zur bisherigen Anbindung an das BKA-IAM bestimmen den Export in Richtung TN-P20-LDAP-Verzeichnis. Ist eines der sechs verpflichtenden Attribute nicht befüllt, erfolgt kein Export des Datensatzes.

Die Benutzerkennung ist das identifizierende Merkmal eines Nutzers und ist für den jeweiligen Datensatz unveränderlich. Die Werte Dienstgrad, TelefonNr und OE-Zugehörigkeit werden in der BV administriert und sind stark veränderlich.

Wird in der BV ein neuer Nutzer angelegt (Übernahme aus dem AD) erfolgt noch kein automatischer Export in Richtung TN-P20-LDAP-Verzeichnis. Erst mit der Vergabe eines Rechtes in der Rechtegruppe P20-Anwendungen wird der Export angestoßen.

OE-Zugehörigkeit: Die Pflege der OE-Struktur erfolgt sowohl in der BV als auch in den jeweiligen P20-Anwendungen. Die in das TN-P20-LDAP-Verzeichnis zu übertragenden OE-Informationen sind „flach“, d. h. sie haben keine innere hierarchische Struktur und stellen zudem nur einen Ausschnitt der vollständigen OE-Hierarchie des TN dar. Diese müssen jedoch eineindeutig zu den in der P20-Anwendung gehaltenen bzw. verwendeten OE-Informationen passen.

Tabelle 1: AF.BV.P20-AW.00 „Übertragung Benutzer und Benutzerinfomationen in TN-P20-LDAP“

Identifikator:	AF.BV.P20-AW.00 „Übertragung Benutzer und Benutzerinfomationen in TN-P20-LDAP“
Name:	Übertragung Benutzer und Benutzerinfomationen in TN-P20-LDAP
Bereich:	BV
Auslöser:	Trigger: a) BV-Nutzer zieht einen Benutzer[i] in eine OE, pflegt dessen Eigenschaften b) BV-Nutzer vergibt P20-Anwendungs-Rolle/Recht an den Benutzer[i] als Berechtigung
Ziel:	Benutzer wird mit den Benutzerinformationen (definierte Attribute) an das TN-P20-LDAP-Verzeichnis übertragen und die unten im Normal- bzw. Alternativablauf beschriebenen Beziehungen sollen erstellt werden.
Vorbedingung:	Die Attribute Benutzerkennung, Vorname, Nachname, E-Mail, UPN, P20-UID, TelefonNr sind befüllt, ein Recht aus der Rechtegruppe einer P20-Anwendung ist vergeben.
Ergebnis im Erfolgsfall:	Datensatz des Nutzers ist im LDAP unterhalb von OU=P20-Benutzer zu finden und Nutzerinformationen wurden übernommen und die unten im Normal- bzw. Alternativablauf beschriebenen Gruppen und Gruppenmitgliedschaften konnten erstellt werden.
Ergebnis im Fehlerfall:	BV-Bearbeiter wird über die nicht erfolgreiche Übertragung an der BV-Oberfläche mit einem Hinweis zur Ursache informiert.
Nachbedingung:	
Normalablauf	1. Export der Daten in das TN-P20-LDAP wird initiiert a) OU=P20-Anwendungen - Gibt es diese P20 Anwendung, in der BV als P20-Rechtegruppe repräsentiert, als OU=AW[k] bereits in diesem Zweig? --> wenn nicht, dann Fehler! --> Abbruch Rechteprovisionierung (Schnittstelle bleibt stehen) b) OU=P20-Benutzer - Gibt es diesen Benutzer "Benutzer[i]" bereits in diesem Zweig? --> wenn nicht, dann diesen als weiteres Benutzerobjekt CN=Benutzer[i] anlegen --> wenn ja, dann Aktualisierung der Nutzerinformationen c) OU=TN-Orgs - Gibt es diese TN-Org TN-OE[j] bereits in diesem Zweig? --> wenn nicht, dann diese OE[j] als weiteres OE-Objekt CN=TN-OE[j] anlegen --> Benutzer[i] als member mit TN-OE[j] verknüpfen d) CN=Benutzer[i] als member mit CN=Zugriff OU=AW[k] verknüpfen --> bei Fehler! --> Abbruch Rechteprovisionierung (Schnittstelle bleibt stehen) e) OU=Funktionsrechte --> keine Aktion

f) OU=Rollen
/* hier erfolgt die Berücksichtigung des neuen typisierenden Merkmals eines Recht/Rolle R[x]!
*(R[x] ist die „Bezeichnung“ des Rechts in der BV) */*

falls Rollen-Typ=Benutzer-Rolle → Verzweigung zu ou=Benutzer-Rolle
- Gibt es Recht/Rolle R[x] als CN=R[x] in diesem Zweig?
--> wenn nicht, dann Fehler! --> Abbruch Rechteprovisionierung (Schnittstelle bleibt stehen)

falls Rollen-Typ=Aufgabenbereich → Verzweigung zu ou=Aufgabenbereiche
- Gibt es Recht/Rolle R[x] als CN=R[x] in diesem Zweig?
--> wenn nicht, dann Fehler! --> Abbruch Rechteprovisionierung (Schnittstelle bleibt stehen)

falls Rollen-Typ=Schutzbereich → Verzweigung zu ou=Schutzbereiche
- Gibt es Recht/Rolle R[x] als CN=R[x] in diesem Zweig?
--> wenn nicht, dann Fehler! --> Abbruch Rechteprovisionierung (Schnittstelle bleibt stehen)

falls Rollen-Typ=Vertretung → Verzweigung zu ou=Marker
- Gibt es Recht/Rolle „Vertretung“ als CN=R[x] in diesem Zweig?
--> wenn nicht, dann Fehler! --> Abbruch Rechteprovisionierung (Schnittstelle bleibt stehen)

g) OU=Intermediate
- Gibt es das Intermediate-Objekt CN=AW[k] | R[x] | OE[j] bereits?
--> wenn nicht, dann anlegen

falls Rollen-Typ=Benutzer-Rolle
--> Gibt es die Benutzer-Rolle CN=AW[k] | R[x] OU=Benutzer-Rollen?
--> wenn nicht, dann Fehler! --> Abbruch
--> Intermediate-Objekt CN=AW[k] | R[x] | OE[j] mit CN=AW[k] | R[x] OU=Benutzer-Rollen verknüpfen

falls Rollen-Typ=Aufgabenbereich
--> Gibt es den Aufgabenbereich CN=AW[k] | R[x] OU=Aufgabenbereiche?
--> wenn nicht, dann Fehler! --> Abbruch
--> Intermediate-Objekt CN=AW[k] | R[x] | OE[j] mit CN=AW[k] | R[x] OU=Aufgabenbereiche verknüpfen

falls Rollen-Typ=Schutzbereich
--> Gibt es den Schutzbereich CN=AW[k] | R[x] OU=Schutzbereiche?
--> wenn nicht, dann Fehler! --> Abbruch
--> Intermediate-Objekt CN=AW[k] | R[x] | OE[j] mit CN=AW[k] | R[x] OU=Schutzbereiche verknüpfen

falls Rollen-Typ=Vertretung
--> Gibt es den Marker CN=AW[k] | Vertretung OU=Marker?

