

@rtus-VBS



KONZEPT

Nutzer und Berechtigungsverwaltung über P20 IAM

Zusammenfassung

Das Fachkonzept beschreibt die Anbindung von dem iVBS @rtus an die Nutzer- und Berechtigungsverwaltung von P20 F-IAM.

FAG IAM Provisionierung @rtus-Kooperation, Jan RÜth

Stand Datum	24.07.2024
Version	1.0
Konzeptverantwortlich	
Status	Abgestimmt
Jira-Ticketnummer	

Beteiligte Akteure

Rolle	Name	Organisation
Weitere Konzeption	Jan R��th	Dataport
Verantwortlich Formulare	-	-
Verantwortlich Kataloge	-	-
Verantwortlich Dataport	Jan R��th Matthias Oppermann	Dataport
Verantwortlich Fachlichkeit @rtus	Maren Tietgen (SH)	Dataport
Fachlichkeit extern	Alberto Blinckmann (HH) Denis V��lkers (HH) Torben Busse (HB) Carsten Bauck (NI) Jens H��upl (AN) Thomas Reiser (AN) Matthias Voltmer (SL) Christian Grim (SL) Paul Klemm (RP) Christian Schwan (RP) Moritz Rubel (RP) Thomas M��ller (BPOL) Grischa Wilke (BPOL)	
Weitere	Fachbereiche der Teilnehmer im Kontext Identity & Access Management	

Dokumentenhistorie/Änderungsnachweis				
Von	Kapitel	Grund für Zustandsübergang/ Änderungsnachweis	Version	Datum
Jan RÜth		Initiale Erstellung	0.2	12.01.2024
Jan RÜth	3.x	Anpassung nach interner Rückmeldung Patrick Stellmann PG IAM - Aufnahme [ANF-032] Lesende Zugriffe für F-IAM - Offene Punkte aus Operationen GET und PATCH entfernt - Beispiel angepasst unter Berücksichtigung von SCIM bei Telefonnummer, Email und Fax - Lösungsansatz zu 3.1 „[Stufe 2b] Verwaltung von Organisationseinheiten / Dienststellen klarer formuliert.	0.3	
Maren Tietgen	2.4	Aktualisierung Abb. 6 Stufen RP/SL	0.4	18.03.2024
Maren Tietgen Jan RÜth	2.3 3.1, 3.4 4.x	Anmerkungen und Antworten BPOL aufgenommen. Überarbeitung Abschnitt 2.3 mit Aufnahme Screenshots zur Rollenverwaltung. Überarbeitung Abschnitt 3.1 und 3.4 bezüglich neuer Vorgaben durch Spezifikation PG IAM (siehe A1.1). Anpassung der Szenarien in Bezug auf Aktionen bezüglich der neuen Vorgaben. Aufnahme Anmerkungen SL und AN. Erledigte Kommentare und Anmerkungen entfernt	0.4.2	25.03.2024
Maren Tietgen Jan RÜth	1.2 4.x	Anmerkungen und Rückmeldungen der Teilnehmer übernommen. Ergänzungen und Konkretisierungen an den Anforderungen auf Basis der gemeinsamen Sichtung und Diskussion in der FAG.	0.4.4 0.4.5	04.05.2024 bis 19.04.2024
Jan RÜth	Titel Gesamtes Dokument	Erstellung Zwischenversion (Abschnitte 1-4) zur finalen Abstimmung durch die FAG Teilnehmer bis Ziel 03.05.2024. Beteiligte Akteure eingetragen. Änderungen übernommen und erledigte Anmerkungen entfernt. Ausfüllhinweise aus Dokument entfernt.	0.5	19.04.2024
Jan RÜth	3.6 1.2, 4.16, 4.17 5-12 14, 15 16.4	[Stufe 2a] Vorgehen bei der Transition von interner auf externer Provisionierung für Bestandskunden Anforderung [ANF-032] und [ANF-033] für Lesende Zugriffe auf IAM ergänzt Initiale Erstellung vom Abschnitt 5-12 zur Umsetzung Glossar eingefügt, Links in Anlagen ergänzt Neues Todo Dataport: Spezifikation und Beschreibung für GET bei OE-Permission fehlt Abbildungsverzeichnis eingefügt	0.6	24.05.2024
Maren Tietgen Matthias Oppermann Jan RÜth		Review der Änderungen und Ergänzung der Version 0.6. Einarbeitung der Korrekturen und Ergänzungen. Korrekturen zur Rechtschreibung wurden ohne Änderungsmodus direkt übernommen, auch in finalen Abschnitten 1 bis 4. Inhaltliche Ergänzungen oder Umformulierungen wurden hingegen im Änderungsmodus durchgeführt.	0.7	11.06.2024
Jan RÜth	8.1, 4.13, 4.14 16.5	Anpassung nach FAG Workshop 19.06.2024 und Änderungen 0.7 übernommen Verständlichkeit „@rtus-Admin Anwenderverwaltung“ verbessert Neuer offener Punkt zur Nachverfolgung: „Hinterfragen der Asynchrone Verarbeitung schreibender Nachrichten“	0.8	19.06.2024

Jan R��th		Finaler Kandidat f��r 1.0 nach FAG Termin am 04.07.2024 Erl��uternde Anmerkung nach R��ckmeldung RP bei Recherche und Mobile eingef��gt.	0.9 0.9.1	17.07.2024
Maren Tietgen		Hebung auf finaler 1.0 nach Zustimmung aller Teilnehmer	1.0	19.07.2024

INHALTSVERZEICHNIS

1	PROBLEMBESCHREIBUNG	8
1.1	<i>Vorwort</i>	8
1.2	<i>Einleitung und Problemstellung</i>	8
2	ABHÄNGIGKEITEN / RAHMENBEDINGUNGEN	10
2.1	<i>Übersicht Objekt: Anwender</i>	10
2.2	<i>Übersicht Objekt: Dienststelle</i>	13
2.3	<i>Übersicht Objekt: Rollen- und Funktionsberechtigung</i>	16
2.4	<i>Planungsübersicht und stufiges Vorgehen</i>	18
2.5	<i>Übersicht „P20 F-IAM“ Benutzerverwaltung</i>	18
2.6	<i>Übersicht über SCIMv2 (Schnittstellen F-IAM)</i>	20
3	LÖSUNGSANSATZ	22
3.1	<i>[Stufe 2b] Verwaltung von Organisationseinheiten / Dienststellen</i>	22
3.2	<i>[Stufe 2a] Verwaltung von Anwendern</i>	23
3.3	<i>[Stufe 2b] Verwaltung Dienststellenzugehörigkeiten</i>	27
3.4	<i>[Stufe 2b] Verwaltung von Berechtigungen</i>	27
3.5	<i>[Stufe 2a] Protokollierung und Nachvollziehbarkeit</i>	32
3.6	<i>[Stufe 2a] Vorgehen bei der Transition von interner auf externer Provisionierung für Bestandskunden</i>	33
4	ANFORDERUNG	35
4.1	<i>[ANF-001][Stufe 2a] Anlage neuer Dienststellen</i>	35
4.2	<i>[ANF-002] [Stufe 2b] Pflege und Aktualisierung der Dienststellenstammdaten</i>	35
4.3	<i>[ANF-003] [Stufe 2b] Deaktivierung (Löschung) von Dienststellen</i>	36
4.4	<i>[ANF-010] [Stufe 2a] Anlage neuer Anwender</i>	36
4.5	<i>[ANF-011] [Stufe 2a] Deaktivierung (logische Löschung) von Anwendern</i>	37
4.6	<i>[ANF-012] [Stufe 2a] Pflege und Aktualisierung der Anwenderstammdaten</i>	40

4.7	[ANF-020] [Stufe 2b] Zuordnung von Anwender zu Dienststelle	41
4.8	[ANF-021] [Stufe 2b] Löschung einer Zuordnung von Anwender zu Dienststelle	44
4.9	[ANF-022] [Stufe 2b] Setzen von Berechtigungen auf Dienststellenebene	44
4.10	[ANF-023] [Stufe 2b] Löschen von Berechtigungen auf Dienststellenebene	45
4.11	[ANF-024] [Stufe 2a] Sperrung von Anwendern auf Dienststellen	45
4.12	[ANF-025] [Stufe 2a] Globale Sperrung von Anwender in @rtus	46
4.13	[ANF-030] [Stufe 2a] Deaktivierung der internen Benutzerverwaltung für externe Provisionierung	47
4.14	[ANF-030] [Stufe 2b] Deaktivierung der internen Benutzerverwaltung für externe Provisionierung	48
4.15	[ANF-031] [Stufe 2a] Protokollierung und Nachvollziehbarkeit	49
4.16	[ANF-032] Lesende Zugriffe für F-IAM: Abfrage von Benutzerdaten	50
4.17	[ANF-033] Lesende Zugriffe für F-IAM: Abfrage von VBS-Rechten	51
5	UMSETZUNG ALLGEMEIN	52
5.1	Technische Komponentenübersicht	52
6	UMSETZUNG DATENMODELL UND SCHNITTSTELLE	54
6.1	Entität/Fachobjekt „IAMNachricht“	54
6.2	Webservice „SCIMv2-REST-Service“	55
6.3	JMX-Dienst „IAMExecuterService“	57
6.4	Komponente „IAMUsecaseExecuter“	58
6.5	JMX-Dienst „IAMProtocolService“	58
6.6	JMX-Dienst „IAMLoeschenService“	58
7	UMSETZUNG VBS	59
7.1	[ANF-030] [Stufe 2a][Stufe 2b] - Umsetzung VBS-Client	59
8	UMSETZUNG @RTUS-ADMIN	59
8.1	[ANF-030] [Stufe 2a][Stufe 2b] - Umsetzung Admin-Client	59
8.2	[ANF-031] [ANF-031][Stufe 2a] Protokollierung und Nachvollziehbarkeit	60

9	UMSETZUNG @RTUS-RECHERCHE.....	61
10	UMSETZUNG @RTUS-MOBILE	61
11	UMSETZUNG KATALOGE	61
12	UMSETZUNG FORMULARE	61
13	HINWEISE ZUR ABNAHME	61
14	GLOSSAR THEMA IAM.....	62
15	ANLAGEN.....	62
16	SAMMLUNG OFFENE PUNKTE.....	63
16.1	<i>Todo: Dataport: Verfolgung Aufnahme „Dienstgrad“ in SCIMv2 IAM</i>	63
16.2	<i>Todo: Dataport: Platzierung Thema „Rechte nur auf spezifischen Dienststellen gültig“</i>	64
16.3	<i>Todo: Dataport: Platzierung Thema „Recht nur einmal pro Dienststelle zu vergeben“</i>	64
16.4	<i>Todo: Dataport: Spezifikation und Beschreibung für GET bei OE-Permission fehlt</i>	65
16.5	<i>Todo: Dataport: Hinterfragen der asynchronen Verarbeitung schreibender Nachrichten</i>	65

ABBILDUNGSVERZEICHNIS

Abbildung 1: @rtus-Client: Anwenderverwaltung Maske Anwenderdaten.....	11
Abbildung 2: @rtus-Client: Anwenderverwaltung Maske Anwenderberechtigungen	11
Abbildung 3: @rtus-Admin Maske Anwender Bearbeiten	12
Abbildung 4: @rtus-Admin Maske Dienststellenverwaltung	14
Abbildung 5: @rtus-Admin Maske Dienststellenverwaltung Dienststellen-Status.....	15
Abbildung 6: Rollenverwaltung in @rtus-Admin.....	17
Abbildung 7: Rollenansicht und -bearbeitung in @rtus-Admin	17
Abbildung 8: Ausbaustufen Anbindung Artus (Quelle Workshop 06.12.23 KTT/BKA/RP/SL/Dataport)	18
Abbildung 9: Schematische Darstellung interne Benutzerverwaltung ohne externe Provisionierung	19
Abbildung 10: Provisionierung über F-IAM von P20	20
Abbildung 11: Beispiel für eine Antwort auf Abfrage User mit Rollen von @rtus.....	30
Abbildung 12: Beispiel PATCH-Operation mit Vergabe SB-Rolle auf einer Dienststelle.....	32
Abbildung 13: Technische Komponentenübersicht	52
Abbildung 14: Kurzbeschreibung der Umsetzungskomponenten.....	54
Abbildung 15: Übersicht neues Fachobjekt IAMNachricht	55
Abbildung 16: Gegenüberstellung SCIMv2-Endpunkte, Anforderungen und Umsetzung	57
Abbildung 17: Neue Konfigurationswerte für Anwenderverwaltung.....	59
Abbildung 18: Neue Konfigurationswerte für @rtus-Admin	60

1 Problembeschreibung

1.1 Vorwort

Dieses Dokument beschreibt die fachlichen und die zentralen technischen Anforderungen für den CR IAM Stufe 2 Provisionierung (siehe Anlage A7). Es beschreibt die Umsetzung und legt damit auch die fachlichen Geschäftsprozesse für die externe Provisionierung von Anwendern, Dienststellen und Benutzerrechten durch das Identity- & Access-Management (IAM) von P20 fest.

Die nachfolgenden Sachverhalte, Themenkomplexe und Begriffe haben teilweise eine hohe Komplexität. Aus Gründen der leichten Lesbarkeit wird in dieses Dokument die „gewohnte“ männliche Sprachform bei personenbezogenen Substantiven und Pronomen verwendet. Dies impliziert jedoch keine Benachteiligung des weiblichen Geschlechts oder intergeschlechtlicher Personen, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen sein.

1.2 Einleitung und Problemstellung

Dieses Konzept ist die Lösungs- und Umsetzungsbeschreibung für den CR IAM Stufe 2 (siehe Anlage A7). In Jira wird dieses als Initiative mit ART-29582 „CR IAM Stufe 2 Provisionierung“ geführt.

Mit dem CR IAM Stufe 1 haben wir für @rtus die Authentifizierung der Anwender über P20 F-IAM umgesetzt. Als iVBS sind wir aber verpflichtet, nicht nur die Authentifizierung über das P20 F-IAM durchzuführen, sondern auch die gesamte Berechtigung der Anwender in @rtus ausschließlich über das F-IAM durchzuführen. Für SL und RP ist diese Anforderung als Voraussetzung für die Inbetriebnahme von @rtus eingestuft worden. Für HH ist dieses ebenfalls von zentraler Bedeutung, da HH bereits heute eine automatisierte Provisionierung von VBS Comvor durchführt. Allerdings sind perspektivisch alle Bestandsteilnehmer verpflichtet, auf die Provisionierung von F-IAM umzustellen. Aufgrund der hohen Priorität für den Wirkbetrieb von SL und RP, muss das Thema in der 10.x umgesetzt und für einen Wirkbetrieb 01.01.2025 bereitgestellt und deshalb zeitnah konzeptioniert werden.

Im Zielbild von P20 sollen Fachanwendungen Informationen bezüglich Anwender, Organisationseinheiten, deren Zuordnungsstruktur zueinander sowie die Berechtigungen der Anwender in Bezug auf IT-Anwendungen aus dem zentralen F-IAM beziehen (A1). Dieser Vorgang wird Provisionierung genannt. Diese Informationen der Teilnehmer werden wiederum von den jeweiligen Teilnehmern in das P20 F-IAM eingepflegt, idealerweise vollautomatisiert über die jeweiligen Teilnehmer IAM's bzw. deren teilnehmerspezifische Benutzerverwaltungen. Wie dieses konkret umgesetzt wird, spielt für das iVBS als Fachverfahren keine Rolle.

@rtus verfügt nach heutigem Sachstand über eine reine interne Benutzerverwaltung. Zur Authentifizierung der Anwender ist in der Regel ein Verzeichnisdienst (konkret ein Active Directory (AD)) angebunden. Durch den CR IAM wurde dieses um eine Authentifizierung über F-IAM erweitert, ohne an der internen Benutzerverwaltung etwas zu verändern.

Die Benutzergrunddaten werden bei der derzeitigen Benutzerverwaltung nur einmalig bei der Anlage eines neuen Anwenders aus den Verzeichnisdienst (AD oder Generic-LDAP) übernommen.

Eine weitere Pflege der Anwenderdaten sowie deren Berechtigung oder Dienststellenzugehörigkeit findet nur in @rtus statt. Diese erfolgt entweder dezentral über die Dienststellenverwaltung im VBS oder zentral über @rtus-Admin durch die @rtus-Fachdienststelle.

@rtus bietet zusätzlich eine eigene Webservice-Schnittstelle für eine externe Benutzerverwaltung an, bei der sich die wesentlichen Funktionen zur Anlage und Berechtigung von Anwendern programmatisch durchführen lassen. Diese wird durch die zentrale Berechtigungsverwaltung der BPOL und ST genutzt. Diese Nutzungsart der externen Benutzerverwaltung entspricht grundsätzlich bereits der Anforderung einer externen Provisionierung.

Auch die Organisationseinheiten (Dienststellen) werden innerhalb von @rtus über @rtus-Admin verwaltet. Die Verwaltung stützt sich da vor allem auf den @rtus-Dienststellenkatalog, der die Dienststellen und deren Struktur insgesamt vorgibt, die dann über @rtus-Admin als @rtus-Dienststelle angelegt und konfiguriert werden kann.

Für die Erreichung des Zielbildes einer zentralen Provisionierung ergeben sich somit drei notwendige Kernziele für dieses Fachkonzept, die sich jeweils in der Beschreibung der Anforderungen für eine Anbindung vom F-IAM widerspiegeln muss:

1. Dienststellenverwaltung

- a. [ANF-001] Anlage neuer Dienststellen
- b. [ANF-002] Pflege und Aktualisierung der Dienststellenstammdaten
- c. [ANF-003] Deaktivierung (Stilllegung) von Dienststellen

2. Anwenderverwaltung

- a. [ANF-010] Anlage neuer Anwender
- b. [ANF-011] Deaktivierung (logische Löschung) von Anwendern
- c. [ANF-012] Pflege und Aktualisierung der Anwenderstammdaten

3. Berechtigungsverwaltung

- a. [ANF-020] Zuordnung von Anwender zu Dienststelle
- b. [ANF-021] Löschung einer Zuordnung von Anwender zu Dienststelle
- c. [ANF-022] Setzen von Berechtigungen auf Dienststellenebene
- d. [ANF-023] Löschen von Berechtigungen auf Dienststellenebene
- e. [ANF-024] Sperrung von Anwendern auf Dienststellen
- f. [ANF-025] Globale Sperrung von Anwender in @rtus

4. Sonstige Anforderungen

- a. [ANF-030] Deaktivierung der internen Benutzerverwaltung für externe Provisionierung
- b. [ANF-031] Protokollierung und Nachvollziehbarkeit
- c. [ANF-032] Lesende Zugriffe für F-IAM: Abfrage von Benutzerdaten
- d. [ANF-033] Lesende Zugriffe für F-IAM: Abfrage von VBS-Rechten

Nicht über F-IAM abgebildet werden die Anwendungsfälle:

- Gruppenverwaltung
- Registratur
- Horizontaler Blockverbund

Diese Anwendungsfälle bleiben funktionell in den Anwendungen sowie im aktuellen Webservice erhalten, wie sie derzeit sind. Sofern die Anwendungsfälle von der oben genannten Anforderung betroffen sind, muss dieses Fachkonzept aber darauf eingehen.

Eine Herausforderung besteht darin, die vorhandene @rtus-Verwaltung und die Anforderungen durch die neue Anbindung soweit harmonisch und kompatibel zu gestalten, dass zunächst in einer Übergangszeit sowohl die vorhandene interne Verwaltung als auch die ausschließlich über externe Provisionierung vorgesehene zukünftige externe Verwaltung unterstützt wird (diese aber nicht parallel genutzt werden).

Eine weitere Herausforderung ist, dass die bisherige interne Verwaltung inkonsistente Zustände durch Plausibilisierung und Abweisung vor der Durchführung von Funktionen verhindert. Beispiel: Ein Anwender kann nicht von einer Dienststelle entfernt werden, wenn dieser noch offene Vorgänge auf der Dienststelle hat. Auch die bisherige Webservice-Schnittstelle zur internen Benutzerverwaltung (BPOL) unterliegt dieser Logik. Der Vorgang der externen Provisionierung einer IT-Anwendung durch IAM verwendet hier eine andere Vorgehensweise: Sie teilt der Fachanwendung jeweils mit, wie der aktuelle Zustand der Verwaltung aussehen muss (ggf. auch durch Deltainformationen) und erwartet unabhängig von Konsistenzen und Plausibilitäten der Fachanwendung, dass dieser Zustand möglichst hergestellt wird. Diese Vorgehensweise bedarf ganz neuer Ansätze und Prozesse für die Bearbeitung dieser Anforderungen. Der Grund für diese Vorgehensweise ist, dass letztendlich die Pflege und Datenhaltungen der Nutzerinformationen asynchron auf verteilten unterschiedlichen Systemen passiert. Jede Ablehnung von @rtus würde eine zwingende organisatorische Maßnahme zur Nachpflege und manuellen Auflösung des Problems führen.

Die PG IAM erkennt solche Inkonsistenzen entweder durch zyklischen Abgleich oder durch aktive Fehlermeldung seitens der Fachverfahren (z.B. iVBS) bei Änderungsnachrichten. Diese Inkonsistenzen werden auf Seiten von F-IAM in ein Protokoll gesammelt und werden den Teilnehmern über eine Weboberfläche zur Verfügung gestellt. Ebenfalls werden Mails an hinterlegten Postfächern der Teilnehmer als Hinweis auf Inkonsistenzen versendet.

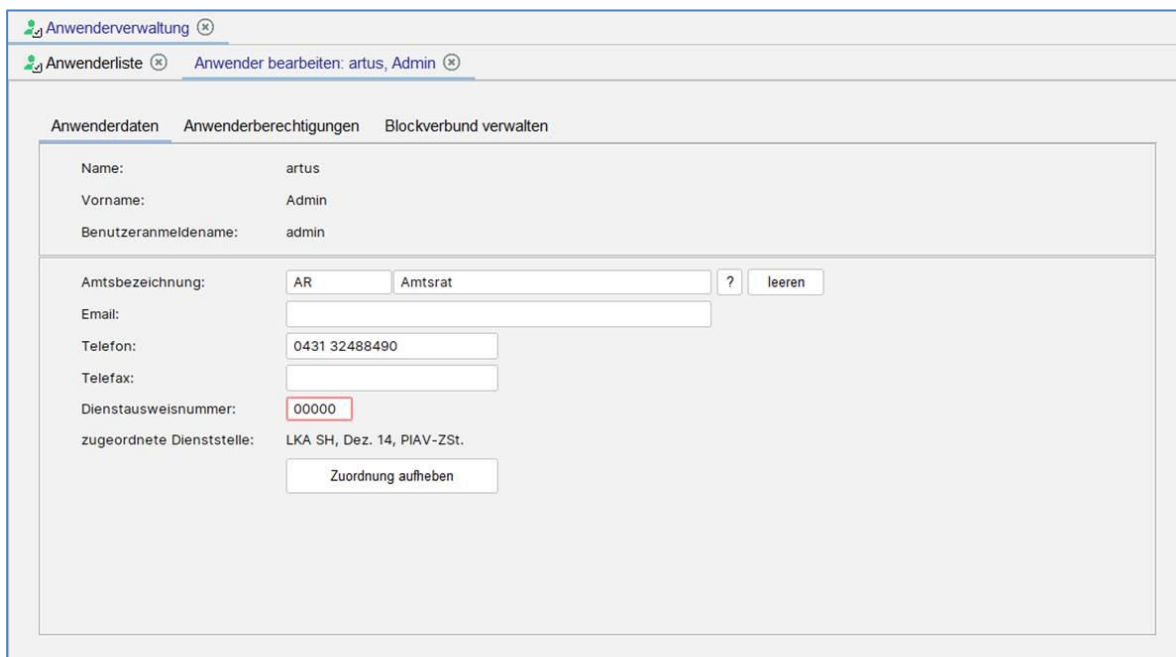
2 Abhängigkeiten / Rahmenbedingungen

Dieser Abschnitt fasst als Grundlage für die späteren lösungsorientierten Abschnitte die aktuellen Konzepte zum Thema Benutzer-, Dienststellen und Rechteverwaltung in @rtus zusammen und stellt die wesentlichen Aspekte für dieses Konzept noch einmal heraus. Des Weiteren benennt und erläutert es weitere Abhängigkeiten und Rahmenbedingungen, die für die nachfolgenden Lösungsansätze relevant sind.

2.1 Übersicht Objekt: Anwender

Dieser Abschnitt gibt eine Übersicht über das Objekt Anwender, dessen relevante Attribute und Verhalten, welches derzeit im iVBS abgebildet wird. Grundsätzlich ist vorgesehen, dieses Verhalten auch bei einer externen Provisionierung aufrechtzuerhalten. Dies erleichtert den Parallelbetrieb von interner und externer Benutzerverwaltung.

Für einen schnellen Überblick werden nachfolgend noch einmal die Masken der Anwenderverwaltung von @rtus-iVBS (dezentral genutzt von Dienststellen) und @rtus-Admin (zentral durch @rtus-Support) dargestellt. Anschließend werden Attribute noch einmal vollständig aufgezählt mit einer kurzen Beschreibung.



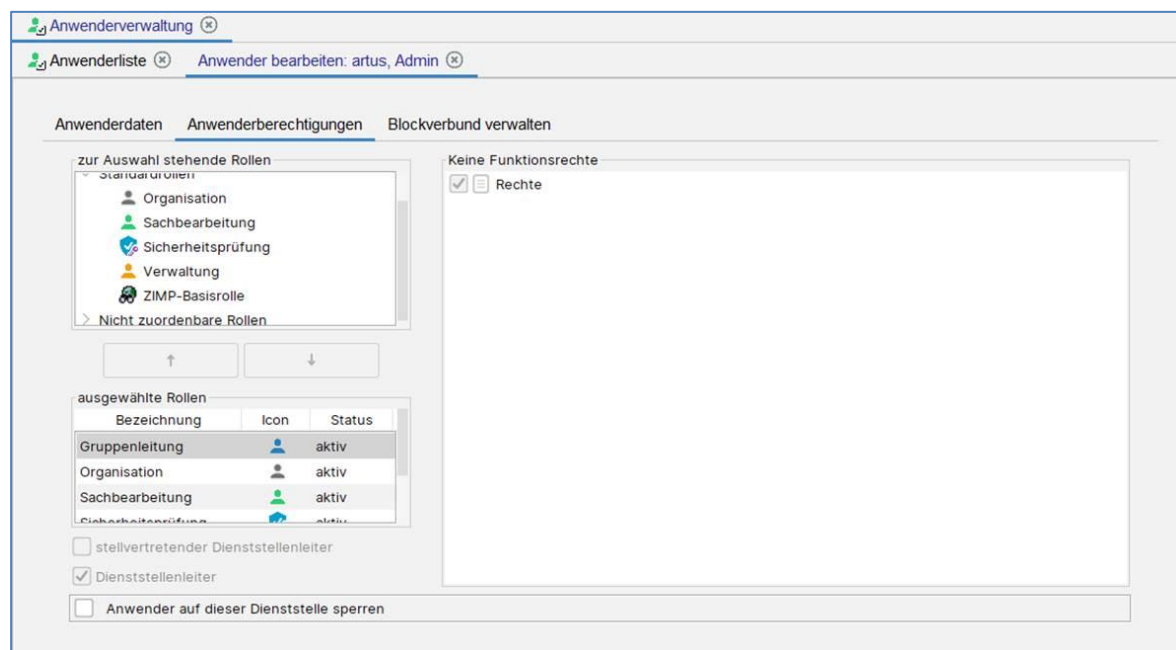
Anwenderverwaltung (X) **Anwenderliste** (X) **Anwender bearbeiten: artus, Admin** (X)

Anwenderdaten | Anwenderberechtigungen | Blockverbund verwalten

Name: artus
 Vorname: Admin
 Benutzeranmeldename: admin

Amtsbezeichnung: AR | Amtsrat | ? | leeren
 Email:
 Telefon: 0431 32488490
 Telefax:
 Dienstaussweisnummer: 00000
 zugeordnete Dienststelle: LKA SH, Dez. 14, PIAV-ZSt.
 Zuordnung aufheben

Abbildung 1: @rtus-Client: Anwenderverwaltung Maske Anwenderdaten



Anwenderverwaltung (X) **Anwenderliste** (X) **Anwender bearbeiten: artus, Admin** (X)

Anwenderdaten | **Anwenderberechtigungen** | Blockverbund verwalten

zur Auswahl stehende Rollen
 Standardrollen:
 Organisation
 Sachbearbeitung
 Sicherheitsprüfung
 Verwaltung
 ZIMP-Basisrolle
 > Nicht zuordenbare Rollen

↑ ↓


ausgewählte Rollen



Bezeichnung	Icon	Status
Gruppenleitung		aktiv
Organisation		aktiv
Sachbearbeitung		aktiv
Sicherheitsprüfung		aktiv


☐ stellvertretender Dienststellenleiter
☒ Dienststellenleiter
☐ Anwender auf dieser Dienststelle sperren

Keine Funktionsrechte
☒ Rechte

Abbildung 2: @rtus-Client: Anwenderverwaltung Maske Anwenderberechtigungen

Anwender 

Liste  Anwender: Admin artus, (00000) 

Anwender: Admin artus 

Login: Global Gesperrt: ☐ Pflege Hilfe: ☐ Priv-OZ-Berechtigungen ☐ Lesen Plus

DN:

Vorname:

Nachname:

Dienstnr.:





Email:

Telefon:



Telefax:

Datei-Berechtigungen



Datei	Recht

0 Sätze    

Blockverbunde:

Name	Berechtigung	Landesweite Berechtigung	Überschreibt Verwaltung	Überschreibt Verborgen	Teilesrecht	Anzahl Mitglieder
Zentrale Auswertung	 Lesen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		5
Datenschutz	 Lesen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		0

Dienststellen:

Beliebiges Feld  enthält 

Nummer	Kurzbezeichnung	Langbezeichnung	Gesperrt	Rollen
161030	PD Ratzeburg, STB 3	Polizeidirektion Ratzeburg, Stabsbereich 3	<input type="checkbox"/>	Dienststellenleitung
8014002	BPOLI See Neustadt in Holstein	Bundespolizeiinspektion See Neustadt in Holstein	<input type="checkbox"/>	Dienststellenleitung
105000	LPA SH	Landespolizeiamt Schleswig-Holstein	<input type="checkbox"/>	Dienststellenleitung
152400	4. PR Lübeck	4. Polizeirevier Lübeck	<input type="checkbox"/>	Dienststellenleitung
162100	PR Bad Oldesloe	Polizeirevier Bad Oldesloe	<input type="checkbox"/>	Dienststellenleitung
162050	PABR Bad Oldesloe	Polizei-Autobahn- und Bezirksrevier Bad Oldesloe	<input type="checkbox"/>	Dienststellenleitung
105140	LPA SH, Dez. 14	Landespolizeiamt, Dezernat 14, Prävention und Öffentlichkeitsarbeit	<input type="checkbox"/>	Dienststellenleitung
106234	LKA SH, SG 231	Landeskriminalamt Schleswig-Holstein, Sachgebiet 231	<input type="checkbox"/>	Dienststellenleitung
8080300	BPOLI FH Berlin-Tegel	Bundespolizeiinspektion Flughafen Berlin-Tegel	<input type="checkbox"/>	Dienststellenleitung
106215	LKA SH, SG 215	Landeskriminalamt Schleswig-Holstein, Sachgebiet 215	<input type="checkbox"/>	Dienststellenleitung
134105	PSt. Wik (stillgelegt)	Polizeistation Wik (stillgelegt)	<input type="checkbox"/>	Dienststellenleitung
04113420	Pol HB S 42	Polizei Bremen, Polizeiinspektion Regionale- und Jugendkriminalität - Besondere Eigentumskriminalität, Kfz...	<input type="checkbox"/>	Dienststellenleitung
145922	KPSt. Eckernförde, SG 2	Kriminalpolizeistelle Eckernförde, Sachgebiet 2	<input type="checkbox"/>	Dienststellenleitung
134302	PSt. Hassee	Polizeistation Hassee	<input type="checkbox"/>	Stellv. Dienststellenleitung
134001	PD Kiel, StSt	Polizeidirektion Kiel, Stabsstelle	<input type="checkbox"/>	Dienststellenleitung
105101	LPA SH 10	Landespolizeiamt, Abteilung 1, Führungsstelle	<input type="checkbox"/>	Dienststellenleitung











 OK  Speichern  Schließen  Aktualisieren  Dienststelle hinzufügen  Zuordnung aufheben  global Sperren  Deaktivieren  Hilfe/Hilfe aktivieren 

Abbildung 3: @rtus-Admin Maske Anwender Bearbeiten

Attribut	Typ	Beschreibung
Login/Benutzeranmeldename	1..1, String 200	Login Zeichenkette aus dem AD oder F-IAM. Entspricht im AD den smAccountName. Muss eindeutig sein.
DN	0..1, String 200	DN-Zeichenkette, vollqualifiziert aus dem Verzeichnisdienst. Wird automatisch gepflegt bei Nutzung eines AD.
UID	0..1, String 200	P20 UID aus F-IAM, wenn vorhanden.
Vorname	1..1, String 200	Vorname
Name	1..1, String 200	Nachname
Email	0..1, String 200	Emailadresse
Telefon	0..1, String 200	Telefonnummer
Telefax	0..1, String 200	Telefaxnummer
Deaktiviert	0..1, Boolean	Wenn deaktiviert (1), gilt der Anwender in @rtus wie gelöscht und wird nur noch historisch für Bestandsvorgänge angezeigt.

Global Gesperrt	0..1, Boolean	Wenn gesperrt (1), kann sich der Anwender nicht mehr an einer @rtus-Anwendung anmelden.
Anwender auf Dienststelle sperren.	0..1, Boolean	Wenn für eine Dienststelle aktiviert (1), kann sich der Anwender auf dieser Dienststelle nicht mehr anmelden. Seine Einstellung und Berechtigung auf dieser Dienststelle bleiben davon unberührt. Erfordert im Kontext die betroffene Dienststelle.
Dienstgrad	0..1, String 200 / Katalog?	

2.2 Übersicht Objekt: Dienststelle

Dieser Abschnitt liefert eine Übersicht über das Fachobjekt der @rtus-Dienststelle. Nachfolgend wird als Überblick die Maske der Dienststellenverwaltung von @rtus-Admin aufgeführt und anschließend die wesentlichen derzeitigen Plausibilitäten und Eigenschaften der Dienststelle dargestellt. Auch hier gilt, dass diese möglichst weitgehend erhalten bleiben sollen, ob ein Parallelbetrieb einer internen und externen Benutzerverwaltung für eine Übergangszeit zu erleichtern.

Anwender
Dienststelle

Liste
Dienststelle: LKA SH, SG 202

Dienststelle: LKA SH, SG 202

XD-Nummer:	106244	Gültig (Katalog):	
Bezeichnung:	Landeskriminalamt Schleswig-Holstein, Sachgebiet 2C	Status:	aktiv
Kurzbezeichnung:	LKA SH, SG 202	Verantw. Nachfolger:	
Strasse:	PZE, Mühlenweg 166	Anzahl Anwender:	17
Ort:	24116 Kiel	Anzahl Gruppen:	7
Telefon:	0431-160-42410	Anzahl Vorgänge:	2177
Fax:	0431-988-6-440241	Anzahl offener Vorgänge:	1850
Leiter:	Admin artus, (00000)	Anzahl Übergaben:	55
Stellvertreter:	Arne Wittmuess, (0005) Dirk Willecke, (0008)		

EKA
VU-Statistik
Aufzeichnung
SiP
PIAV
Weitere Module

KA-Protokoll-Verbergen	<input type="checkbox"/>	DST-INPOL-Name	
Zugriff gesperrte KA-Dokumente	<input type="checkbox"/>	Zugriff gesperrte KA-Aufzeichnungen	<input type="checkbox"/>
Merkblätterstellung erlaubt	<input type="checkbox"/> Für alle Dienststellen global aktiviert.		
KAH-Dienststelle	<input type="checkbox"/>	INPOL-G07-Terminalkennung	
KA-CC-Mail-Adresse		KA-Mail-Adressen	
KA-Unterrichtung-Mail-Adresse			

OK
Speichern
Schließen
Aktualisieren
ortsbez. Suche
Status ändern
Optionen
umbenennen
Berechtigungen

Abbildung 4: @rtus-Admin Maske Dienststellenverwaltung

Anwender Dienststelle

Liste Dienststelle: LKA SH, SG 202

Dienststelle: LKA SH, SG 202 Dienststellen-Status

Die ausgewählte Dienststelle ist aktiv

- ☒ weitergeben/ablegen
- ☒ empfangen
- ☒ erstellen

verantwortl. Nachfolge-Dienststelle:

weitere Nachfolge-Dienststellen

Name	Straße	Ort	XD-NR
------	--------	-----	-------

Abbildung 5: @rtus-Admin Maske Dienststellenverwaltung Dienststellen-Status

Attribut/Referenzobjekt	Typ	Beschreibung
Information zu der Dienststelle	Dienststellen_Kat mit Referenz auf Katalog ALLG_DST	In der Datenbank wird für eine Dienststelle lediglich ihre Katalog-Referenz (ID) auf den Katalog ALLG_DST gespeichert. Alle Attribute bzw. grundlegenden Informationen zur Dienststelle werden aus dem Katalogeintrag bezogen. Die XD-Nummer ist ein fachlicher Schlüssel, die nicht dauerhaft eindeutig bleibt.
Leiter	1..1, Anwender	Referenziert den Leiter der Dienststelle. Bisher ein Muss-Referenz für eine aktive @rtus-Dienststelle. Leiter und Vertreter haben immer automatisch alle Berechtigungen auf der Dienststelle.
Stellvertreter	0..n, Anwender	Referenziert die Stellvertreter der Dienststellenleitung. Leiter und Vertreter haben immer automatisch alle Berechtigungen auf der Dienststelle.
Status	1..1, Enumeration Keine Artus-Dst Stillgelegt Aktiv	Definiert den Status der Dienststelle. Aktiv:

	Passiv Reorganisation	Dienststelle ist eine vollständige @rtus-Dienststelle, darf Vorgänge erstellen und Empfangen. Passiv: Dienststelle bzw. deren Anwender können sich in @rtus Anmelden, können aber keine Vorgänge empfangen oder Erstellen. Reorganisation: Die Dienststelle befindet sich übergangsweise in Reorganisation. Das bedeutet, sie wird organisatorisch geändert (Zusammenlegung, Auflösung). Es gibt immer eine Nachfolgerdienststelle, die rechtlich die Verantwortung für den Bestand der Dienststelle trägt. In der Übergangszeit können Anwender auf beiden Dienststellen arbeiten, Vorgänge aber nur noch auf der Nachfolgerdienststelle erstellen. Bestehende Vorgänge können abgeschlossen oder schnell auf die neue 1:1 übertragen werden.
--	--------------------------	--

Wie der Abbildung zu entnehmen ist, gibt es zahlreiche weitere Eigenschaften und Optionen, die an einer @rtus-Dienststelle konfiguriert werden können und müssen. Dieses Konzept geht davon aus, dass diese auch weiterhin nachträglich über @rtus-Admin konfiguriert wird.

2.3 Übersicht Objekt: Rollen- und Funktionsberechtigung

Das Rollen- und Rechtekonzept von @rtus ist extrem komplex und wird hier nur zusammenfassend mit den wesentlichen Aspekten für dieses Konzept dargestellt. Detaillierte Informationen lassen sich über die jeweiligen Fachkonzepte (A4, A5) erschließen.

@rtus unterscheiden im Wesentlichen die Datenberechtigung und die Funktionsberechtigung. Die Datenberechtigung definiert, auf welche Daten (Vorgänge) der Anwender mit welchen Recht (Standard, Lesend, Ändern, Verborgend) Zugriff hat. Die Datenberechtigung erhält der Anwender entweder durch seine Dienststellenzugehörigkeit (vertikale Berechtigung) oder durch seine Zugehörigkeit zu einem Blockverbund (horizontale Berechtigung). Derzeit können über den Artus-Webservice (Nutzung durch BPOL, ST) sowohl die Dienststellenzuordnung als auch die Zuordnung zum horizontalen Blockverbund verwaltet werden.

Die Funktionsberechtigung beschreibt, welche Funktionen ein Anwender auf dessen zugeordneten Dienststellen ausführen darf. Eine Funktionsberechtigung wird in der Regel pro ausführbare Funktion in @rtus eingeführt (z.B. Ort erstellen, löschen, ändern). Einzelne Funktionsberechtigungen werden zusammengefasst und in einer oder mehrerer Rollen gebündelt. Es gibt einige Basisrollen im @rtus (Sachbearbeitung, Verwaltung, Organisation, Leitung, Stellvertreter, etc.). Diese können beliebig und dynamisch über @rtus-Admin im Funktionsumfang geändert werden. Es können neue Rollen, basierend auf einer oder mehrerer Basisrollen, geschaffen werden und es können Eigenschaften von dynamischen Rollen auch an abgeleitete Rollen vergeben werden.

Die Rollen werden Anwendern derzeit entweder dezentral durch Organisationsrollen über den @rtus-Client oder zentral über @rtus-Admin sowie über den Artus-Webservice vergeben.

Das Rollen- und Rechtekonzept wurde in @rtus 6.0 neu umgesetzt und die Teilnehmer migrieren mit @rtus 7.0 alle auf das neue Konzept. Das alte (starre) Rollenkonzept wird mit @rtus 9.0 entfallen. Einzelne Funktionsberechtigungen können nach dem neuen Berechtigungskonzept nur noch über Rollen verändert werden, nicht mehr direkt am Anwenderobjekt.

Die Nachfolgenden Darstellung veranschaulichen die neue Rollenverwaltung über @rtus-Admin:

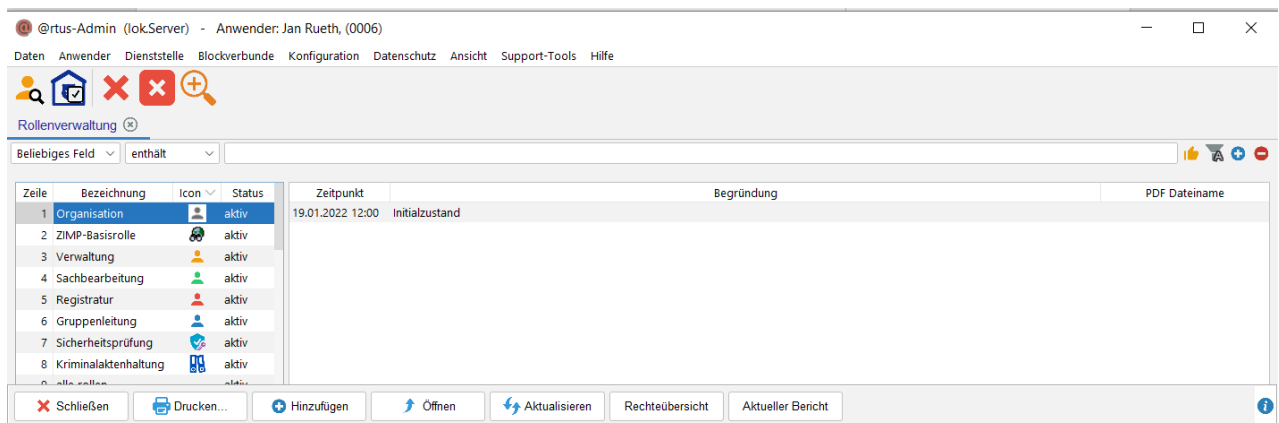


Abbildung 6: Rollenverwaltung in @rtus-Admin

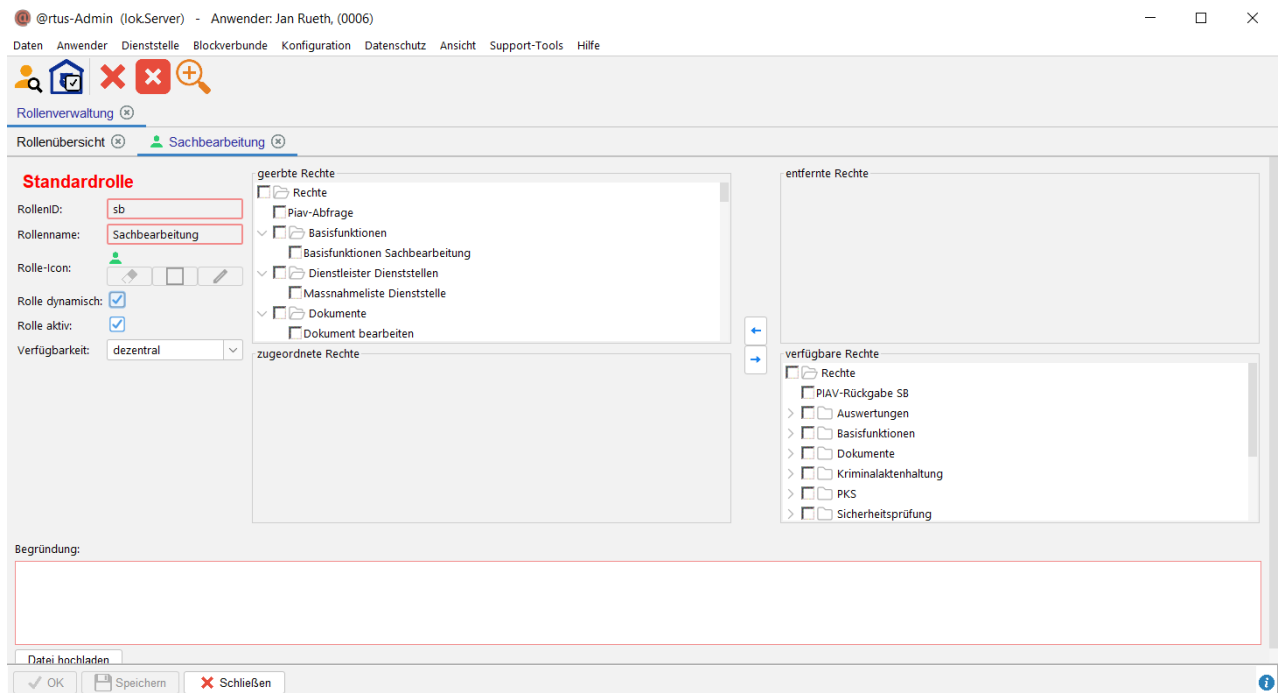


Abbildung 7: Rollenansicht und -bearbeitung in @rtus-Admin

2.4 Planungsübersicht und stufiges Vorgehen

	Stufe 1a	Stufe 1b	Stufe 2a	Stufe 2b
Nutzer-Login	SSO via IAM	SSO via IAM	SSO via IAM	SSO via IAM
Nutzer-Konten	zusätzliche, manuelle Verwaltung in @rtus, ohne Übernahme von AD-Attributen	zusätzliche, manuelle Verwaltung in @rtus, mit Übernahme von AD-Attributen	automatischer Abgleich TN-ADFS mit @rtus via IAM	automatischer Abgleich TN-ADFS mit @rtus via IAM
Nutzer-Rollen und Zugehörigkeit Dienststellen	manuell in @rtus verwaltet	manuell in @rtus verwaltet	manuell in @rtus verwaltet	automatischer Abgleich TN-Benutzerverwaltung mit @rtus via IAM
Nutzung	(nur für Testbetrieb von @rtus-Umgebungen vor iVBS-Einführung)	(nur für Testbetrieb von @rtus-Umgebungen vor iVBS-Einführung)	ab 19.11.2024 für Schulung und Wirkbetriebsaufnahme iVBS nutzbar	Nutzung für iVBS schnellstmöglich avisiert, aber Terminlage noch unklar

Abbildung 8: Ausbaustufen Anbindung Artus (Quelle Workshop 06.12.23 KTT/BKA/RP/SL/Dataport)

Die Abbildung stellt ein stufiges Vorgehen für die Anbindung von Artus an das IAM dar, welches aus einem Workshop mit SL, RP, PG IAM, BKA IAM und Dataport vom 06.12.23 entstanden ist (siehe A5). Die Stufe 1a und 1b sollten bereits mit dem Einsatz der Artus Version ab 8 möglich sein. Dieses Konzept fokussiert sich hier auf die Umsetzung der Stufe 2a und 2b.