	--> wenn nicht, dann Fehler! --> Abbruch --> Intermediate-Objekt CN=AW[k]-R[x]-OE[j] mit Marker CN=AW[k] | Vertretung OU=Marker verknüpfen --> Intermediate-Objekt CN=AW[k] | R[x] | OE[j] mit TN-Org CN=OE[j] verknüpfen h) CN=Benutzer[i] als member mit Intermediate-Objekt CN=AW[k] | R[x] | OE[j] verknüpfen
Alternativablauf:	BV-Nutzer vergibt das spezielle P20-Anwendungs-Rolle/Recht an den Benutzer als Fremdberechtigung: Ablauf ist analog zur Rollenzuordnung im Normalablauf --> Ausnahme: a) … b) ... ~~c)~~ OU=TN-Orgs - Gibt es diese TN-Org "TN-OE[j]" bereits in diesem Zweig? --> wenn nicht, dann diese OE als weiteres OE-Objekt CN=TN-OE[j] anlegen ~~--> Benutzer[i] als member mit TN-OE[j] verknüpfen [diese Verknüpfung erfolgt hier nicht!!!]~~ d) ... Anmerkung: Es soll die entsprechende OE-Gruppe für die Rolle (Intermediate) angelegt werden, aber der User NICHT zum Mitglied werden, da es nicht seine primäre OE ist.
Plausibilitäten:	*Keine*
Häufigkeit:	*Nicht relevant*
Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

2.2 AF.BV.P20-AW.01 „Änderung Nutzereigenschaften eines P20-Benutzers“

In der BV erfolgt die Pflege der Benutzereigenschaften. Ausnahmen bilden hier die Attribute Benutzerkennung, Nachname, Vorname, UPN und Emailadresse. Diese werden im AD gepflegt und sind in der BV unveränderlich. Die oben im Anwendungsfall AF.BV.P20-AW.00 „Übertragung eines P20-Benutzers mit Nutzerinfomationen in TN-P20-LDAP“ aufgelisteten Attribute

- TelefonNr
- Dienstgrad

werden in der BV durch den jeweils zuständigen BV-Anwender gepflegt. Ändern sich diese Attribute, so ist an das TN-P20-LDAP-Verzeichnis eine entsprechende Aktualisierung zu senden. Auslöser des Sendens ist das Speichern der Änderung. Der geänderte Datensatz wird an das TN-P20-LDAP-Verzeichnis übermittelt. Die SNIT_ITK-BV-TN-LDAP erkennt, dass ein Objekt dieser Benutzerkennung bereits vorhanden ist und aktualisiert dieses.

Anmerkung:

Erfolgt eine Änderung im AD auf den in der BV nicht veränderbaren Daten, so sind diese ebenfalls in das TN-P20-LDAP-Verzeichnis zu überstellen. Auslöser des Sendens ist das Speichern der Übernahme der Änderung aus dem AD. (Eine Änderung der Benutzerkennung ist ausgeschlossen!)

Tabelle 2: AF.BV.P20-AW.01 „Änderung Nutzereigenschaften eines P20-Benutzers“

Identifikator:	AF.BV.P20-AW.01 „Änderung Nutzereigenschaften eines P20-Benutzers“
Name:	Übertragung der Nutzereigenschaften in LDAP
Bereich:	BV
Auslöser:	Änderung einer Nutzereigenschaft
Ziel:	Änderung der Nutzereigenschaften Nutzer wird an LDAP übertragen
Vorbedingung:	Der Nutzer ist in der BV einer OE zugeordnet und wurde bereits an LDAP übertragen.
Ergebnis im Erfolgsfall:	Änderungen an den Eigenschaften des Benutzers ist im LDAP zu finden
Ergebnis im Fehlerfall:	Abbruch des Anwendungsfalls und Eintrag des Fehlers in ein „Schnittstellen-Logbuch“
Nachbedingung:	
Normalablauf	1. BV-Nutzer ändert dessen Eigenschaften 2. Export der Daten in LDAP wird initiiert 3. Daten kommen im LDAP an
Alternativablauf:	Keine
Plausibilitäten:	*Keine*
Häufigkeit:	*Nicht relevant*
Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

2.3 AF.BV.P20-AW.02 „Rechte-Entzug einzeln“

Einem Benutzer wird ein in der BV vergebenes Recht/Rolle für eine P20-Anwendung entzogen. Im Ergebnis können noch weitere Rechte dieser P20-Anwendung beim Benutzer verbleiben. Ebenfalls möglich ist der Entzug des letzten verbliebenen Rechts/Rolle einer P20-Anwendung. Das führt dann an der SNIT_ITK-BV-TN-LDAP zu einer alternativen Bereinigung.

Tabelle 3: AF.BV.P20-AW.02 „Rechte-Entzug einzeln“

Identifikator:	AF.BV.P20-AW.02 „Rechte-Entzug einzeln“
Name:	Rechte-Entzug einzeln
Bereich:	BV
Auslöser:	Automatisches Auslösen nach Entzug eines einzelnen Rechts/Rolle
Ziel:	Änderung wird an LDAP übertragen und führt dort zur Anpassung der Struktur
Vorbedingung:	Der Nutzer ist bereits im TN-P20-LDAP-Verzeichnis eingetragen und hat dort die erforderlichen memberOf-Beziehungen zum Zugriff auf die betreffende P20-Anwendung sowie eine memberOf-Beziehung zum „intermediate“-Objekt, welches die zu löschende Recht/Rolle-Dienststelle-Verknüpfung im LDAP-Verzeichnis repräsentiert.
Ergebnis im Erfolgsfall:	Entzug der Berechtigung in der BV führt zu einer korrekten korrespondierenden Anpassung des Rechteentzugs im TN-P20-LDAP-Verzeichnis.
Ergebnis im Fehlerfall:	Entzug der Berechtigung in der BV führt NICHT zu einer korrekten korrespondierenden Anpassung des Rechteentzugs im TN-P20-LDAP-Verzeichnis.
Nachbedingung:	
Normalablauf	1. Suchen des zum Trippel (Anwendung AW[k], Dst, Recht/Rolle) korrespondierenden „intermediate“-Objekt im LDAP-Verzeichnis. 2. Entfernen der member-Beziehung zwischen Benutzer und „intermediate“-Objekt *(Das „memberOf“ Attribut des Users wird geladen und darin eine passend benannte Gruppe gesucht. Und dort wird er entfernt.)* 3. Falls dieses „intermediate“-Objekt nach Schritt 2 keine weitere Referenz auf einen Nutzer enthält, soll es ebenfalls entfernt werden. 4. Falls nach Schritt 3 keine weitere Referenz von diesem Benutzer zu intermediate-Objekten der Anwendung AW[k] existiert, wird die Referenz zwischen diesem Benutzer und dem Objekt „cn=Zugriff“ im Zweig AW[k] entfernt.
Alternativablauf:	Keine
Plausibilitäten:	Trippel (Anwendung AW[k], Dst, Recht/Rolle) sollte nur im Unterbaum genau einer P20-Anwendung zu finden sein
Häufigkeit:	*Nicht relevant*
Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

2.4 AF.BV.P20-AW.03 „Entfernen der OE-Zugehörigkeit eines Benutzers“

Die Zugehörigkeit eines Benutzers zu einer OE als Stammdienststelle wird im P20-TN-LDAP-Verzeichnis referenziert durch die Gruppenmitgliedschaft des Benutzers in einer OE im Zweig ou=TN-Orgs.

Im Zusammenhang mit einem Wechsel der Stammdienststelle (AF.BV.Kern.01 „vollständiger Rechteentzug beim Wechsel der Stammdienststelle eines Benutzers“) muss diese Gruppenmitgliedschaft entfernt werden.

Tabelle 4: AF.BV.P20-AW.03 „Entfernen der OE-Zugehörigkeit eines Benutzers“

Identifikator:	AF.BV.P20-AW.03 „Entfernen der OE-Zugehörigkeit eines Benutzers“
Name:	Entfernen der OE-Zugehörigkeit eines Benutzers
Bereich:	BV
Auslöser:	Wechsel der Stammdienststelle (AF.BV.Kern.01 „vollständiger Rechteentzug beim Wechsel der Stammdienststelle eines Benutzers“)
Ziel:	Bestehende Gruppenmitgliedschaft des Benutzer in einer OE wird im P20-TN-LDAP-Verzeichnis entfernt.
Vorbedingung:	Benutzer hat eine bestehende Gruppenmitgliedschaft zu einer OE im P20-TN-LDAP-Verzeichnis im Zweig ou=TN-Orgs
Ergebnis im Erfolgsfall:	Gruppenmitgliedschaft im P20-TN-LDAP-Verzeichnis ist entfernt. Ebenfalls wird die OE entfernt, falls es keine weiteren Mitgliedschaften zu anderen Benutzern gibt.
Ergebnis im Fehlerfall:	Gruppenmitgliedschaft besteht weiter.
Nachbedingung:	
Normalablauf	1. Benutzer unter ou=P20-Benutzer finden 2. Entfernen der member-Beziehung zur referenzierten Stammdienststelle des Benutzers → falls die Stammdienststelle keine weitere Referenz (keine memberOf-Beziehung) zu einem Benutzer mehr hat, dann diese OE aus dem Zweig ou=TN-Orgs entfernen
Alternativablauf:	Keine
Plausibilitäten:	
Häufigkeit:	*Nicht relevant*
Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

2.5 AF.BV.P20-AW.04 „Recht/Rolle wird in der BV einer OE entzogen“

Wird ein Recht/Rolle in der BV einer OE zur Vergabe entzogen, so werden bislang alle erteilten Berechtigungen basierend auf diesem Recht/Rolle den Mitarbeitern entzogen. Darüber hinaus

kann diese Rolle auch nicht mehr vergeben werden. Dies betrifft ebenso erteilte Fremdberechtigungen an Mitarbeitern anderer OEen die dieses Recht/Rolle erhalten haben. Dieser Entzug muss in das TN-P20-LDAP-Verzeichnis gespiegelt werden.