Für einen ersten produktiven Einsatz und für die Aufnahme im Schulungsbetrieb wird seitens SL und RP die Stufe 2a ausreichen. 2b wäre wünschenswert, allerdings müssten dann auch bei den Teilnehmern noch Herausforderungen wie die Einführung einer zentralen Benutzer- und Berechtigungsverwaltung mit Anbindung an dem F-IAM erfolgen.

Dieses Konzept wird beide Stufen abdecken, wobei die Anforderung dann bei Bedarf mit 2a oder 2b gekennzeichnet werden. Im Folgenden werden Anforderungen und Lösungsansätze ggf. dann mit den Zusatz 2a oder 2b für die stufenweise Umsetzung gekennzeichnet.

2.5 Übersicht „P20 F-IAM“ Benutzerverwaltung

Dieser Abschnitt bietet einen zusammenfassenden Überblick über die Anbindung von F-IAM an @rtus iVBS. Dieser Abschnitt soll das grundlegende Verständnis der Lösung darstellen und ersetzt nicht die vorhandene Dokumentation (A1) der PG IAM.

Die Abbildung 9 stellt im Wesentlichen den aktuellen Sachstand der heutigen Lösung dar. Die Authentifizierung über F-IAM durch die @rtus-Client-Anwendungen wurde mittels OIDC (sowie SAML2, JWT) umgesetzt. Die Pflege der Anwender erfolgt weiterhin in der internen Benutzerverwaltung von @rtus. Bei Anlage neuer Anwender können die Grunddaten über die Anbindung des Verzeichnisdienst (LDAP-Legacy) übernommen werden. Als Beispiel einer Berechtigung von P20 Anwendung wurde in diesem Schaubild ZIMP eingefügt, spielt aber für dieses Konzept eine untergeordnete Rolle.

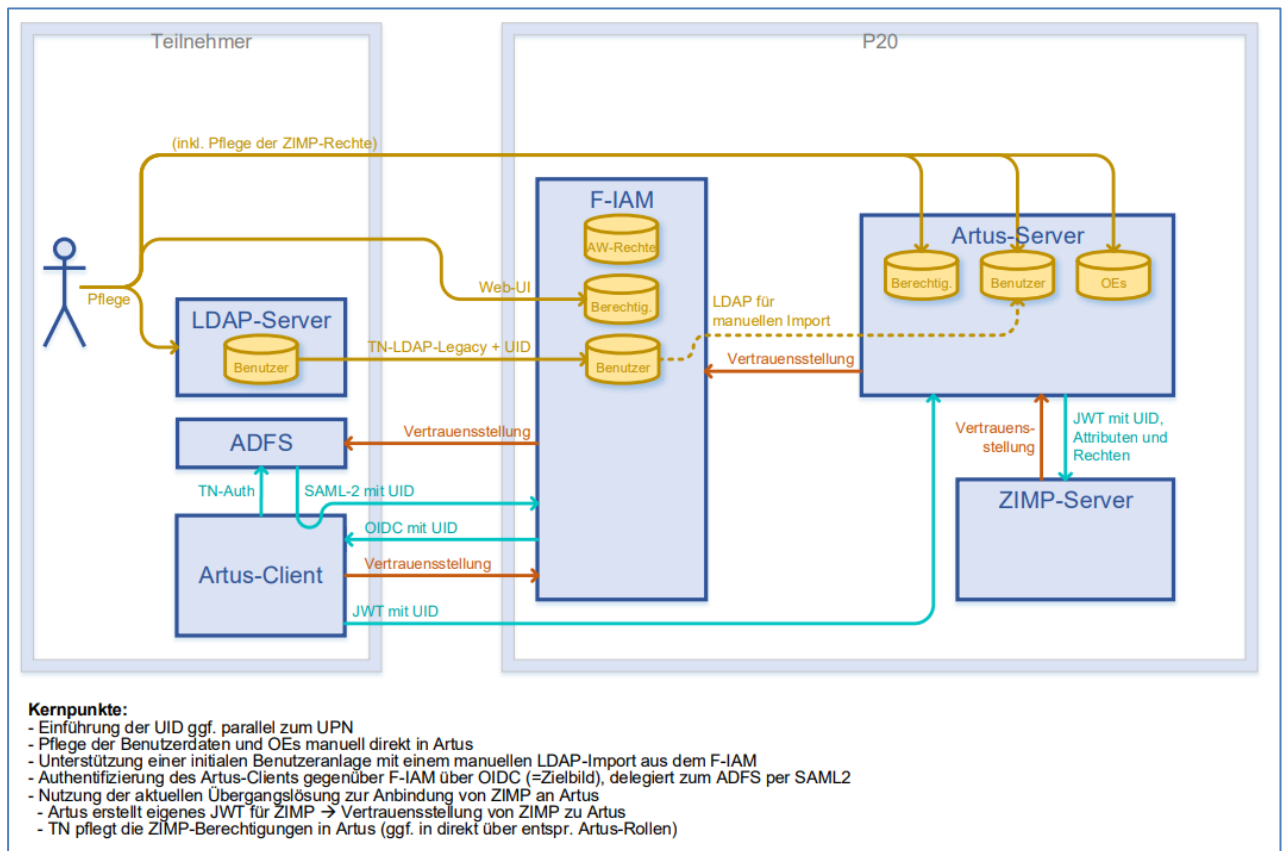


Abbildung 9: Schematische Darstellung interne Benutzerverwaltung ohne externe Provisionierung

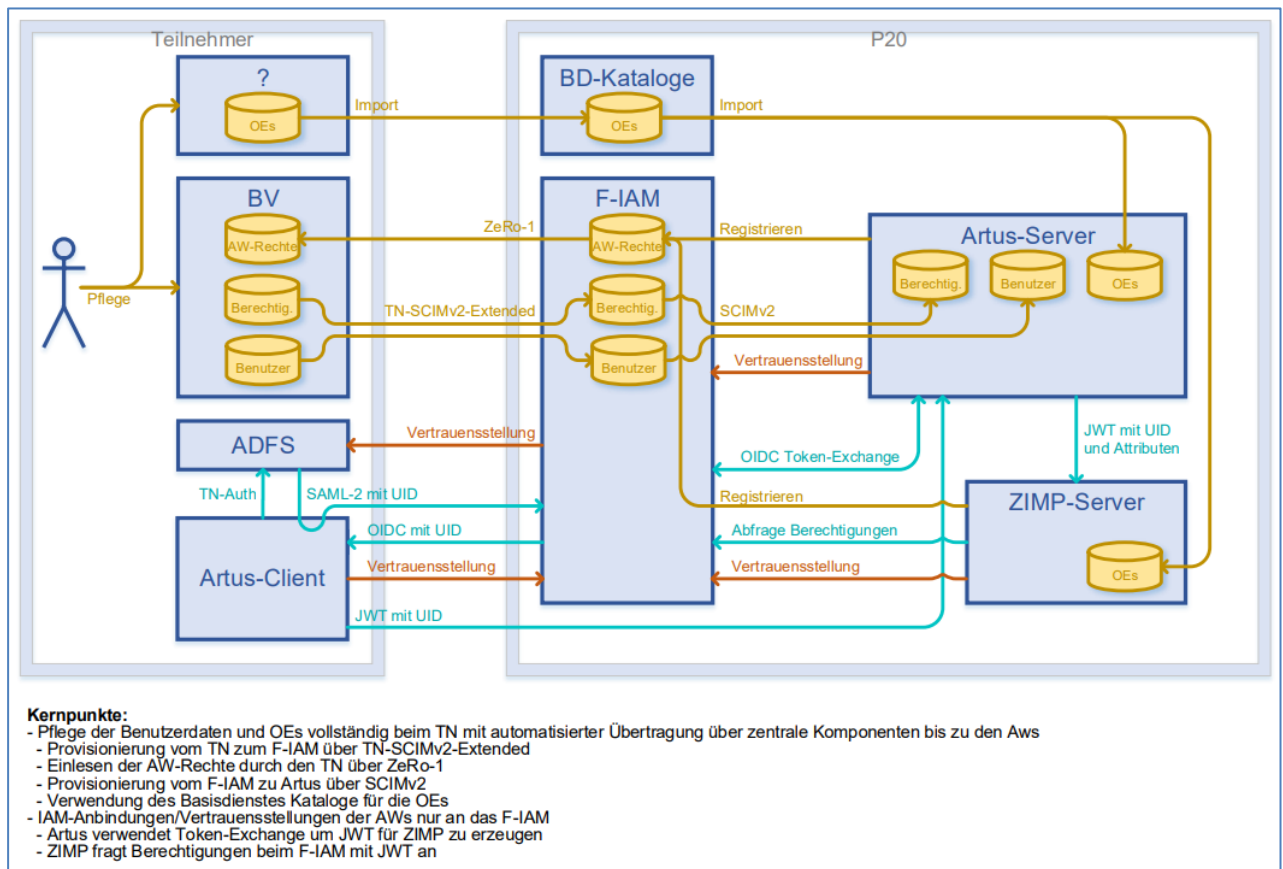


Abbildung 10: Provisionierung über F-IAM von P20

Die Abbildung 10 zeigt das Zielbild, wobei diese Darstellung ein wenig über die Stufe 2 der externen Provisionierung hinausgeht. Zunächst zeigt das Schaubild, dass sowohl die Benutzer als auch die Berechtigungen über eine teilnehmerspezifische Benutzerverwaltung (BV) erfolgen wird. Diese wird dann ins F-IAM übertragen. Das F-IAM überträgt wiederum diese Informationen und Änderungen an das iVBS @rtus. In beiden Fällen stützt sich dieser Datenaustausch auf das Protokoll SCIMv2. Dieser Teil deckt sich mit dem Vorhaben der Stufe 2 und den Umsetzungszielen von diesem Konzept.

Ergänzend wird hier die Provisionierung der Organisationseinheiten (Dienststellen) dargestellt, welche mit dem Basisdienst Kataloge sichergestellt werden soll. Dieser wird aufgrund der fehlenden Voraussetzungen noch nicht durch dieses Konzept abgedeckt und mit einer Interimslösung versehen werden müssen.

2.6 Übersicht über SCIMv2 (Schnittstellen F-IAM)

Die Anbindung von Fachanwendungen mittels SCIMv2 wird im Anlage A1 „Anbindung von Anwendungen an das F-IAM“ unter Abschnitt 4.6 vorgegeben:

4.6.1. Provisionierung per SCIMv2

*Die Anbindung per SCIMv2 erfolgt gemäß RFC7643, RFC7644 und RFC7642. Das Zuweisen von Berechtigungen mit Dienststellenbezug ist mit diesen Standards nicht möglich und erfordert eine Schemaerweiterung, die im Rahmen der zentralen Bereitstellung noch zu spezifizieren ist. Aus diesem Grund wird zwischen den Schnittstellen „SCIMv2-Core“ für die Basisfunktionalität und „SCIMv2- Extended“ für die schemaerweiterte Variante unterscheiden. In beiden Fällen muss die Anwendung SCIMv2-Schnittstelle bereitstellen. **Hierbei fungiert die Anwendung als SCIMv2 Server und das F-IAM als SCIMv2 Client.** Die Verbindung ist per https abzusichern.*

SCIM steht für „System for Cross-domain Identity Management“, Version 2 (SCIM 2) und ist ein Standardprotokoll, das von der Internet Engineering Task Force (IETF) entwickelt wurde. SCIM 2 bietet eine standardisierte Methode zum Austausch von Identitätsinformationen zwischen Identitätsdomänen, insbesondere zwischen Identitätsanbietern (IdP) und Serviceanbietern (SP). Der IdP entspricht hierbei dem F-IAM und der SP der Fachanwendung wie ein iVBS. Hier ist eine zusammenfassende Übersicht über den SCIM-Version-2-Standard aufgeführt (siehe auch A2):

1. Zielsetzung:
 - SCIM 2 zielt darauf ab, die Verwaltung von Identitäten in verschiedenen Domänen zu erleichtern, insbesondere in Cloud-basierten Umgebungen.
2. RESTful Protokoll:
 - SCIM 2 verwendet das Representational State Transfer (REST)-Protokoll für die Kommunikation zwischen Identitäts- und Serviceanbietern. Dies erleichtert die Integration und den Datenaustausch über das HTTP-Protokoll.
3. JSON-basierte Datenformat:
 - Die Datenübertragung zwischen Identitäts- und Serviceanbietern erfolgt im JSON-Format, was die Interoperabilität erleichtert und die Datenübertragung effizienter macht.
4. Kernfunktionen:
 - SCIM 2 definiert grundlegende Funktionen für die Verwaltung von Benutzeridentitäten, darunter die Abfrage, Erstellung, Aktualisierung und Löschung von Benutzerkonten (CRUD-Operationen).
5. Schemas und Erweiterungen:
 - SCIM 2 definiert standardisierte Schemata für Benutzer- und Gruppenattribute. Darüber hinaus können Implementierungen eigene Erweiterungen definieren, um spezifische Anforderungen abzudecken.
6. Endpunkte:
 - SCIM 2 definiert bestimmte Endpunkte für Benutzer- und Gruppenoperationen, die von Serviceanbietern bereitgestellt werden, um Identitätsinformationen zu verwalten.
7. Authentifizierung und Autorisierung:
 - SCIM 2 unterstützt verschiedene Methoden zur Authentifizierung und Autorisierung, darunter OAuth, um sicherzustellen, dass nur autorisierte Entitäten auf Identitätsinformationen zugreifen können.
8. Filterung und Sortierung:
 - SCIM 2 ermöglicht die Filterung und Sortierung von Abfrageergebnissen, um die Effizienz bei der Verarbeitung großer Datenmengen zu verbessern.

9. Eventbenachrichtigungen:

- Implementierungen von SCIM 2 können Eventbenachrichtigungen unterstützen, um Identitätsanbieter über Änderungen an Benutzerkonten zu informieren.

10. Beispielanwendung:

- Ein typisches Anwendungsszenario ist die Integration von Identitätsmanagement in Cloud-Diensten, bei denen ein Identitätsanbieter Benutzerkonten erstellt, aktualisiert oder löscht und diese Änderungen an den Serviceanbieter über SCIM 2 übermittelt.

SCIM bietet hierbei eher einen abstrakten Rahmen zum Austausch dieser Informationen. Die konkrete Definition der auszutauschenden Daten (Attribute der Benutzer und Gruppen etc.) obliegt den beteiligten Systemen. Somit muss basierend auf diesem Konzept und den Vorgaben von F-IAM eine technische Spezifikation für die konkrete Nutzung von SCIM im Zusammenspiel mit F-IAM noch erstellt werden.

SCIM spezifiziert Operationen, um Benutzer und Gruppen zu pflegen und zu verwalten. Es arbeitet nach dem CRUD-Prinzip (Create, Update, Delete), um jeweils Objekte hinzuzufügen, zu aktualisieren oder wieder zu entfernen. SCIM spezifiziert weiterhin die möglichen Quittungen und Fehlercode. Wie eingehend erläutert, geht das F-IAM jedoch davon aus, dass das iVBS die Anweisungen umsetzt. Ablehnung oder Fehler sollten, sofern irgendwie möglich, nur aus technischen Gründen erfolgen.

3 Lösungsansatz

Dieser Abschnitt beschreibt die Lösungsansätze, deren konkrete Ausarbeitung und Umsetzung dann im Abschnitt 4 und Abschnitt 5 detailliert im Kontext der Anforderungen beschrieben werden.

3.1 [Stufe 2b] Verwaltung von Organisationseinheiten / Dienststellen

Viele Geschäftsprozesse und Funktionen in @rtus basieren immanent auf das Vorhandensein des Dienststellen-Katalogs ALLG_DST. Dieser Katalog bildet mind. die gesamten verfügbaren Dienststellen sowie deren Hierarchie vom Teilnehmer ab, enthält aber auch Dienststellen anderer Teilnehmer oder Behörden. Da wir für eine längere Übergangszeit sowohl die interne Benutzer- und Dienststellenverwaltung wie auch die externe Verwaltung für unsere Teilnehmer anbieten müssen, besteht die Notwendigkeit für kompatible Lösungen.

Nach aktuellem Sachstand existiert in absehbarer Zeit weder bei P20 Katalogbasisdienst noch bei IAM ein durchgängiges Konzept zur Verwaltung und Pflege der Organisationseinheiten insbesondere der Dienststellen. Diese obliegt weiterhin den Teilnehmern. Im Zielbild sollen die Dienststellen über einen Katalogbasisdienst abrufbar sein, wie aber die Zuordnung zwischen IAM und Katalog sichergestellt wird und wie diese Prozesse ablaufen, ist derzeit vollkommen offen¹.

¹ Einzelne Teilnehmer wie Hamburg haben für sich einen vorhandenen Prozess basierend auf ihrer Benutzerverwaltung.

Daher gehen wir in diesem Konzept davon aus, dass zunächst der Dienststellen-Katalog ALLG_DST weiterhin existiert und weiterhin als Grundlage für die vorhandenen und neuen Anwendungsfälle dienen muss. Perspektivisch lässt sich durchaus vorstellen, dass dieser später durch eine Synchronisierung über den Katalogbasisdienst gepflegt und verwaltet wird. Derzeit werden die vorhandenen Katalogpflegeprozesse der @rtus-Kooperation wie bisher die Pflege der Dienststellen übernehmen.

Damit werden die Gesamtzahl aller möglichen Dienststellen sowie deren hierarchische Zuordnung zueinander weiterhin komplett über den @rtus-Dienststellen-Katalog ALLG_DST abgebildet. Der F-IAM referenziert Dienststellen lediglich über deren technischen Schlüssel/ID.

Als Vorschlag schlagen wir die Kataloggruppen-ID von @rtus vor. Auf keinen Fall darf ein veränderlicher Schlüssel wie die Dienststellenummer (Hierarchienummer, XD-Nummer) verwendet werden, da diese Erfahrungsgemäß eben nicht für immer konstant und eindeutig bleibt und sich damit nicht als Identifier bzw. Schlüssel für einen systemübergreifenden Austausch eignet. Sollte die Kataloggruppen-ID nicht als geeigneter technischer Schlüssel dienen können, so muss zwingend eine neuer technischer Schlüssel für den Austausch definiert werden, der dann auch im Katalog ALLG_DST aufgenommen und gepflegt werden muss. Dieses ist organisatorisch sicherzustellen.

Das Vorhandensein eines Katalogeintrags im Dienststellenkatalog von @rtus macht aus einer Dienststelle noch keine @rtus-Dienststelle. Eine neue @rtus-Dienststelle wird über @rtus-Admin eingerichtet und erhält dort eine Reihe von Einstellungen, die für eine Dienststelle vorgenommen werden müssen (vergleiche 2.2). Eine neue Dienststelle wird somit aus dem Dienststellenkatalog bei Einrichtung ausgewählt und referenziert den Katalogeintrag, aber sie ist eben erst in @rtus nutzbar, wenn sie über @rtus-Admin eingerichtet worden ist.

Dieser Prozess entspricht den heutigen Funktionen und bleibt weiterhin bestehen und kann somit in einen organisatorischen Prozess auch im Zusammenspiel mit IAM umgesetzt werden.

Der Prozess müsste folgende Reihenfolge sicherzustellen:

1. Katalogeintrag in @rtus-Katalog
2. Katalogeintrag muss ausgerollt werden
3. Einrichten der Dienststelle in @rtus Admin
4. Erstmalige Verwendung der Dienststelle für die Berechtigung von Anwendern in der BV
5. Anwender können auf Dienststellen über BV und F-IAM in @rtus über SCIM berechtigt werden

Der Eintrag kann auch in der BV vorher erzeugt werden (vor Schritt 1), falls die BV eine ID für den Eintrag erzeugen muss. Trotzdem darf die BV den Eintrag erst ab Schritt 4 verwenden.

3.2 [Stufe 2a] Verwaltung von Anwendern

Unter Verwaltung von Anwendern werden die folgenden drei Anforderungen betrachtet:

- [ANF-010] Anlage neuer Anwender
- [ANF-011] Deaktivierung (logische Löschung) von Anwendern
- [ANF-012] Pflege und Aktualisierung der Anwenderstammdaten

Dieser Abschnitt beschreibt den Lösungsansatz für die Anforderungen.

Für alle oben genannten Aktionen definiert SCIMv2 Core bereits die notwendige Entität (User) und Operationen an. Diese sollen entsprechend bei einer Umsetzung genutzt werden.

Wie in Anlage A1.1 „Anbindung von Anwendungen an das F-IAM“ festgelegt wurde, stellt @rtus die Operationen serverseitig bereit und der F-IAM nutzt diese Operationen, um die oben genannten Aktionen im iVBS auszuführen.

Endpunkt	Operation	Beschreibung	Relevant für Anwendung	Anmerkung
/Users	GET	Abfrage aller Benutzer	immer	Dient dem F-IAM zum Abgleich der User
	POST	Erstellen eines neuen Benutzers	immer	[ANF-010] Anlage neuer Anwender Erzeugt einen neuen Nutzer (Objekt Anwender) in @rtus oder aktualisiert diesen, wenn dieses vorhanden ist.
/Users/{User-ID}	GET	Abfrage eines konkreten Benutzers, ID wird von AW vergeben Liefert auch die Liste aller Berechtigungszuweisungen (auch mit OU-Bezug), sofern es nicht über Query-Parameter unterbunden wird.	immer	Dient dem F-IAM zum Abgleich der User
	PATCH	Ändern von Benutzerattributen		[ANF-012] Pflege und Aktualisierung der Anwenderstammdaten Wenn eine Umsetzung erfolgt, können hiermit einzelne Attribute vom Nutzer geändert bzw. bei mehrfachwerten hinzugefügt oder gelöscht werden.
	DELETE	Löschen eines Benutzers		Diese Operation löscht den Nutzer nicht aus @rtus, sondern deaktiviert den Anwender logisch. Zum Deaktivieren eines Nutzers muss in @rtus Plausibilitäten geprüft und wenn notwendig, den Nutzer bzw. deren referenzierte Daten in eine konsistenten gebracht werden. Die Operation muss ausgeführt werden und darf

			nicht abgelehnt werden. Der genaue Prozess wird im umsetzungsteil beschrieben.
--	--	--	--

Nachfolgende Tabelle beschreibt die Abbildung der Attribute von @rtus Anwender-Fachobjekt zur SCIM Entität „User“

Attribut @rtus	SCIM Attribut User “Core”	SCIM Attribut User “Extended”	Anmerkung
ID_IAM	[1..1] id	-	Technische ID von F-IAM
Login/Benutzeranmelde-name	[1..1] userName	-	
DN	-	-	entfällt
UID	-	[0..1] p20UID	
Dienstnummer	-	[1..1] dienstnr	
Vorname	[1..1] name/givenName	-	
Name	[1..1] name/familyName	-	
Email	[0..n] emails	-	Erstes Objekt mit type = “work“ wird übernommen, am besten mit „primary=true“
Telefon	[0..n] phoneNumbers	-	Erstes Objekt mit type = “work“ wird übernommen, am besten mit „primary=true“
Telefax	[0..n] phoneNumbers	-	Erstes Objekt mit type = “fax“ wird übernommen
Deaktiviert	-	-	Entfällt hier als Attribut und wird bei der Dienststellenzuordnung betrachtet und wird nur intern bei Löschung gesetzt.
Global Gesperrt	active	-	Sperrt den Anwender, wenn ArtusGlobalGesperrt =true
Anwender auf Dienststelle sperren.		?	Entfällt hier als Attribut und kann nur über @rtus durchgeführt werden.

Die oben aufgeführte Tabelle weist das Attribut-Mapping von der SCIM-Entität „User“ auf das Fachobjekt „Anwender aus. Einige Attribute lassen sich dem vorhandenen Kerndatenmodell von SCIM zuordnen, andere müssen nach SCIM-Standard dann durch eine Schema-Erweiterung durch iVBS und F-IAM umgesetzt werden.

Die nachfolgende Darstellung zeigt beispielhaft das Ergebnis einer GET-Anfrage für einen Anwender vom iVBS @rtus an das F-IAM, wobei hier gegenüber A1.1 bereits Attribute weggelassen worden sind, die nicht vom @rtus unterstützt werden.

```

HTTP/1.1 200 OK
{ "schemas" : [
  "urn:ietf:params:scim:schemas:core:2.0:User"
, "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"
, "urn:ietf:params:scim:schemas:extension:p20:2.0:User"
, "urn:ietf:params:scim:schemas:extension:p20:2.0:Group"
, "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"
]
, "id" : "2819c223-7f76-453a-919d-413861904646"
, "meta" : {
  "resourceType" : "User"
, "version" : "99"
, "created" : "2011-08-01T21:32:44.882Z"
, "lastModified" : "2011-08-01T21:32:44.882Z"
, "location" : "https://.../scim/v2/Users/2819c223-..."
}
, "userName": "max.mustermann"
, "active" : true
, "name" : {
  "familyName" : "Mustermann"
, "givenName" : "Max"
}
, "emails": [
  { "primary": true
  , "type" : "work"
  , "value" : "max.mustermann@somewhere.com",
  }
]
, "phoneNumbers": [
  { "primary" : true
  , "type" : "work"
  , "value" : "+49 123 456789"
  }
, { "type" : "fax"
  , "value" : "+49 987 654321"
  }
]
, "urn:ietf:params:scim:schemas:extension:p20:2.0:User": {
  "p20UId" : "T-36-0-18-101-123456789"
, "p20DepartmentNumber" : "LKA-123"
, "policeTitleKey" : "123"
}
, "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission": [
  { "value" : "AW-OE-Recht-1"
  , "scope" : "OE-1"
  , "inherit" : true
  }
, { "value" : "AW-OE-Recht-2"
  , "scope" : "OE-1"
  , "inherit" : false
  }
]
}

```

In den nachfolgenden Abschnitt 3.3 und 3.4 zur Dienststellenzuordnung und Berechtigung

3.3 [Stufe 2b] Verwaltung Dienststellenzugehörigkeiten

In @rtus ist es durchaus möglich, dass Anwender ohne Rollen (ohne Funktionsberechtigung) einer Dienststelle zugeordnet sein können. Dieses ist vermutlich kein Regelfall. Jedoch allein die Zuordnung eines @rtus-Anwenders zu einer Dienststelle vergibt indirekt eine Datenberechtigung auf die Dienststelle. Je nach Einstellung der Dienststellenvorgangsberechtigung, erhält der Anwender ein Recht auf den Vorgangsdatenbestand der Dienststelle, welches in der Regel ein lesender Zugriff darstellt.

SCIMv2 verfügt im Kern nicht über die Möglichkeit, einen Anwender eine Menge von Dienststellen zuzuordnen. Auch die Hamburger Benutzerverwaltung sieht es nicht vor, Anwendern ohne Berechtigung bzw. einer Rolle eine Zuordnung zu einer Dienststelle zu machen. Die Zuordnung zu einer Dienststelle erfolgt hier implizit über die Vergabe einer Berechtigung auf einer Dienststelle.

Allerdings könnte in einem stufigen Vorgehen die Möglichkeit einer Zuordnung ohne Rollenvergabe eine nützliche Funktion sein, die bei vorhandener Zuordnung im der Benutzerverwaltung administrativen Aufwand verringern kann. Daher soll der Lösungsansatz zur Verwaltung von Berechtigungen auch eine reine Zuordnung zur Dienststelle ohne Rollenvergabe ermöglichen.

Weiter Informationen sind demnach im nächsten Abschnitt zur Vergabe von Rollen (Berechtigung) auf Dienststellen zu entnehmen.

3.4 [Stufe 2b] Verwaltung von Berechtigungen

In @rtus unterscheiden wir bereits im Abschnitt 2.3 beschriebenen Daten- und Funktionsberechtigung. Datenberechtigung erhält der Anwender über die Zuordnung zu Dienststellen oder zu Horizontalen Blockverbunden. Funktionsberechtigungen werden in Rollen beliebig gruppiert und in der Regel werden dann diese Rollen in Bezug auf eine Dienststelle vergeben. Im Detail lässt sich zwar über die interne Benutzerverwaltung von @rtus auch noch mal explizit für jede dieser zugeordneten Rolle bei einem Anwender eine gesonderte Konfiguration der Funktionsberechtigung machen, spielt aber hier nur eine untergeordnete Rolle.

Die Datenberechtigung über Blockverbund wird weiterhin nur innerhalb von @rtus vergeben und wird wie bisher auch, über die bestehenden Mittel von @rtus-Admin sowie der möglichen Vergabe über die interne Verwaltung im VBS durchgeführt.

Die (vertikale) Datenberechtigung auf Dienststellenebene wird über die Zuordnung von Rollen für ein Anwender auf den Dienststellen vergeben. Wird eine Rolle auf einer Dienststelle vergeben, wird der Anwender dieser Dienststelle in @rtus zugeordnet und entsprechend hat er automatisch die Datenberechtigung für die Dienststelle. Alternativ kann dem Anwender nur eine Dienststelle ohne

Rollen zugewiesen werden. Damit ist der der Dienststelle zugeordnet, hätte aber keinerlei Funktionsberechtigung auf der Dienststelle.