Tabelle 5: AF.BV.P20-AW.04 „Recht/Rolle wird in der BV einer OE entzogen“

Identifikator:	AF.BV.P20-AW.04 „Recht/Rolle wird in der BV einer OE entzogen“
Name:	Recht/Rolle wird in der BV einer OE entzogen
Bereich:	BV
Auslöser:	Manueller Entzug einer Rolle für die Vergabe in einer OE
Ziel:	Alle bislang erteilten Berechtigungen basierend auf diesem Recht/Rolle werden den Mitarbeitern dieser OE entzogen. Ebenso werden erteilte Fremdberechtigungen an Mitarbeitern anderer OEen, basierend auf diesem Recht/Rolle entzogen.
Vorbedingung:	
Ergebnis im Erfolgsfall:	Das im TN-P20-LDAP-Verzeichnis erstellte Intermediate-Objekt, welches die Einschränkung dieses Rechtes/Rolle auf diese OE repräsentiert wird gelöscht. Damit sollten dann alle darauf basierenden member/memberOf-Beziehungen dieses intermediate-Objekts mit entfernt sein.
Ergebnis im Fehlerfall:	
Nachbedingung:	
Normalablauf	1. Einzelner Rechteentzug für jedes Trippel aus (Benutzer, Recht, OE) über AF.BV.P20-AW.02 Rechte-Entzug einzeln“
Alternativablauf:	
Plausibilitäten:	
Häufigkeit:	*Nicht relevant*
Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

2.6 AF.BV.P20-AW.05 „OE wird in der BV gelöscht“

Wird in der BV eine Organisationseinheit (OE) gelöscht, so ist bislang das Verhalten dadurch bestimmt, dass dann alle dieser OE zugeordneten Mitarbeiter keiner OE mehr zugeordnet sind und alle Berechtigungen mit Bezug zu dieser OE für diese Mitarbeiter entfernt werden. Dies gilt ebenfalls für Fremdberechtigungen, die in anderen OEen basierend auf dieser OE vergeben wurden. Dieser Entzug muss in das TN-P20-LDAP-Verzeichnis gespiegelt werden.

Tabelle 6: AF.BV.P20-AW.05 „OE wird in der BV gelöscht“

Identifikator:	AF.BV.P20-AW.05 „OE wird in der BV gelöscht“
Name:	OE wird in der BV gelöscht
Bereich:	BV
Auslöser:	Manuelles Entfernen einer gesamten OE in der BV
Ziel:	Im Nachgang des bereits jetzt existierenden Verhaltens der BV beim Löschen einer OE wird das Rücksetzen der Berechtigungen und das Löschen der OE in das TN-P20-LDAP-Verzeichnis gespiegelt.
Vorbedingung:	
Ergebnis im Erfolgsfall:	Alle Berechtigungen, die basierend auf Rechten dieser OE an Benutzer dieser OE oder an Fremdberechtigte vergeben wurden, sind im P20-TN-LDAP-Verzeichnis entfernt. Ebenso entfernt ist dort die OE im Zweig ou=TN-Orgs.
Ergebnis im Fehlerfall:	
Nachbedingung:	
Normalablauf	OE[j] repräsentiert die zu löschende OE **1.** Für alle in der BV vergebenen Rechte dieser OE a. AF.BV.P20-AW.02 „Rechte-Entzug einzeln“ für jedes Trippel (Benutzer, Recht, OE) **2.** Abschließend im Zweig ou=TN-Orgs cn=TN-OE[j] ← dieses Objekt löschen
Alternativablauf:	
Plausibilitäten:	
Häufigkeit:	*Nicht relevant*
Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

2.7 AF.BV.P20-AW.06 „Recht/Rolle einer P20-AW-Rechtegruppe wird gelöscht“

Schrittweise für alle MA in der BV, die dieses Recht/Rolle haben, einen Anwendungsfall zum Einzelrechtentzug ausführen AF.BV.P20-AW.02 „Rechteentzug einzeln“

Tabelle 7: AF.BV.P20-AW.06 „Recht/Rolle einer P20-AW-Rechtegruppe wird gelöscht“

Identifikator:	AF.BV.P20-AW.06 „Recht/Rolle einer P20-AW-Rechtegruppe wird gelöscht“
Name:	Recht/Rolle einer P20-AW-Rechtegruppe wird gelöscht
Bereich:	BV
Auslöser:	Manuelles Auslösen in der Rechteverwaltung der BV
Ziel:	Korrespondierend zur bereits existierenden Verfahrensweise in der BV, dass alle bestehenden Rechtvergaben an Nutzer bzgl. dieses Rechtes entfernt werden, wird diese Änderung auch an das TN-P20-LDAP-Verzeichnis übertragen und führt dort zur Anpassung im Verzeichnisbaum.
Vorbedingung:	keine
Ergebnis im Erfolgsfall:	Gelöschtes Recht/Rolle ist nicht mehr im LDAP vergeben.
Ergebnis im Fehlerfall:	
Nachbedingung:	
Normalablauf	3. Für jeden BV-Benutzer in der BV. a. Für jede erstellte Recht/Rollen-Vergabe dieser P20-Anwendung i. AF.BV.P20-AW.02 „Rechteentzug einzeln“
Alternativablauf:	
Plausibilitäten:	
Häufigkeit:	*Nicht relevant*
Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

3 Anwendungsfälle BV-ADMIN-TOOL

3.1 AF.BV.Admin-Tool.00 „Löschen aller Benutzerberechtigungen im TN-P20-LDAP“

Hiermit erfolgt eine Bereinigung aller im TN-P20-LDAP gespeicherten Benutzer-Berechtigungszuordnungen. In dieser Bereinigung werden die Benutzer selbst und alle „intermediate“-Objekte in allen P20-Anwendungsobjekten entfernt. Erhalten bleibt für alle P20-Anwendungen der Rollenzuschnitt (die Zuordnungen zwischen Rollen und Funktionsrechten).

Hinweis zur Abstimmung mit F-IAM (BKA):

Das Löschen von Benutzern im TN-P20-LDAP-Verzeichnis muss durch den TN möglich sein! Andernfalls gäbe es keine Korrekturmöglichkeiten für den durch den TN bereitgestellten Datenbestand an der Schnittstelle. Das F-IAM muss mit dieser Situation umgehen können.