Wird die Zuordnung zur Dienststelle entfernt (keine Rolle und keinerlei mehr Zuordnung zur Dienststelle), wird auch in @rtus die Zuordnung zur Dienststelle aufgehoben und damit die Datenberechtigung entfernt. Was im Detail dabei zu beachten ist und wie dieser Prozess automatisiert bearbeitet werden soll, ist im späteren Abschnitt der Umsetzung beschrieben.

Dieses Fachkonzept legt fest, dass über F-IAM bis auf weiteres ausschließlich Rollen von @rtus vergeben werden können. Die einzelnen Funktionsberechtigungen werden weiterhin ausschließlich intern über @rtus-Admin den Rollen zugeordnet bzw. aktiviert oder eben deaktiviert. Somit können über das F-IAM nur Rollen auf Dienststellen vergeben werden. Artus kennt weit über 700 Funktionsberechtigungen, die mit jeder Version und Funktionalität weiter ansteigen. Die Vergabe von Berechtigungen in @rtus erfolgt aber immer auf Ebene ganzer Rollen, so dass dieses nun auf dem F-IAM abgebildet wird.

Die derzeitigen Lösungen der Benutzerverwaltungen in den Ländern (sofern überhaupt vorhanden) unterstützen noch keine vergleichbare Rollenverwaltung, wie es derzeit das iVBS @rtus verfügbar ist. Daher muss zunächst die Funktion im VBS erhalten bleiben und zunächst die Vergabe der Rechte über Rollen vollzogen werden. Im Zielbild sollen laut PG IAM Benutzerverwaltungen dazu ertüchtigt werden, so dass in einer weiteren späteren Ausbaustufe @rtus auch die Vergabe von Einzelberechtigungen ermöglichen soll (wird hier nicht weiter betrachtet).

Folgende Basisrollen sollen mindestens über das F-IAM vergeben werden können:

Rolle @rtus	ID aus Rolle Vergabe und Einsicht über @rtus-Admin mit Präfix „ART_“	Anmerkung
Dienststellenleitung	ART_DSTL	In @rtus technisch keine eigene Rolle, sondern eine Beziehung, wird aber in F-IAM als Rolle abgebildet. Es kann nur ein Anwender Leiter einer Dienststelle sein.
Stellv. Dienststellenleitung	ART_DSTVL	In @rtus technisch keine eigene Rolle, sondern eine Beziehung, wird aber in F-IAM als Rolle abgebildet. Es dürfen mehrere Anwender Stellvertreter sein.
Sachbearbeitung	ART_SB	-
Verwaltung	ART_VW	-
Organisation	ART_ORG	-
Kriminalaktenhaltung	ART_KAH	Können nur auf KAH-Dienststellen vergeben werden oder werden ansonsten ignoriert.
Sicherheitsüberprüfung	ART_SIP	Können nur auf SiP-Dienststellen vergeben werden oder werden ansonsten ignoriert.
ZIMP-Basisrolle	ART_ZIMP	

Zugeordnet (ohne Rollen)	ART_ZO	Anwender ist der Dienststelle zugeordnet, aber ohne weitere Rollen
--------------------------	--------	--

Die Sonderrollen Gruppenleitung und Registratur werden nicht über F-IAM vergeben und werden wie bisher administriert. Das Entfernen der Zuordnung einer Dienststelle und die Auswirkung auf diese beiden Sonderrollen wird ebenfalls in späteren Abschnitten erläutert.

Das dynamische Rollenkonzept von @rtus erlaubt auf Basis einer oder mehrerer Rollen auch beliebig viele neue und eigene Rollen, die über @rtus-Admin konfiguriert und vergeben werden können (verweis auf Rollen- und Rechtekonzept A3). Auch diese Rollen können über das F-IAM vergeben werden. Hierzu müssen auch für diese Rollen externe Schlüssel vergeben werden, die eindeutig für die Rolle sind. Es ist organisatorisch sicherzustellen, dass nur diese externen Schlüssel genutzt werden und diese auch vorher im iVBS für eine Rolle vergeben worden sind.

Ebenfalls stellt das dynamische Rollenkonzept sicher, dass bei der Vergabe der Sonderrollen Dienststellenleitung und stellv. Dienststellenleitung die vorherigen Rollen erhalten bleiben. Vorher wurden die Rollen als Seiteneffekt immer entzogen². Dieses ist im Kontext von IAM sehr zu begrüßen, da dadurch sichergestellt wird, dass sie Sichten bei der Vergabe von Rollen zwischen BV, IAM und iVBS erhalten bleiben und nicht durch Seiteneffekte auseinanderlaufen.

Der Austausch der Berechtigungen erfolgt über den SCIM-Endpunkt „OE-Permission. Entsprechend der in Anlage A1.1 geschilderten Endpunkte und Operationen können hier die Berechtigungen (Rollen) von @rtus für TN-/F-IAM elektronisch zur Verfügung gestellt werden, sowie Rechte für Anwender mittels PATCH-Operation vergeben werden.

Beispiel in JSON auf Basis A.1.1 (zum besseren Verständnis):

² Siehe: [\[ART-32100\] Neues Rollenkonzept - Dienststellenleiter nach Umstellung - Artus JIRA \(extrapol.de\)](#)

```
GET /Users/{id}
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8.....
HTTP/1.1 200 OK
{ "schemas" : [
  "urn:ietf:params:scim:schemas:core:2.0:User"
, "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"
, "urn:ietf:params:scim:schemas:extension:p20:2.0:User"
, "urn:ietf:params:scim:schemas:extension:p20:2.0:Group"
, "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"
]
, "id" : "2819c223-7f76-453a-919d-413861904646"
...
, "urn:ietf:params:scim:schemas:extension:p20:2.0:User":
{ "p20Uid" : "T-36-0-18-101-123456789"
, "p20DepartmentNumber" : "LKA-123"
, "p20PoliceTitleKey" : "123"
}
"urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission": [
, { "value" : "ART_DSTL"
, "scope" : "1111111110"
, "inherit" : false
}
, { "value" : "ART_SB"
, "scope" : "1111111111"
, "inherit" : false
}
, { "value" : "ART_VW"
, "scope" : "1111111111"
, "inherit" : false
}
, { "value" : "ART_ZO"
, "scope" : "1111111112"
, "inherit" : false
}
]
}
```

Abbildung 11: Beispiel für eine Antwort auf Abfrage User mit Rollen von @rtus

Im Beispiel oben wäre der Nutzer Max Mustermann mit folgenden Rechten angelegt worden:

- Auf Dienststelle 1111111110 mit den Rollen Dienststellenleitung
- Auf Dienststelle 1111111111 mit den Rollen Sachbearbeitung und Verwaltung
- Auf Dienststelle 1111111112 zugeordnet, aber ohne weitere Rollen

Folgende Tabelle beschreibt die Attribute einer Berechtigung (OuPermission)

SCIM Attribut User "Extended"	Anmerkung
[1..1] scope	Technische ID der Organisationseinheit (Dienststelle). Diese bezieht sich auf die Vorgaben im Abschnitt 3.1
[1..1] value	Die Berechtigung, die auf die OE/Dienststelle bezogen erteilt werden soll. Diese enthält den technischen Schlüssel der Rolle, wie sie unter Abschnitt 3.4 beschrieben sind.
[1..1] inherit	Bestimmt, ob das Recht durch Vererbung vergeben wurde. Muss von der TN-IAM bzw. BV unterstützt werden. Ist bis auf weiteres bedeutungslos für iVBS @rtus.

Folgende SCIM-Operationen (siehe A1.1) auf „OE-Permissions“ lösen nachfolgende Aktionen aus:

Endpunkt	Operation	Beschreibung	relevant für AWs	Anmerkung
/OU-Permissions	GET	Abfrage von Rechten mit OE-Bezug, die für die AW zugewiesen werden können Liefert auch die Liste der Zuweisungen, sofern es nicht über Query-Parameter unterbunden wird.	für AW mit Berechtigungen mit OE-Bezug	
/OU-Permissions/{OU-Permission-ID}	GET	Liefert auch die Liste der Zuweisungen, sofern es nicht über Query-Parameter unterbunden wird.		
	PATCH	Berechtigungszuweisung mit OE-Bezug hinzufügen/entfernen		

Die Rollen werden über die Patch-Operation auf dem Endpunkt „OU-Permission“ gepflegt (siehe A1.1). Hierbei wird die Nutzer-ID als sowie die OE übertragen. Der Endpunkt adressiert in der URL dann das jeweilige Recht.


```

PATCH /OU-Permission/ART_SB
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8.....
{ "schemas"      : ["urn:ietf:params:scim:api:messages:2.0:PatchOp"]
, "Operations"   : [
  { "op"         : "add"
  , "path"       : "members"
  , "value"      : [
    { "type"      : "User"
    , "value"     : "2819c223-7f76-453a-919d-413861904646"
    , "scope"     : "1111111112"
    , "inherit"   : false
    }
  ]
}
]
}}}
```

Abbildung 12: Beispiel PATCH-Operation mit Vergabe SB-Rolle auf einer Dienststelle

In oben dargestellter Patch-Operation, wird dem Anwender mit der angebenen ID die Rolle Sachbearbeitung auf Dienststelle 1111111112 vergeben.

Die vollständige Spezifikation der PG IAM zu SCIMv2 und Erweiterung ist unter <https://confluence.bka.extrapol.de/pages/viewpage.action?pageId=213925217> einsehbar.

3.5 [Stufe 2a] Protokollierung und Nachvollziehbarkeit

Sowohl die interne als auch die externe Provisionierung vergeben letztendlich Nutzern Funktions- als auch Datenberechtigungen in Artus.

Aus diesem Grund muss jederzeit aus datenschutzrechtlichen Gründen nachvollziehbar sein, welche Rechte der Anwender momentan hat und wie diese Berechtigung vergeben worden sind.

F-IAM als P20 Basisdienst protokolliert Veränderungen über den Protokollbasisdienst von P20. Ob diese Protokollierung vollständig oder ggf. ausreichend ist, wird hier nicht betrachtet. Vielmehr beschreibt dieser Abschnitt, welche Protokollierung auf Seiten Artus vorgenommen werden müssen, um eine Nachvollziehbarkeit auch auf Seiten Artus zu gewährleisten und auch durch die erhöhte technische Komplexität, mögliche Analysen bei Problemen zu unterstützen.

Ebenfalls wir davon ausgegangen, dass auch die Benutzerverwaltungen der Teilnehmer ihren Pflichten zur Protokollierung und Nachvollziehbarkeit nachkommen.

Es gibt in @rtus drei Ebenen der Protokollierung:

- Technische Protokollierung im Log von Client/Server
Hierbei schreibt die Anwendung lokal in eine Logdatei. Auf Clientseite hat diese eine konfigurierbare Größe und wird überschrieben. Auf Serverseite wird die Datei vollständig ohne

Begrenzung geführt und nach Kundenvorhaben gepackt und nach definierten Ablaufzeiten betrieblich gelöscht. Diese Logdateien dienen zur kurzfristigen Nachvollziehbarkeit und Problemanalyse.

- Protokolleinträge in einer Datenbank-Protokolltabelle

In der Artus-Datenbank wird eine Protokolltabelle geführt, die definierte Ereignisse jeweils als ein Protokolleintrag schreibt. Diese Protokolleinträge können über Artus-Admin abgefragt werden. Sie werden nach einer konfigurierbaren Zeit gelöscht (ca. 6 bis 12 Monate). In der Regel werden dort Änderungen/Löschungen auf Fachobjekte dokumentiert (ebenfalls konfigurierbar) oder andere definierte Ereignisse wie z.B. der Vorgangszugriff auf fremde Vorgangsdaten.

- Übermittlung von Statusdaten an ULS

Hierbei werden vor allem zur Überwachung der korrekten Funktion der verschiedenen technischen und fachlichen Komponenten und Schnittstellen hilfreiche und notwendige Daten an das Auswerte- und Überwachungssystem ULS (Universal Logging System) übermittelt. Hierbei werden keine Fachdaten übertragen. Diese Daten können über das ULS ausgewertet oder aufbereitet und dort überwacht werden.

Für die externe Provisionierung sollen alle drei Ebenen der Protokollierung genutzt werden. Jede für ihre vorgesehene Zielrichtung. Die konkreten Vorgaben werden dann bei den jeweiligen Anforderungen in den späteren Abschnitten beschrieben.

Aufgrund der hohen Sensibilität im Kontext der Berechtigung von Anwendern, sollen die Nachrichten aus dem F-IAM für eine konfigurierbare Zeit vollständig in der Datenbank gespeichert werden. Dieses erleichtert sowohl die Problemanalyse als auch die Nachvollziehbarkeit von Änderungen. Zusätzlich kann diese Speicherung bei Bedarf auch bei einer asynchronen Nachrichtenverarbeitung genutzt werden.

3.6 [Stufe 2a] Vorgehen bei der Transition von interner auf externer Provisionierung für Bestandskunden

Bestandsteilnehmer sind im diesem Kontext Teilnehmer, die von einer internen Benutzer- und Rechteverwaltung in Artus auf eine externe Provisionierung über F-IAM und BV wechseln möchten und einen Datenbestand mit Anwendern und Rechten besitzen.

Sicherlich bedarf es bei einer konkret anstehenden Transition eines Teilnehmers einer eigenständigen Betrachtung, Planung und Test der Transition. Trotzdem sollen in diesem Konzept Lösungsansätze bedacht werden, die aus heutiger Sicht eine solche Transition zumindest ermöglichen können.

Der Lösungsansatz wird nach derzeitiger Einschätzung bereits durch die SCIMv2-Schnittstelle seitens F-IAM eingebracht. Die Spezifikation beschreibt folgende Operationen zur Abfrage von Benutzern und Berechtigungen:

- Auf Endpunkt „Users“
 - 1.4.3 Suchen (Search)
 - 1.4.4 Abrufen (WellKnown) (A1.1.)
- Auf Endpunkt „OE-Permission“
 - 1.1.2 Berechtigungsdefinitionen Abfragen“
 - 1.1.3 Berechtigungszuweisungen Abfragen“

Werden diese Abfragemöglichkeiten direkt von der BV auf dem iVBS Artus genutzt, könnte die BV den aktuellen Zustand der (internen) Berechtigungen im SCIMv2-Format abfragen. Dieses könnte bei einer Transition genutzt werden, um die Nutzer, Dienststellenzuordnung und Rechte über ein Migrationsskript oder Software abzufragen und in der BV des Teilnehmers anlegen zu lassen. Damit würde sich der Zustand der internen Berechtigungsverwaltung von Artus auf eine BV übertragen lassen.

Damit die Transition über die SCIMv2-Schnittstelle reibungslos funktioniert, ist es erforderlich, dass die Benutzer aus der BV- und der Artusdatenbank des jeweiligen Bestandteilnehmers dasselbe UPN als identifizierendes Merkmal haben. Zu diesem Zweck wurden bereits Updateskripte für die Artusdatenbank im Anhang des Tickets [ART-32483](#) erstellt und sind als vorbereitende Maßnahme zwingend erforderlich.

In der Transition sollten migrierte Anwender, Berechtigungen und Dienststellenzuordnung zwar an das F-IAM übermittelt werden, jedoch werden diese Änderungen nicht weiter an das VBS übermittelt. Hier muss noch mit der PG IAM geklärt werden, ob sie die Übermittlung an das Fachverfahren ihrerseits während einer solchen Migration unterdrücken können.

Hinweis: Die Operationen sind beide zwar in der Spezifikation aufgeführt, aber inhaltlich noch nicht beschrieben und mit Beispielen versehen.

4 Anforderung

In diesem Abschnitt werden die Anforderungen und jeweils fachliche notwendige Verhaltensszenarien beschrieben. Wie die einzelnen Anforderungen dann konkret umgesetzt werden, wird später im Abschnitt 5 für jede Anforderung beschrieben.

4.1 [ANF-001][Stufe 2a] Anlage neuer Dienststellen

Ereignis:

Es soll eine neue Dienststelle für @rtus eingerichtet werden.

Lösungsart:

Organisatorisch

Aktionen:

- Die Stammdaten der Dienststelle sind bekannt
 - Kurz- und Langbezeichnung
 - Dienststellenhierarchienummer (XD-Nummer)
 - Übergeordnete Dienststellen
 - Kontaktdaten (Email, Telefon, Fax)
- Die Stammdaten werden bei jeweiligem Teilnehmer an die produktverantwortliche Stelle iVBS @rtus oder einer zentralen Katalogredaktion gemeldet
- Die produktverantwortliche Stelle prüft und übergibt es als Auftrag an die Katalogpflege
- Die Katalogpflege legt die Dienststelle neu an und vergibt damit auch einen technischen Schlüssel
- Der Katalog wird ausgerollt per Software-Update oder in dringenden Fällen per Katalog-Onlineupdate
- Die Dienststelle wird in Artus Admin angelegt
- Der Eintrag wird manuell in der Benutzerverwaltung eingetragen bzw. darf ab diesem Zeitpunkt verwendet werden

4.2 [ANF-002] [Stufe 2b] Pflege und Aktualisierung der Dienststellenstammdaten

Ereignis:

Die Stammdaten einer existierenden Dienststelle sollen geändert/aktualisiert werden

Lösungsart:

Organisatorisch

Aktionen:

- Die zu ändernden Stammdaten der Dienststelle sind bekannt

- Die Stammdaten werden bei jeweiligem Teilnehmer an die produktverantwortliche Stelle gemeldet oder einer zentralen Katalogredaktion gemeldet
- Die produktverantwortliche Stelle prüft und übergibt es als Auftrag an die Katalogpflege
- Die Katalogpflege aktualisiert die Stammdaten
- Soll die Hierarchie der Dienststelle geändert werden, so sollte eine Anpassung der Dienststellenhierarchienummer (XD-Nummer) erfolgen
- Die technische ID der Dienststelle darf dabei nicht geändert werden
- Der Katalog wird ausgerollt per Software-Update oder in dringenden Fällen per Katalog-Onlineupdate
- Die Dienststelle darf die ganze Zeit in der Benutzerverwaltung/F-IAM weiter genutzt/referenziert werden

4.3 [ANF-003] [Stufe 2b] Deaktivierung (Löschung) von Dienststellen

Ereignis:

Eine Dienststelle soll stillgelegt werden.

Lösungsart:

Organisatorisch

Aktionen:

- Die stillzulegende Dienststelle ist bekannt
- Es wurde eine aktive Dienststelle benannt, die für den Bestand der stillzulegenden Dienststelle die Verantwortung übernimmt
- Die beiden Dienststellen werden beim jeweiligen Teilnehmer an die produktverantwortliche Stelle gemeldet
- Die produktverantwortliche Stelle prüft und bearbeitet den Auftrag über @rtus-Admin
- Mittels @rtus-Admin und den Geschäftsprozess „Dienststellen-Reorganisation“ wird die stillzulegende Dienststelle in den Status Reorganisation gesetzt und die Nachfolgerdienststelle hinterlegt
- Es folgt eine Übergangsphase, in der aktive Vorgänge endbearbeitet werden oder auf die Nachfolgerdienststelle abverfügt werden
- Nach dieser Phase werden alle Benutzer und Rechte von der Dienststelle über Benutzerverwaltung und F-IAM entfernt
- Über @rtus-Admin wird die Dienststelle stillgelegt

4.4 [ANF-010] [Stufe 2a] Anlage neuer Anwender

Ereignis:

Ein neuer Anwender soll in @rtus angelegt werden.

Lösungsart:

Automatisiert über Schnittstelle F-IAM

Aktionen:

- Die Daten vom neuen Anwender sind vollständig bekannt
- Der Anwender wird in der Benutzerverwaltung vom Teilnehmer eingetragen
- Sollte der Teilnehmer noch keine Benutzerverwaltung (TN-IAM) haben, kann diese im Teilnehmer-Verzeichnisdienst angelegt und dann über das Web-UI vom F-IAM gepflegt werden
- Der Anwender wird im F-IAM oder TN-IAM dem iVBS @rtus zugeordnet
- Das F-IAM ruft die SCIMv2 Operation POST auf den Endpunkt „User“ auf
- Artus trägt den Anwender in Artus als neuen Anwender ein, sofern dieser nicht bereits existent. Keine Fehlermeldung bei existierendem Anwender
- Der Anwender steht nun zur Vergabe von Berechtigungen bereit.
- Ohne Dienststellenzuordnung hat der Anwender kein Recht, sich an Artus anzumelden

Eine Berechtigung des Anwenders durch Zuordnung an eine Dienststelle oder Rollenvergabe kann mit dem Anlegen bereits erfolgen oder später durch andere (nachfolgende) Anwendungsfälle (siehe hierzu die Beschreibung von [\[ANF-020\] \[Stufe 2b\] Zuordnung von Anwender zu Dienststelle](#) bzw. [\[ANF-022\] \[Stufe 2b\] Setzen von Berechtigungen auf Dienststellenebene](#) fortgefahren.)
? erfolgen/ durchgeführt werden..?

4.5 [ANF-011] [Stufe 2a] Deaktivierung (logische Löschung) von Anwendern

Ereignis:

Ein aktiver Anwender soll in @rtus irreversibel deaktiviert werden.

Ziel:

Alle Vorgänge, Rollen und Dienststellen sind vom Anwender entfernt.

Lösungsart:

Automatisiert über Schnittstelle F-IAM.

Es muss technisch geprüft werden, ob die Aktionen asynchron laufen müssen.

Aktionen:

- Die Daten vom zu deaktivierenden Anwender sind bekannt
- Der Anwender wird in der Benutzerverwaltung vom Teilnehmer als „deaktiviert“ im Sinne einer logischen Löschung markiert
- Das F-IAM ruft bei Artus die SCIMv2 Operation DELETE auf den Endpunkt „User“ auf
- Artus führt die Deaktivierung mittels der nachfolgend definierten Szenarien und Prozessschritten durch
- Diese Deaktivierung wird auf allen Dienststellen angewendet und muss vom iVBS vor Rückmeldung an F-IAM auf Erfolg geprüft werden
- Artus protokolliert die Änderungen aus den Szenarien in der Protokoll-Tabelle

Fehlerszenario 1: „Anwender existiert nicht oder ist bereits deaktiviert“

- Vorbedingungen
 - Anwender existiert nicht in Artus oder ist bereits deaktiviert
- Aktionen

- Fehlerquittung an F-IAM
- Eintrag in Logdatei von Artus
- Nachbedingungen
 - F-IAM übernimmt die Fehlerquittung in ein Fehlerprotokoll und informiert ein hinterlegtes Teilnehmerpostfach per Mail über den Fehler
 - Das Fehlerprotokoll bzw. gefundene Abweichungen sollen laut PG IAM für die Teilnehmer einsehbar sein. Die Abweichung muss manuell aufgelöst werden in BV und F-IAM

Szenario 2: „Anwender existiert, ‚normale‘ Rollen, mögl. mit aktiven Vorgängen“

- Vorbedingungen
 - Anwender ist ein aktiver Anwender in Artus
 - Anwender ist der Dienststelle zugeordnet
 - Anwender hat keine Sonderrollen
 - Dienststellenleitung oder Stellv.
 - Gruppenleitung oder Stellv.
 - Registratur
- Aktionen
 - Hat der Anwender noch aktive Vorgänge auf der Dienststelle als Sachbearbeiter
 - Jeder aktive Vorgang wird bearbeitet
 - Es wird ein Eintrag im Lauf des Vorgangs dazu gemacht
 - Vorgang ist einer Gruppe zugeordnet, dann wird der Vorgang in die Gruppenvorlage gebracht
 - Vorgang ist keiner Gruppe zugeordnet, dann wird der Vorgang in die Verwalterliste gebracht
 - Hinweis: Jetziger Webservice von @rtus verfügt bereits über eine solche Umsetzung mit dem Aufruf „force=true“
 - Eintrag in Logdatei von Artus
 - Anwender werden alle Rollen entzogen
 - Anwender wird von der Zuordnung der Dienststelle entfernt
 - Anwender wird in @rtus permanent deaktiviert (logisch gelöscht)
- Nachbedingungen
 - Bei Kriminalaktenhaltung: Die „aktiven“ Merkblätter werden durch die Merkblatteingangsliste und ggf. durch die Merkblattliste Verwaltung auf neue oder bestehende Sachbearbeiter der Kriminalaktenhaltung manuell verteilt
 - Bei Sicherheitsüberprüfung: Die „aktiven“ Sip-Anträge können durch die Mitarbeiter der SiP-Dienststelle auf neue oder bestehende Sachbearbeiter manuell verteilt werden. Hierfür bietet die Antragsliste alle Möglichkeiten der Filterung

Die Verwalter oder Gruppenleiter können die in ihren Eingangslisten liegende Vorgänge erneut auf die Sachbearbeiter verteilen.

Szenario 3: „Anwender existiert und ist Dienststellenleiter“

- Vorbedingungen
 - Anwender ist ein aktiver Anwender in Artus
 - Anwender ist der Dienststelle zugeordnet
 - Anwender hat Sonderrolle „Dienststellenleitung“
 - Besonderheit:

- Dienststellenleitung hat alle Funktionsberechtigung aller Rollen
- Es kann nur eine Dienststellenleitung geben
- Es muss eine Dienststellenleitung eingetragen sein
- Aktionen
 - Es werden die Aktionen wie bei Szenario 2 ausgeführt
 - Dem Anwender werden alle Rollen/Rechte auf der Dienststelle entzogen (weil er gelöscht werden soll)
 - Anwender wird von der Zuordnung der Dienststelle entfernt
 - Der Superuser @rtus-Admin wird interimweise als Dienststellenleitung eingetragen
 - Eine Mail an den @rtus-Support wird versendet, bei dem diese Änderung zur Kenntnis angezeigt wird. Inhalte
 - Ereignis mit Datum und Uhrzeit
 - Betroffene Dienststelle
 - Betroffener Anwender
 - Eintrag in Logdatei von Artus
- Nachbedingungen
 - Es wird davon ausgegangen, dass die interimweise Zuordnung des Superuser @rtus-Admin zeitnah durch eine weitere Zuordnung eines neuen Dienststellenleiters erfolgt

Szenario 4: „Anwender existiert und ist stellv. Dienststellenleiter“

- Vorbedingungen
 - Anwender ist ein aktiver Anwender in Artus
 - Anwender ist der Dienststelle zugeordnet
 - Anwender hat Sonderrolle „Stellv. Dienststellenleitung“
 - Besonderheit:
 - Stellv. Dienststellenleitung hat alle Funktionsberechtigung aller Rollen
 - Es kann mehrere stellv. Dienststellenleitungen geben
- Aktionen
 - Es werden die Aktionen wie bei Szenario 2 ausgeführt
 - Dem Anwender werden alle Rollen/Rechte auf der Dienststelle entzogen
 - Anwender wird von der Zuordnung der Dienststelle entfernt
 - Eintrag in Logdatei von Artus
- Nachbedingungen
 - Keine

Szenario 5: „Anwender existiert ist Gruppenleiter oder stellv. Gruppenleiter“

- Vorbedingungen
 - Anwender ist ein aktiver Anwender in Artus
 - Anwender ist der Dienststelle zugeordnet
 - Anwender hat Sonderrolle „Gruppenleiter oder stellv. Gruppenleiter“
 - Besonderheit:
 - Es kann nur eine Gruppenleitung geben
 - Es muss eine Gruppenleitung geben
 - Gruppenleitung wird nur in @rtus gepflegt
 - Stellv. kann es mehrere geben
- Aktionen
 - Grundsätzliches Vorgehen wie bei Szenario 2

- Ist der Anwender Gruppenleiter einer Gruppe, so wird ein beliebiger Stellv. aus der Gruppe als Gruppenleiter eingetragen. Der Anwender wird damit als Gruppenleiter ausgetragen
 - Gibt es keinen Stellv. in der Gruppe, wird der Dienststellenleiter eingetragen
- Ist der Anwender stellv. Gruppenleiter einer Gruppe, so wird er als Stellv. ausgetragen
- Eintrag in Logdatei von Artus
- Nachbedingungen
 - Keine

Szenario 6: „Anwender existiert und der Anwender ist Mitglied einer Registratur“

- Vorbedingungen
 - Anwender ist ein aktiver Anwender in Artus
 - Anwender ist der Dienststelle zugeordnet
 - Dienststelle verfügt über eine Registratur oder ist zugeordnet
 - Der Anwender ist der Registratur zugeordnet
 - Besonderheit:
 - Registraturen haben auf alle Dienststellen Zugriff in verwaltender Rolle
- Aktionen
 - Grundsätzliches Vorgehen wie bei Szenario 2
 - Der Anwender verliert seine Zuordnung zur Registratur, da ein Mitglied der Registratur auf allen Dienststellen gleich berechtigt und zugeordnet sein muss
 - Die Zuordnung zur Registratur vom Anwender wird aufgehoben
 - Die Rolle Registratur wird bei allen Dienststellen der Registratur vom Anwender entfernt
 - Eintrag in Logdatei von Artus
- Nachbedingungen
 - Keine

4.6 [ANF-012] [Stufe 2a] Pflege und Aktualisierung der Anwenderstammdaten

Ereignis:

Die Stammdaten eines aktiven Anwenders sollen aktualisiert werden. Gängiges Beispiel wäre eine Namensänderung durch Heirat.

Lösungsart:

Automatisiert über Schnittstelle F-IAM

Aktionen:

- Die Daten vom neuen Anwender sind vollständig bekannt
- Der Anwender wird in der Benutzerverwaltung vom Teilnehmer eingetragen
- Sollte der Teilnehmer noch keine Benutzerverwaltung haben, kann diese im Teilnehmer-Verzeichnisdienst angelegt werden und dann über das Web-UI vom F-IAM gepflegt werden
- Der Anwender ist im F-IAM dem iVBS @rtus zugeordnet
- Das F-IAM ruft die SCIMv2 Operation PATCH auf den Endpunkt „User“ auf
- @rtus aktualisiert die Stammdaten, sofern diese in Abschnitt 3.2 abgedeckt sind
- Artus protokolliert die Änderungen aus den Szenarien in der Protokoll-Tabelle

Hinweis von SH: Bei Namensänderung wird derzeit in SH eine neue Windows-Kennung vergeben. Ob dieses dann im Kontext von P20-IAM auch zu einem neuen Account führt, ist derzeit nicht klar. Wäre es so, wären dann die Anwendungsfälle „[ANF-010] [Stufe 2a] Anlage neuer Anwender“ bzw. „[ANF-011] [Stufe 2a] Deaktivierung (logische Löschung) von Anwendern“ durchzuführen.

4.7 [ANF-020] [Stufe 2b] Zuordnung von Anwender zu Dienststelle

Ereignis:

Einem Anwender sollen eine oder mehrere Dienststellen im VBS zugewiesen werden. Eine Rollenvergabe kann zeitgleich erfolgen (Regelfall), muss aber nicht zwingend.