Tabelle 8: AF.BV.Admin-Tool.00 „Löschen aller Benutzerberechtigungen im TN-P20-LDAP“

Identifikator:	AF.BV.Admin-Tool.00 „Löschen aller Benutzerberechtigungen im TN-P20-LDAP“
Name:	Löschen aller Benutzerberechtigungen im TN-P20-LDAP
Bereich:	BV
Auslöser:	Manuelles Auslösen durch einen Administrator.
Ziel:	Bereinigung aller im TN-P20-LDAP gespeicherten Benutzer-Berechtigungszuordnungen.
Vorbedingung:	keine
Ergebnis im Erfolgsfall:	Alle Berechtigungen aller Nutzer auf P20-Anwendungen sowie die verbindenden „intermediate“-Objekte werden vollständig im TN-P20-LDAP-Verzeichnis gelöscht.
Ergebnis im Fehlerfall:	Unvollständig bereinigtes TN-P20-LDAP ist nicht mehr konsistent und muss daher durch LDAP-Administrator nachbearbeitet werden.
Nachbedingung:	
Normalablauf	1. Für jeden P20-Benutzer im TN-P20-LDAP-Verzeichnis. a. Löschen des P20-Benutzer i. Annahme 1: damit werden auch alle memberOf-Beziehungen jedes Benutzers zum „Zugriffs“-Anker in jedem P20-Anwendungszweig gelöscht ii. Annahme 2: damit werden auch alle memberOf-Beziehungen jedes Benutzers zu den verbundenen „intermediate“-Zweigen in jedem P20-Anwendungszweig gelöscht iii. Annahme 3: damit wird auch die memberOf-Beziehungen des Benutzers zu der verbundenen „TN-OE“ im TN-Orgs-Zweig gelöscht 2. Löschen aller „intermediate“-Objekte in jedem P20-Anwendungs-Zweig 3. Löschen aller „TN-OE“-Objekte im TN-Orgs-Zweig, die keine member-Beziehung zu einem P20-benutzer haben. 4. Ende
Alternativablauf:	Keine
Plausibilitäten:	
Häufigkeit:	*Nicht relevant*

Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

3.2 AF.BV.Admin-Tool.01 „Initialer P20-Voll-Export nach LDAP“

Ziel des initialen P20-Voll-Exports ist der vollständige Neuaufbau der Berechtigungszuordnungen im TN-P20-LDAP-Verzeichnis für alle Benutzer. Dem Neuaufbau muss mit AF.BV.Admin-Tool.00 „Löschen aller Benutzerberechtigungen im TN-P20-LDAP“ eine Bereinigung vorangehen.

Tabelle 9: AF.BV.Admin-Tool.01 „Initialer P20-Voll-Export nach LDAP“

Identifikator:	AF.BV.Admin-Tool.01 „Initialer P20-Voll-Export nach LDAP“
Name:	Initialer P20-Voll-Export nach LDAP
Bereich:	BV
Auslöser:	Manuelles Auslösen durch einen Administrator.
Ziel:	Ziel des initialen P20-Voll-Exports ist der vollständige Neuaufbau der Berechtigungszuordnungen im TN-P20-LDAP-Verzeichnis für alle Benutzer.
Vorbedingung:	Alle Nutzer- und Berechtigungsinformationen sind vollständig aus dem TN-PS-LDAP entfernt (AF.BV.Admin-Tool.00 „Löschen aller Benutzerberechtigungen im TN-P20-LDAP“ ist erfolgreich durchgelaufen)
Ergebnis im Erfolgsfall:	Alle Nutzer sowie deren Berechtigungen auf P20-Anwendungen werden nach Prüfung der Rechte/Rollen-Konsistenz neu übernommen.
Ergebnis im Fehlerfall:	Beim Abbruch der Konsistenzprüfung verbleibt das TN-P20-LDAP-Verzeichnis ohne jegliche Zuordnung von Benutzern zu Rollen. Nur die Zuordnung von Funktionsrechten zu Rollen bleibt bestehen.
Nachbedingung:	
Normalablauf	1. Durchführung AF.BV.P20-AW.05 „Konsistenzprüfung Rechte/Rollen“ → Abbruch bei vorhandenen Inkonsistenzen 2. Für jeden Benutzer a. Für jede P20-Anwendung (jede P20-Rechtegruppe) i. Für jedes vergebene Recht/Rolle dieser P20-Anwendung 1. AF.BV.P20-AW.00 „Übertragung eines P20-Benutzers mit Nutzerinformationen in TN-P20-LDAP“ 3. Ende
Alternativablauf:	Keine
Plausibilitäten:	*Interne Prüfung der Rechte/Rollen-Konsistenz*
Häufigkeit:	*Nicht relevant*
Anwendungsfall enthält:	

Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

3.3 AF.BV.Admin-Tool.02 „Konsistenzprüfung Rechte/Rollen“

Jedes in der BV zur Vergabe für eine P20-Anwendung angelegte Recht/Rolle muss im TN-P20-LDAP-Verzeichnis eine korrespondierende Entsprechung in dem Zweig „Rollen“ der jeweiligen P20-Anwendung haben. Dabei ist es unerheblich, ob einer solchen Recht/Rolle bereits eine weitere Untersetzung aus dem Zweig „Funktionsrechte“ zugeordnet wurde oder nicht.
Wird eine solche Entsprechung nicht gefunden, so wird diese Recht/Rolle-Inkonsistenz Bestandteil des aktuellen Fehler-Logs.

Tabelle 10: AF.BV.Admin-Tool.02 „Konsistenzprüfung Rechte/Rollen“

Identifikator:	AF.BV.Admin-Tool.02 „Konsistenzprüfung Rechte/Rollen“
Name:	Konsistenzprüfung Rechte/Rollen
Bereich:	BV
Auslöser:	Kann implizit aus einem anderen AF oder durch manuelles Auslösen durch den Administrator ausgelöst werden.
Ziel:	Bestehende Inkonsistenzen in der Rechte/Rollen-Abbildung zwischen BV und TN-P20-LDAP-Verzeichnis werden gefunden und für den Benutzer zur schrittweisen Behebung gelistet.
Vorbedingung:	keine
Ergebnis im Erfolgsfall:	Prüfung konnte für jedes P20-Anwendung und für jede jeweils in der BV angelegte Rolle durchgeführt werden. Insofern eine Inkonsistenz festgestellt wurde, konnte diese mit einem entsprechenden Hinweis gelistet werden.
Ergebnis im Fehlerfall:	Noch festzulegen!
Nachbedingung:	
Normalablauf	1. In der BV für jede Rechtegruppe einer P20-Anwendung [AW<i>] a. Prüfung, ob es im TN-P20-LDAP-Verzeichnis unter ou=P20-Anwendungen eine korrespondierenden Anwendungszweig ou=AW<i> gibt → wenn nicht, dann Inkonsistenz gefunden, listen und zur nächsten BV-Rechtegruppe einer P20-Anwendung übergehen b. Für jedes Recht/Rolle der Rechtegruppe i. Prüfung, ob Recht/Rolle unter ou=Rollen entsprechend der jeweiligen Typisierung der Rolle mit Eintrag cn=**AW<i> | Rolle/Recht** ou=Benutzer-Rollen bzw. cn=**AW<i> | Rolle/Recht** ou=Aufgabenbereiche bzw. cn=**AW<i> | Rolle/Recht** ou=Schutzbereiche bzw. cn=**AW<i> | Vertretung** ou=Marker zu finden ist → wenn nicht, dann Inkonsistenz gefunden; listen und zum nächsten Recht/Rolle übergehen

	c. OPTIONAL: Zusätzlich kann in einer dritten inneren Schleife auch noch auf die konsistente Zuordnung von Funktionsrechten geprüft werden. (→ Aufwand/Komplexität!)
Alternativablauf:	*keiner*
Plausibilitäten:	*Keine*
Häufigkeit:	*Nicht relevant*
Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

3.4 AF.BV.Admin-Tool.03 „Initiale Anlage Rollen+Funktionsrechte für eine P20-Anwendung“

Zur initialen und konsistenten Anlage der Rollen und Funktionsrechte einer P20-Anwendung AW[i] im TN-P20-LDAP-Verzeichnis werden die Rollen und Funktionsrechte sowie deren Verknüpfung untereinander (Rollenzuschnitt) aus einem Quell-Konfigurationsdatenbestand (CSV-Datei), gelesen und sukzessive an das TN-P20-LDAP-Verzeichnis übertragen und dort entsprechend der Vorgaben in Abschnitt „1.3 Strukturierung des TN-P20-Übergabeverzeichnisdienstes“ des Lastenheftes angelegt. Vorab werden alle bestehenden Rollen, Funktionsrechte, Intermediate-Objekte für diese P20-Anwendung (ou=AW[i]) entfernt (gelöscht).

Auf diese Art erfolgt eine administrativ-hilfreiche Entkoppelung der fachlichen Rollenkonfiguration und Rechtezuordnung von der tatsächlich physischen Anlage dieser im TN-P20-LDAP-Verzeichnis. Nach Ausführung dieser initialen Neuanlage des Rollenzuschnitts für eine P20-Anwendung, muss zwingend „AF.BV.ADMIN-TOOL.01 „Konsistenzprüfung Rechte/Rollen" und „AF.BV. ADMIN-TOOL.03 Initialer Voll-Export für eine P20-Anwendung“ manuell angestoßen werden.

Generell ist die BV das führende System! Daher muss das TN-P20-LDAP-Verzeichnis mit den in der BV vorhandenen Rollen umgehen können. Inkonsistenzen sind unzulässig und müssen zwingend behoben werden.

Diese Funktionalität ist so lang erforderlich, so lange die Funktionsrechte nicht direkt in der BV angelegt und dort zu Rollen geschnitten werden können.

Die F-IAM-Komponente ZeRo soll zukünftig Anwendungs-Funktionsrechte zum Herunterladen in die TN-Umgebung anbieten, so dass dann die TN-BV diese für einen Rollenzuschnitt (Zuordnung von Funktionsrecht zu Rolle) nutzen könnte. Ziel ist es, dass auf TN-Seite nur Funktionsrechte und Rollen genutzt werden, die der F-IAM auch kennt und weiterverarbeiten kann.

Tabelle 11: AF.BV.Admin-Tool.03 „Initiale Anlage Rollen+Funktionsrechte für eine P20-Anwendung“

Identifikator:	AF.BV.Admin-Tool.03 „Initiale Anlage Rollen+Funktionsrechte für eine P20-Anwendung“
Name:	Initiale Anlage Rollen+Funktionsrechte für eine P20-Anwendung
Bereich:	BV
Auslöser:	Manuelles Auslösen durch den Administrator.
Ziel:	Für eine P20-Anwendung wird aus einer zugehörigen CSV-Datei der zu dieser Anwendung vorliegende Rollenzuschnitt ausgelesen und an das TN-P20-LDAP-Verzeichnis übertragen, dort angelegt und festgeschrieben.
Vorbedingung:	CSV-Datei mit Rollenzuschnitt für eine P20-Anwendung liegt entsprechend der vereinbarten Struktur vor. Die Spalte 1 beinhaltet für jede Zeile den Namen der P20-Anwendung. (siehe Anlage 5)
Ergebnis im Erfolgsfall:	Der in der CSV-Datei definierte Rollenzuschnitt der P20-Anwendung ist im TN-P20-LDAP-Verzeichnis verfügbar. Eventuell bestehende frühere Rollenzuschnitte wurden vorab entfernt. Die Protokollierung zur erfolgten Rollenanlage und der Zuordnung der Funktionsrechte soll über die bereits in der BV bestehende Berichte-Seite abrufbar bzw. einsehbar sein.
Ergebnis im Fehlerfall:	Meldung im Admin-Tool über nicht vollständig abgeschlossene Übertragung und Anlage (Fehlermeldung). Darüber hinaus verbleibt der bis dahin unvollständig angelegte Rollenzuschnitt im TN-P20-LDAP-Verzeichnis zur Fehleranalyse.
Nachbedingung:	
Normalablauf	1. Prüfen, ob P20-Anwendung (ou=AW[i]) bereits Bestandteil des Verzeichnisbaums im TN-P20-LDAP-Verzeichnis ist a. → falls ja, alle bestehenden Rollen, Funktionsrechte, Intermediate-Objekte für diese P20-Anwendung (ou=AW[i]) entfernen b. → P20-Anwendung (ou=AW[i]) im Verzeichnisbaum einschließlich seiner Strukturelemente: cn=Zugriff, ou=Funktionsrechte, ou=Rollen, ou=Benutzer-Rollen ou= Rollen, ou=Aufgabenbereiche ou= Rollen, ou=Schutzbereiche ou= Rollen, ou=Marker ou= Rollen und ou=Intermediate anlegen 2. für jede Rolle der CSV-Datei a. Anlage der Rolle entsprechend seiner Typisierung (Objekttyp) als cn=AW[i] | Rolle[i] unter ou=Benutzer-Rollen ou= Rollen, ou=Aufgabenbereiche ou= Rollen, ou=Schutzbereiche ou= Rollen, ou=Marker ou= Rollen (Eintrag in Spalte B der Anlage 5) b. für jedes Funktionsrecht der Rolle[i] aus CSV-Datei i. Anlage des Funktionsrechtes als cn= AW[i] | FR[i] (Eintrag in Spalte D der Anlage 5) ii. Verknüpfen von FR[i] mit Rolle[i] (unter Beachtung der o.g. Typisierung) durch Herstellung der member-Beziehung entsprechend der Struktur-Vorgabe im Abschnitt 1.3

	iii. Erzeugung eines Protokolleintrages
Alternativablauf:	
Plausibilitäten:	*Der Name der P20-Anwendung in Spalte 1 der csv-Datei muss dabei der Bezeichnung der BV-Rechtegruppe entsprechen, aus der heraus diese Rollen/Rechte dann in der BV vergeben werden sollen.*
Häufigkeit:	*eher selten;* *nach Änderung des Rollenzuschnitts (neue Zusammensetzung der Rolle; Aufnahme zusätzlicher Funktionsrechte; Entfernen ungültiger Funktionsrechte)*
Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

3.5 AF.BV.Admin-Tool.04 „Initialer Vollexport für eine P20-Anwendung“

Ziel des "initialen Voll-Exports für eine P20-Anwendung" ist der vollständige Neuaufbau der Berechtigungszuordnungen TN-P20-LDAP-Verzeichnis für alle Benutzer dieser P20-Anwendung. Dem Neuaufbau geht eine Bereinigung voran. In dieser Bereinigung werden alle „intermediate“-Objekte in diesem P20-Anwendungs-Objekt entfernt.

Erhalten bleibt in dieser P20-Anwendung der Rollenzuschnitt (Zuordnungen zwischen Rollen und Funktionsrechten).

Tabelle 12: AF.BV.Admin-Tool.04 „Initialer Voll-Export für eine P20-Anwendung“

Identifikator:	AF.BV.Admin-Tool.04 „Initialer Voll-Export für eine P20-Anwendung“
Name:	Initialer Voll-Export für eine P20-Anwendung
Bereich:	BV
Auslöser:	Manuelles Auslösen durch den Administrator.
Ziel:	Änderung wird an LDAP übertragen und führt dort zur Anpassung der Struktur
Vorbedingung:	keine
Ergebnis im Erfolgsfall:	Benutzern zugeordnete Berechtigungen dieser P20-Anwendung nach Prüfung der Rechte/Rollen-Konsistenz neu übernommen
Ergebnis im Fehlerfall:	Abbruch, wenn Prüfung der Rechte- und Rollen-Konsistenz Inkonsistenzen aufdeckt.
Nachbedingung:	
Normalablauf	1. Für diese P20-Anwendung im LDAP prüfen, ob die ou=Intermediate noch untergeordnete Objekte enthält → wenn ja, dann Fehler! → Abbruch 2. Für jeden BV-Benutzer in der BV. a. Für jedes vergebene Recht/Rolle dieser P20-Anwendung i. AF.BV.P20-AW.00 „Übertragung eines P20-Benutzers mit Nutzerinfomationen in TN-P20-LDAP“
Alternativablauf:	Keine

Plausibilitäten:	*Interne Prüfung der Rechte/Rollen-Konsistenz*
Häufigkeit:	*Nicht relevant*
Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

3.6 AF.BV.Admin-Tool.05 „Änderung von Funktionsrechtezuordnungen in Rollen“

Vom Administrator in der CSV-Datei erfasste Anpassungen in der Zuordnung von Funktionsrechten zu Rollen (Anpassung des Rollenzuschnitts) werden in das TN-P20-LDAP-Verzeichnis übertragen. Dabei werden weder neue Rollen angelegt noch werden bereits angelegte Rollen entfernt. Es wird nur für bereits angelegte Rollen die Zuordnung der Funktionsrechte überschrieben.

Tabelle 13: AF.BV.Admin-Tool.05 „Änderung von Funktionsrechtezuordnungen in Rollen“

Identifikator:	AF.BV.Admin-Tool.05 „Änderung von Funktionsrechtezuordnungen in Rollen“
Name:	Änderung von Funktionsrechtezuordnungen in Rollen
Bereich:	BV
Auslöser:	Manuelles Auslösen durch den Administrator.
Ziel:	Änderung wird an LDAP übertragen und führt dort zur Anpassung der Struktur
Vorbedingung:	keine
Ergebnis im Erfolgsfall:	Neuer Rollenzuschnitt für bestehende Rollen wurde entsprechend der CSV-Datei übernommen.
Ergebnis im Fehlerfall:	
Nachbedingung:	
Normalablauf	1. für jede Rolle der CSV-Datei für die eine Entsprechung im TN-P20-LDAP-Verzeichnis gefunden wird a. für jedes Funktionsrecht der Rolle[i] aus CSV-Datei, das noch nicht an die Rolle gehangen wurde i. Anlage des Funktionsrechtes als cn= AW[i] | FR[j] ii. Verknüpfen von FR[i] mit Rolle[i] durch Herstellung der member-Beziehung entsprechend der Struktur-Vorgabe im Abschnitt 1.3 iii. Erzeugung eines Protokolleintrages b. für jedes Funktionsrecht der Rolle[i] im TN-P20-LDAP-Verzeichnis, das nicht in der CSV-Datei dieser Rolle zugeordnet ist i. Entfernen der Gruppenmitgliedschaft dieses Funktionsrechtes an der Rolle ii. Entfernen dieses Funktionsrechtes cn= AW[i] | FR[j] iii. Erzeugung eines Protokolleintrages
Alternativablauf:	Keine

Plausibilitäten:	*Interne Prüfung der Rechte/Rollen-Konsistenz*
Häufigkeit:	*Nicht relevant*
Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

3.7 AF.BV.Admin-Tool.06 „Neuanlage einer Rolle mit Funktionsrechten“

Diese Möglichkeit der Neuanlage einer Rolle mit Funktionsrechten für eine Anwendung AW[i] ist bspw. von besonderer Bedeutung für die Integration neuer, hinzukommender Anwendungskomponenten. Diese besitzen meist einen zusätzlichen Satz an komponentenspezifischen Funktionsrechten, die über eine eigenständige Rolle Wirkung entfalten sollen. In der CSV-Datei (Anlage 2) werden durch den Administrator die zusätzlichen Rollen- und Rechtekombinationen ergänzt und das Admin-Tool überträgt alle noch nicht im TN-P20-LDAP-Verzeichnis für diese Anwendung auffindbaren Rollen und Rechte gruppiert sie entsprechend der Vorgaben zur Verzeichnisstruktur (Abschnitt 1.4).

Tabelle 14: AF.BV.Admin-Tool.06 „Neuanlage einer Rolle mit Funktionsrechten“

Identifikator:	AF.BV.Admin-Tool.06 „Neuanlage einer Rolle mit Funktionsrechten“
Name:	Neuanlage einer Rolle mit Funktionsrechten
Bereich:	BV
Auslöser:	Manuelles Auslösen durch den Administrator.
Ziel:	Änderung wird an LDAP übertragen und führt dort zur Anpassung der Struktur
Vorbedingung:	Rolle darf im TN-P20-LDAP-Verzeichnis noch nicht vorhanden sein.
Ergebnis im Erfolgsfall:	Neue Rolle mit Funktionsrechtezuordnung wurde entsprechend der CSV-Datei übernommen und im TN-P20-LDAP-Verzeichnis angelegt.
Ergebnis im Fehlerfall:	Keine Übernahme in das TN-P20-LDAP-Verzeichnis
Nachbedingung:	
Normalablauf	1. für jede Rolle der AW[i]-spezifischen CSV-Datei, für die **keine Entsprechung im TN-P20-LDAP-Verzeichnis** für die Anwendung gefunden wird a. Unter Beachtung der Typisierung - Anlage der Rolle als cn=AW[i] | Rolle[j] im Zweig der Anwendung ou=AW[i] unter ou = Benutzer-Rollen ou=Rollen bzw. ou = Aufgabenbereiche ou=Rollen bzw. ou = Schutzbereiche-Rollen ou=Rollen bzw. ou = Marker ou=Rollen b. für jedes Funktionsrecht der Rolle[j] aus CSV-Datei i. Anlage des Funktionsrechtes als cn= AW[i] | FR[k] im Zweig der Anwendung ou=AW[i] ii. Verknüpfen von FR[k] mit Rolle[j] durch Herstellung der member-Beziehung entsprechend der Struktur-Vorgabe im Abschnitt 1.3

	iii. Erzeugung eines Protokolleintrages
Alternativablauf:	Keine
Plausibilitäten:	Rolle darf im TN-P20-LDAP-Verzeichnis noch nicht vorhanden sein.
Häufigkeit:	*Nicht relevant*
Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

4 Anwendungsfälle BV-Kernkomponente

4.1 AF.BV.Kern.00 „Anlage Rechtegruppe einer P20-AW“

In der BV wird ein Katalog der P20-Anwendungen inkl. eines Leerwertes eingeführt. Jede Rechtegruppe der BV bekommt bei Anlage oder Änderung ein Attribut mit diesem Katalog. Ein Leerwert bedeutet, dass keine Zuordnung zu einer P20-Anwendung erfolgt. Andernfalls wird die jeweilige BV-Rechtegruppe dieser P20-Anwendung zugeordnet. Alle in der Rechtegruppe enthaltenen „Rollen“ werden dann der hinterlegten P20-Anwendung zugeordnet und im LDAP-Export berücksichtigt (Eine BV-Rechtegruppe müsste damit eigentlich „Rollengruppe“ heißen.)

Es können mehrere Rechtegruppen derselben P20-Anwendung zugeordnet sein. Dadurch werden mehrere Gruppierungen in der BV für eine P20-Anwendung ermöglicht (z.B. bei SÜP)

Tabelle 15: AF.BV.Kern.00 „Anlage Rechtegruppe einer P20-AW“

Identifikator:	AF.BV.Oberfläche.00 „Anlage Rechtegruppe einer P20-AW“
Name:	Anlage Rechtegruppe einer P20-AW
Bereich:	BV
Auslöser:	Manueller Aufruf
Ziel:	Rechtegruppe ist nach Anlage oder Änderung genau einer oder keiner P20-Anwendung zugeordnet.
Vorbedingung:	
Ergebnis im Erfolgsfall:	
Ergebnis im Fehlerfall:	
Nachbedingung:	
	1. Anlage einer Rechtegruppe wie bisher. 2. In der Administration der Rechtegruppe wird aus dem neu einzuführenden Katalog der P20-Anwendungen das Attribut (P20-Anwendung) gesetzt. → <Leerwert>: keine Zuordnung zu einer P20-Anw. → <P20-Anwendung>: Rechtegruppe gehört zur ausgewählten P20-Anw.
	Keine
Plausibilitäten:	*Die P20-AW einer Rechtegruppe darf nicht mehr geändert werden können, weil dies erhebliche Änderungen im LDAP bedeutet.*
Häufigkeit:	*Nicht relevant*
Anwendungsfall enthält:	
Anwendungsfall erweitert:	
Anmerkungen:	
Offene Fragen:	

4.2 AF.BV.Kern.01 „vollständiger Rechteentzug beim Wechsel der Stammdienststelle eines Benutzers“

Das ist tatsächlich ein BV-interner Anwendungsfall und kein AF der Schnittstelle. Das Lösen eines Nutzers aus einer OE ist nur möglich indem er in eine neue OE gezogen wird. Hierbei verliert er (grundsätzlich) alle Rechte, ist jedoch der NEUEN OE zugewiesen.

Anmerkung:

Diesen AF gibt es bereits jetzt in der BV. Daher wird er hier in diesem Dokument nicht beschrieben.

5 Anlagen

Anlagen sind selbstverfasste, ergänzende Dokumente zum Lastenheft.

Anlage	Dokument
Anlage 1	In diesem Dokument enthalten zum Verständnis, aber ohne Relevanz für die Erstellung der SNIT ITK-BV-TN-LDAP (Abschnitt 5.1 s. u.)
Anlage 2	n.a.
Anlage 3	Lösungsskizze nach Erstbewertung der Version: ANF-1031 Lastenheft_BV_LDAP_PLX_00.00.06 durch ITK-Entwicklung (Abschnitt 5.2 s. u.)
Anlage 4	Vorlage zur groben Aufwandschätzung (Abschnitt 5.3 s. u.)
Anlage 5	CSV-Datei zur Definition der Rollen-Funktionsrechte-Verschachtelung AW-Bsp_Rollenzuschnitt_00-00-01.csv

5.1 Anlage 1 (PLX-Spezifika)

(PLX) Benutzer	***Bemerkung***	***Allgemein***
Login	Hauptsuchkriterium für Benutzer bei der Anmeldung, daher Empfehlung: sAMAccountName	
Vorname		Die aus dem AD ermittelten Attributwerte des (AD) Users müssen die Werte für dem (PLX) Benutzer lediglich enthalten und nicht exakt übereinstimmen. Wichtig ist jedoch, dass die Werte eindeutig ermittelbar sind. So können Einwahl und Durchwahl im gleichen (AD) Attribut hinterlegt sein, es muss nur definiert sein, wie die Trennung der Bestandteile erfolgt. Die Selektion eines (PLX) Benutzer-Attributes aus einem (AD) User-Attribut erfolgt per regulärem Ausdruck.
Name		
MailAdresse		
Einwahl	Allgemeine Amtseinwahl, z.B. 030/4664, die externe Telefonnummer wird aus Einwahl und Durchwahl zusammengesetzt.	
Durchwahl	Hausinterne Durchwahl des Mitarbeiters, die externe Telefonnummer wird aus Einwahl und Durchwahl zusammengesetzt. Frage: Wenn es keine Einwahl gibt, also Einwahl eine leere Zeichenkette ist, wäre dann die Durchwahl gleich der hausinternen Durchwahl?	
Fax		
Amtsbezeichnung	Der Wert muss gemäß Katalog KAT_Amtsbezeichnung Spalte „Amtsbezeichnung kurz“ vergeben werden.	
Fachaufsichtsgrad	Zulässige Werte „hart“ oder „weich“	
Zimmernummer		
Dienstgruppe	Eindeutiger Name der Dienstgruppe des Benutzers innerhalb seiner Stammdienststelle	

5.2 Anlage 3 (Lösungsskizze nach Erstbewertung ANF-1031 Lastenheft_BV_LDAP_PLX_00.00.06)

- P20-Anwendung / BV-Rechtegruppen:
  - In der BV wird ein Katalog der P20-Anwendungen inkl. eines Leerwertes eingeführt.
  - Jede Rechtegruppe der BV bekommt ein Attribut mit diesem Katalog.
    - Leerwert bedeutet keine Zuordnung zu einer P20-Anwwendung
    - Ansonsten wird die jeweilige BV-Rechtegruppe dieser P20-Anwendung zugeordnet
  - Alle in der Rechtegruppe enthaltenen „Rollen“ werden dann der hinterlegten P20-Anwendung zugeordnet und im LDAP-Export berücksichtigt
    - Eine BV-Rechtegruppe müsste damit eigentlich „Rollengruppe“ heißen
    - Es können mehrere Rechtegruppen derselben P20-Anwendung zugeordnet sein. Dadurch werden mehrere Gruppierungen in der BV für eine P20-Anwendung ermöglicht (z.B. bei SÜP)
- Die BV (das Kern-Produkt) berücksichtigt bzgl. des LDAP-Exportes zunächst nur die allgemeinen Anwendungsfälle:
  - Ein Anwender wird berechtigt
    - Ggf. Neuanlage im LDAP
  - Ein Anwender verliert eine BV-Rolle
  - Daten eines Anwenders ändern sich
    - Ggf. Änderung einer OE
  - BV-Rolle wird gelöscht
    - Impliziter Entzug aller vergebenen BV-Rollen
- Alle Anwendungsfälle, welche sich spezifisch auf das LDAP-Verzeichnis beziehen, werden **nicht** in der BV realisiert:
  - Konsistenzprüfung
  - Vollständiger Neu-Aufbau (Vollexport mit vorheriger Leerung)
  - Neu-Aufbau einer P-20Anwendung bzw. des Rollenzuschnitts
- Treten bei einem dieser Abläufe Fehler auf, muss ein Admin unmittelbar eingreifen. Im worst case, wurden alle User und/oder Rollen im LDAP erfolgreich gelöscht und die Neuanlage läuft auf einen Fehler. Dann existieren keine Daten im User/Berechtigungen im LDAP und in den jeweiligen Anwendungen kann kein Anwender mehr arbeiten.
  Eine solche Aktion darf u.E. daher nur ein Admin ausführen, welcher ggf. auch sofort korrigierend eingreifen kann.
- Der AF zur Vergabe einer Rolle, beschreibt bereits jetzt, dass im Falle einer fehlenden P-20 Anwendung oder der Rollen-Gruppe im LDAP, der Export auf einen Fehler laufen soll. Dies zeigt bzw. bestätigt die Trennung der Standard AF der BV von der Basis-Konfiguration des LDAP (Basisstruktur, P20-Anwendungen, Rollen und Funktionsrechte). Diese Basisstrukturen können z.B. bei einem SCIMv2 anders aussehen und andere Daten+Abläufe benötigen. Dies muss in der Schnittstelle und nicht der Kern-BV abgebildet werden.

5.3 Anlage 4 (Vorlage zur groben Aufwandschätzung)

Arbeitspaket	**Aufwand (PT)**
Abstimmungen und Aufbau der Entwicklungsumgebung (BV, LDAP usw.)	
BV-Erweiterungen - Rechtegruppen mit P20-AW (darf nicht mehr änderbar sein!) - Neue Attribute (z.B. Fachaufsichtsgrad) - Pflegemaske für Katalog *AF.BV.Kern.00 „Anlage Rechtegruppe einer P20-AW“*	
Einrichten einer Kopie des LDAP-Exportes	
DB-Export (alle P20-Rechtegruppen, Attribute usw.)	
Anlage/Aktualisierung eines AW - Prüfung bisheriger Code (User-Objekt) - Prüfung/Anlage OE-Gruppe - Anpassung Gruppenmitgliedschaft (alt weg, neu vergeben) *AF.BV.P20-AW.00 „Übertragung eines P20-Benutzers mit Nutzerinformationen in TN-P20-LDAP“* *AF.BV.P20-AW.01 „Änderung Nutzereigenschaften eines P20-Benutzers“*	

Rechtevergabe/-Entzug
- Entfernen aus Intermediate-Gruppe
- Löschung leerer Intermediate-Gruppe
- Prüfung & Anlage neuer OE- und I-Gruppe
- Aufnahme in Gruppen
  ○ Intermediate in OE
  ○ Intermediate in Rolle
  ○ User in Intermediate
  ○ User in „Zugriff“ (P20-AW)
AF.BV.P20-AW.02 „Rechte-Entzug einzeln“
AF.BV.P20-AW.03 „Entfernen der OE-Zugehörigkeit eines Benutzers“
AF.BV.P20-AW.04 „Recht/Rolle wird in der BV einer OE entzogen“
AF.BV.P20-AW.05 „OE wird in der BV gelöscht“
AF.BV.P20-AW.06 „Recht/Rolle einer P20-AW-Rechtegruppe wird gelöscht“	

Tool: Komplette Löschung der Bewegungsdaten (alle Anwenderkonten und P20-AW) *AF.BV.Admin-Tool.00 „Initialer P20-Voll-Export nach LDAP“*	
Tool: Konsistenzprüfung - Auslesen aller P20-Rechtegruppen inkl. enthaltener BV-Rechte aus BV - Abgleich BV-Daten mit Basisstruktur in LDAP (alle P20-AW und Rollen vorhanden) *AF.BV.Admin-Tool.01 „Konsistenzprüfung Rechte/Rollen“*	
Tool: Import P20-AW/Rollen/Funktionsrechte	

- Import und kompletter Neuaufbau einer P20-Struktur ○ CSV - Option zum Löschen der kompletten P20-AW (AF2). Ansonsten nur Abgleich (AF4+5) - Anlage P20- AW inkl. Basisgruppe „Zugriff“ - Anlage der Rollen - Anlage der Funktionsrechte und Mitgliedschaften in Rollengruppen Danach durch separate Funktionen die Konsistenzprüfung und den Full-Export auslösen (Admin!) Hinweis: Seitens der Entwicklung möchten wir für Admins keine komplexen Abläufe/Prozesse realisieren, sondern Werkzeuge an die Hand geben. Damit kann man flexibler agieren und auch unerwartete Situationen besser lösen, als mit vordefinierten mehrstufigen Prozessen. *AF.BV.Admin-Tool.02 „Initiale Anlage Rollen+Funktionsrechte für eine P20-Anwendung“* *AF.BV.Admin-Tool.04 „Änderung von Funktionsrechtezuordnungen in Rollen“* *AF.BV.Admin-Tool.05 „Neuanlage einer Rolle mit Funktionsrechten“*	
Voll-Export für eine spezifische P20-AW *AF.BV.Admin-Tool.03 „Initialer Vollexport für eine P20-Anwendung“*	
Dokumentation	
Testunterstützung	

5.4 Anlage 5 CSV-Datei zur Definition der Rollen-Funktionsrechte-Verschachtelung

Tabelle 16: Auszug aus Bsp-CSV-Datei Rollenzuschnitt

Anwen-dungs-name	Rollenname	Objekttyp	Zugriffsfunktion
P20-AW-1	RL_iVBS-Bearbeiter	Funktionsberechtigungen	grundrecht
P20-AW-1	RL_iVBS-Bearbeiter	Funktionsberechtigungen	objekte_loeschen_aktiver_vorgang
P20-AW-1	RL_iVBS-Bearbeiter	Funktionsberechtigungen	vorgang_oeffnen
P20-AW-1	RL_iVBS-Bearbeiter	Funktionsberechtigungen	vorgangsliste_ansehen
P20-AW-1	RL_iVBS-Bearbeiter	Funktionsberechtigungen	vorgangsliste3_ansehen
P20-AW-1	RL_iVBS-Bearbeiter	Funktionsberechtigungen	zuarbeit_abschliessen
P20-AW-1	AB_Allgemein	Aufgabenbereich	Ordnungswidrigkeit
P20-AW-1	AB_Allgemein	Aufgabenbereich	Verkehrsunfall
P20-AW-1	AB_Allgemein	Aufgabenbereich	Gefahrenabwehr
P20-AW-1	AB_Tötungsdelikte	Aufgabenbereich	Tötungsdelikte
P20-AW-1	AB_Sexualdelikte	Aufgabenbereich	Sexualdelikte
P20-AW-1	AB_Verkehrsunfall	Aufgabenbereich	Verkehrsunfall
P20-AW-1	SB_Staatsschutz	Schutzbereich	Staatsschutz
P20-AW-1	SB_OK	Schutzbereich	OrganisierteKriminalität
P20-AW-1	SB_WiKri	Schutzbereich	WiKri
P20-AW-1	Vertretung	Marker	Vertretung

Spalten-Legende:

Nr.	Spalten-name	SNIT-relev.	Bedeutung
1	**Anwen-dungs-name**	**ja**	Ist der Bezeichner der P20-Anwendung, der verwendet wird für: 1. Bezeichnung der Anwendung im TN-P20-LDAP unterhalb von ou=P20-Anwendungen |__ ou=***<Anwendungsname>*** 2. Die manuelle Anlage der zu dieser Anwendung korrespondierenden Rechtegruppe in der BV sollte exakt den gleichen Namen haben, da mit dem Namen der Rechtegruppe bei Änderungen im TN-P20-LDAP nach dem korrekten Anwendungszweig gesucht wird.

Nr.	Spalten-name	SNIT-relev.	Bedeutung
2	**Rollen-name**	**ja**	Ist der Bezeichner einer Rolle, mit dem 1. im TN-P20-LDAP Rollen angelegt werden ou=P20-Anwendungen |__ou=<*Anwendungsname*> |__… |__… |__ou=Rollen |__ou=Benutzer-Rollen |__cn=***<Anwendungsname>|<Rollenname>*** /* Objekttyp = „Funktionsberechtigungen“*/ |__ou=Aufgabenbereiche |__cn=***<Anwendungsname>|<Rollenname>*** /* Objekttyp = „Aufgabenbereich“*/ |__ou=Schutzbereiche |__cn=***<Anwendungsname>|<Rollenname>*** /* Objekttyp = „Schutzbereich“*/ |__ou=Marker |__cn=***<Anwendungsname>|<Rollenname>*** /* Objekttyp = „Marker“*/ 2. in der BV in der korrespondierenden Rechtegruppe die vergebbaren Rollen/Rechte angelegt werden müssen. Die manuell angelegten Rollen/Rechte in der korrespondierenden Rechtegruppe in der BV sollten jeweils exakt den gleichen Namen haben, da mit diesen Namen der Rollen bei Eintragung/Änderung/Löschung von Berechtigungen im TN-P20-LDAP „operiert“ wird.

Nr.	Spalten-name	SNIT-relev.	Bedeutung
3	**Objekttyp**	~~nein~~ **ja**	Die Spalte **Objekttyp** muss nun durch das BV-Admin-Tool beim Einlesen interpretiert werden. Bislang diente sie nur als Hilfsspalte zur Verwaltung der Erstellung und Änderung der csv-Datei durch den Administrator. Dieser Objekttyp muss nun als typisierendes Merkmal an der Rolle in der BV vermerkt werden und dient beim Export über die SNIT-LDAP zur Unterscheidung der jeweiligen Ablage im LDAP-Verzeichnis. Folgende Bezeichner für Objekttypen sind in der csv-Datei zulässig: 1. „Funktionsberechtigungen“ 2. „Aufgabenbereich“ 3. „Schutzbereich“ 4. „Marker“ ~~Hierbei handelt es sich ausschließlich um eine Hilfsspalte zur Verwaltung der Erstellung und Änderung der csv-Datei für den Administrator.~~ ~~Hintergrund – Rollen fassen Zugriffsfunktionen unterschiedlichen Typs der Spalte 4 zusammen bspw. unterscheidet PLX:~~ ~~1. Funktionsberechtigungen (Rolle beginnt mit <RL_*>)~~ ~~2. Aufgabenbereich (Rolle beginnt mit <AB_*>)~~ ~~3. Schutzbereich (Rolle beginnt mit <SB_*>)~~ ~~Anhand dieses Namen-prefixes kann eine Zielanwendung Rollen-Inhalte (Inhaltstypen) unterscheiden und entsprechend weiterverarbeiten.~~
4	**Zugriffs-funktion**	**ja**	Ist der Bezeichner einer Zugriffsfunktion, die initial im TN-P20-LDAP angelegt und entsprechend des Rollenzuschnitts mit Rollen durch Gruppenmitgliedschaft verbunden werden. 1. im TN-P20-LDAP Rollen angelegt werden ou=P20-Anwendungen |__ou=<*Anwendungsname*> |__… |__ou=Funktionsrechte |__ cn=***<Zugriffsfunktion>*** |__... |__...

Umfassende Beispieldatei:
AW-Bsp_Rollenzuschnitt_00-00-01.csv

6 Referenzen

Referenzen sind NICHT selbstverfasste, ergänzende Dokumente zum Lastenheft.

Referenz	Dokument