Lösungsart:

Automatisiert über Schnittstelle F-IAM.

Es muss technisch geprüft werden, ob die Aktionen asynchron laufen müssen.

Aktionen:

- Die Daten vom neuen Anwender sind vollständig bekannt
- Der technische Dienststellenschlüssel ist bekannt oder in F-IAM Web-UI oder in der Benutzerverwaltung auswählbar hinterlegt (siehe auch dazu Abschnitt 3.1 und Anforderung [\[ANF-001\]\[Stufe 2a\] Anlage neuer Dienststellen](#))
- Die Rolle(n) sind bekannt, die der Anwender auf der Dienststelle erhalten soll
- Der Anwender mit der Zuordnung zur Dienststelle und ggf. Rolle(n) wird in der Benutzerverwaltung vom Teilnehmer eingetragen
- Sollte der Teilnehmer noch keine Benutzerverwaltung haben, kann diese im Teilnehmerverzeichnisdienst angelegt und dann über das Web-UI vom F-IAM gepflegt werden
- Das F-IAM ruft die SCIMv2 Operation PATCH auf den Endpunkt „OU-Permission“ auf (siehe auch Abschnitt 3.3 und 3.4.)
- Artus führt eine Zuordnung zur Dienststelle und ggf. Vergabe der Rollen mittels der nachfolgend definierten Szenarien und Prozessschritten durch
- Es muss für eine Zuordnung mind. die Rolle „ART_ZO“ gesetzt sein.
- Artus protokolliert die Änderungen aus den Szenarien in der Protokoll-Tabelle

Fehlerszenario 1: „Anwender existiert nicht“

- Vorbedingungen
 - Anwender existiert nicht in Artus oder ist bereits deaktiviert
- Aktionen
 - Auftrag wird ignoriert
 - Eintrag in Logdatei von Artus
 - **Fehlerquittung an F-IAM**
- Nachbedingungen
 - F-IAM übernimmt die Fehlerquittung in ein Fehlerprotokoll und informiert ein hinterlegtes Teilnehmerpostfach per Mail über den Fehler

- Das Fehlerprotokoll bzw. gefundene Abweichungen sollen laut PG IAM für die Teilnehmer einsehbar sein. Die Abweichung muss manuell aufgelöst werden in BV und F-IAM

Fehlerszenario 2: „Dienststelle existiert nicht im Katalog ALLG_DST“

- Vorbedingungen
 - Dienststelle existiert nicht in Artus im Katalog
- Aktionen
 - Auftrag wird ignoriert
 - Eintrag in Logdatei von Artus
 - **Fehlerquittung an F-IAM**
- Nachbedingungen
 - F-IAM übernimmt die Fehlerquittung in ein Fehlerprotokoll und informiert ein hinterlegtes Teilnehmerpostfach per Mail über den Fehler
 - Das Fehlerprotokoll bzw. gefundene Abweichungen sollen laut PG IAM für die Teilnehmer einsehbar sein. Die Abweichung muss manuell aufgelöst werden in BV und F-IAM

Fehlerszenario 3: „Dienststelle ist bereits deaktiviert/stillgelegt“

- Vorbedingungen
 - Dienststelle ist bereits deaktiviert/stillgelegt
- Aktionen
 - Auftrag wird ignoriert
 - Eintrag in Logdatei von Artus
 - **Fehlerquittung an F-IAM**
- Nachbedingungen
 - Das Problem muss nachgehend manuell analysiert und aufgelöst werden

Fehlerszenario 4: „Rollen-Schlüssel unbekannt“

- Vorbedingungen
 - Rollen-Schlüssel unbekannt (siehe Abschnitt 3.4)
- Aktionen
 - Auftrag wird ignoriert
 - Eintrag in Logdatei von Artus
 - **Fehlerquittung an F-IAM**
- Nachbedingungen
 - F-IAM übernimmt die Fehlerquittung in ein Fehlerprotokoll und informiert ein hinterlegtes Teilnehmerpostfach per Mail über den Fehler
 - Das Fehlerprotokoll bzw. gefundene Abweichungen sollen laut PG IAM für die Teilnehmer einsehbar sein. Die Abweichung muss manuell aufgelöst werden in BV und F-IAM

Fehlerszenario 5: „Rollen-Schlüssel ist ungültig“

- Vorbedingungen
 - Rollen-Schlüssel ungültig (siehe Abschnitt 3.4)

- Aktionen
 - Auftrag wird ignoriert
 - Eintrag in Logdatei von Artus
 - Fehlerquittung an F-IAM
- Nachbedingungen
 - F-IAM übernimmt die Fehlerquittung in ein Fehlerprotokoll und informiert ein hinterlegtes Teilnehmerpostfach per Mail über den Fehler
 - Das Fehlerprotokoll bzw. gefundene Abweichungen sollen laut PG IAM für die Teilnehmer einsehbar sein. Die Abweichung muss manuell aufgelöst werden in BV und F-IAM

Szenario 6: „Zuordnung zu einer existierenden aktiven Dienststelle“

- Vorbedingungen
 - Dienststelle existiert und ist aktiv
 - Anwender existiert und ist aktiv
 - Rollen-Schlüssel sind bekannt
 - Rolle ist nicht Dienststellenleiter
 - Es muss für eine Zuordnung mind. die Rolle „ART_ZO“ gesetzt sein
- Aktionen
 - Anwender wird der Dienststelle in @rtus zugeordnet
 - Dem Anwender werden besagte Rollen hinzugefügt
 - Gibt es nur die Rolle „ART_ZO“, wird nur die Zuordnung gemacht
- Nachbedingungen
 - Keine

Szenario 7: „Zuordnung einer existierenden aktiven Dienststelle als Dienststellenleiter“

- Vorbedingungen
 - Dienststelle existiert und ist aktiv
 - Anwender existiert und ist aktiv
 - Neue Rolle ist Dienststellenleiter
 - Besonderheit: Es kann nur ein Anwender Dienststellenleiter sein
- Aktionen
 - Anwender wird der Dienststelle in @rtus zugeordnet
 - Der Anwender wird als Dienststellenleiter eingetragen
 - Der Anwender erhält volle Berechtigung für die Dienststelle
 - Der ursprüngliche Leiter wird als Leiter ausgetragen
- Nachbedingungen
 - Keine

Forderung an BV:

- BV muss sicherstellen, dass die Rolle Dienststellenleiter pro Dienststelle nur einem Anwender vergeben werden kann
- Zusätzlich wird dieser Aspekt auch in Offene Punkte aufgenommen und dort zusammen mit der PG IAM weiterverfolgt
- Vorgabe: Zuerst muss das Recht „Dienststellenleiter“ vom ersten Leiter entfernt und dann erst beim neuen Leiter gesetzt werden. Hierdurch wird eine Inkonsistenz vermieden, da hier die vorhandenen Szenarien durchgeführt werden

Fehlerszenario 8: „Dienststellenbezogene Rolle nicht auf Dienststelle erlaubt“

- Vorbedingungen
 - Anwender und Dienststelle existieren (?)
 - Die Rolle ist eine Rolle, die nur auf bestimmten Dienststellen zulässig ist (z.B. Kriminalaktenhaltung, Sicherheitsprüfung)
- Aktionen
 - Auftrag wird ignoriert
 - Eintrag in Logdatei von Artus
 - **Fehlerquittung an F-IAM**
- Nachbedingungen
 - F-IAM übernimmt die Fehlerquittung in ein Fehlerprotokoll und informiert ein hinterlegtes Teilnehmerpostfach per Mail über den Fehler
 - Das Fehlerprotokoll bzw. gefundene Abweichungen sollen laut PG IAM für die Teilnehmer einsehbar sein. Die Abweichung muss manuell aufgelöst werden in BV und F-IAM

Forderung an BV:

- BV sollte sicherstellen, dass die dienststellenbezogenen Rollen nur auf den Dienststellen vergeben werden können
- Zusätzlich wird dieser Aspekt auch in Offene Punkte aufgenommen und dort zusammen mit der PG IAM weiterverfolgt

4.8 [ANF-021] [Stufe 2b] Löschung einer Zuordnung von Anwender zu Dienststelle

Ereignis:

Ein aktiver Anwender ist einer Dienststelle zugeordnet. Die Zuordnung soll nun aufgehoben werden.

Lösungsart:

Automatisiert über Schnittstelle F-IAM.

Es muss technisch geprüft werden, ob die Aktionen asynchron laufen müssen.

Aktionen:

- Dem Anwender werden über TN-IAM/F-IAM alle Rollen auf der Dienststelle entzogen
- Mit Rolle „ART_ZO“ wird auch die Dienststellenzuordnung durch Artus aufgehoben
- Siehe [\[ANF-023\] \[Stufe 2b\] Löschen von Berechtigungen auf Dienststellenebene](#)

4.9 [ANF-022] [Stufe 2b] Setzen von Berechtigungen auf Dienststellenebene

Ereignis:

Ein aktiver Anwender ist einer Dienststelle zugeordnet und ihm soll eine (weitere) Rolle auf der Dienststelle hinzugefügt werden.

Lösungsart:

Automatisiert über Schnittstelle F-IAM.

Es muss technisch geprüft werden, ob die Aktionen asynchron laufen müssen.

Aktionen:

Die Aktionen und Szenarien sind identisch zu [\[ANF-020\] \[Stufe 2b\] Zuordnung von Anwender zu Dienststelle](#) nur eben mit enthaltender Rollenangabe.

[4.10 \[ANF-023\] \[Stufe 2b\] Löschen von Berechtigungen auf Dienststellenebene](#)

Ereignis:

Ein aktiver Anwender ist einer Dienststelle zugeordnet und ihm soll eine Rolle auf der Dienststelle entzogen werden.

Lösungsart:

Automatisiert über Schnittstelle F-IAM.

Es muss technisch geprüft werden, ob die Aktionen asynchron laufen müssen.

Aktionen:

- Die Daten vom Anwender sind vollständig bekannt
- Der technische Dienststellenschlüssel ist bekannt oder in F-IAM Web-UI oder in der Benutzerverwaltung (BV?) auswählbar hinterlegt (siehe auch dazu Abschnitt 3.1 und Anforderung [\[ANF-001\]\[Stufe 2a\] Anlage neuer Dienststellen](#))
- Die betroffenen Rolle(n) vom Anwender und der Dienststelle werden in der Benutzerverwaltung vom Teilnehmer ausgetragen
- Sollte der Teilnehmer noch keine Benutzerverwaltung haben, kann diese im Teilnehmer-Verzeichnisdienst angelegt werden und dann über das Web-UI vom F-IAM gepflegt werden
- Das F-IAM ruft die SCIMv2 Operation PATCH mit „remove“ auf den Endpunkt „OU-Permission“ auf siehe auch Abschnitt 3.3 und 3.4.
- Artus entzieht dem Anwender die Rollen auf der Dienststelle und wendet hier die Szenarien wie bei [\[ANF-011\] \[Stufe 2a\] Deaktivierung \(logische Löschung\) von Anwendern](#) an, ohne gleich die Zuordnung zu entfernen und ohne den Anwender logisch zu löschen
- Sollte es die letzte Rolle sein, wird die Zuordnung zur Dienststelle aufgehoben
- Artus protokolliert die Änderungen aus den Szenarien in der Protokoll-Tabelle

[4.11 \[ANF-024\] \[Stufe 2a\] Sperrung von Anwendern auf Dienststellen](#)

Ereignis:

Der VBS-Zugang von einem Anwender auf einer konkreten Dienststelle soll für diese Dienststelle gesperrt werden.

Lösungsart:

Organisatorisch über @rtus Anwenderverwaltung.

Aktionen:

- Der Dienststellenleiter, Stellvertreter oder ein Mitarbeiter mit Organisationsrechten auf der Dienststelle nutzt die Anwenderverwaltung und sperrt den Anwender auf seiner Dienststelle.

Es ist davon auszugehen, dass dieser Anwendungsfall ein höchst seltenes Ereignis darstellt, es aber beim Eintritt auch eine zeitliche Dringlichkeit erfordert. Da es auch technisch unter der SCIM-Entität *OUPermissions* gar nicht so trivial abgebildet werden kann, erscheint eine manuelle Lösung hier angemessen. Ebenfalls wird davon ausgegangen, dass dann auch im Nachgang einer rechtmäßigen Sperrung auf einer Dienststelle, der Anwender dann auch seine Zuordnung zur Dienststelle verliert. Dann würden die vorhandenen Szenarien ausgelöst werden.

4.12 [ANF-025] [Stufe 2a] Globale Sperrung von Anwender in @rtus

Ereignis:

Der gesamte VBS-Zugang für einen Anwender soll gesperrt werden, ohne beim Anwender zunächst die Zuordnung oder Berechtigung zu verändern.

Lösungsart:

Automatisiert über Schnittstelle F-IAM.

Aktionen:

- Die Daten vom neuen Anwender sind vollständig bekannt
- Die Sperrung vom Anwender wird in der Benutzerverwaltung als Attribut vom Teilnehmer eingetragen (siehe Abschnitt 3.2)
- Sollte der Teilnehmer noch keine Benutzerverwaltung haben, kann diese im Teilnehmer-Verzeichnisdienst angelegt werden und dann über das Web-UI vom F-IAM gepflegt werden
- Der Anwender ist im F-IAM dem iVBS @rtus zugeordnet
- Das F-IAM ruft die SCIMv2 Operation PATCH-Operation auf den Endpunkt „User“ auf mit dem (?) Attribut active=false
- @rtus setzt die Sperrung am Objekt Anwender
- Artus protokolliert die Änderungen aus den Szenarien in der Protokoll-Tabelle

Die Sperrung zu entfernen ist identisch mit dem obigen Ablauf.

Hinweis: Eine Sperrung über F-IAM ist eine Sperrung auf alle angebundenen Fachverfahren, nicht nur auf das iVBS.

4.13 [ANF-030] [Stufe 2a] Deaktivierung der internen Benutzerverwaltung für externe Provisionierung

Mit der Inbetriebnahme der externen Provisionierung über das F-IAM, verfügt Artus nicht mehr über die Datenhoheit im Bereich der Anwenderverwaltung und Berechtigung. Der Datenbestand von Artus muss also in diesem Bereich (möglichst) synchron zu den Verwaltungsdaten im F-IAM sein. Die Wahrheit der Anwenderverwaltung und Berechtigung liegt demnach im F-IAM.

Damit die Datenbestände vom F-IAM und Artus nicht auseinanderlaufen, dürfen die Daten Anwenderverwaltung und Berechtigung nicht mehr über @rtus veränderbar sein.

In der Stufe 2a werden zunächst keine Berechtigungen vom F-IAM übertragen. Somit sollen diese Anwendungsfälle in @rtus bis zur Stufe 2b weiter genutzt werden können.

Konkret müssen sich folgende Anwendungsfälle per Konfiguration abschalten lassen. Die Masken sollen weiterhin zur Ansicht zugänglich sein. Lediglich die schreibenden Aktionen (inkl. Kontextmenü) sollen deaktiviert werden:

Anwendungsfall: „VBS Anwenderliste“

- Keine Veränderung

Anwendungsfall: „VBS Anwender Hinzufügen“

- Die Suche darf nur noch über die eingetragenen Anwender in Artus gehen
- Es darf keine Suche im Verzeichnisdienst oder AD erfolgen
- Entsprechend dürfen auch keine Anwender aus dem AD oder Verzeichnisdienst übernommen werden

Anwendungsfall: „VBS Anwender Bearbeiten“

- Reiter „Anwenderdaten“
 - Nur noch folgende Felder dürfen editiert werden können:
 - Amtsbezeichnung
 - Alle weiteren Felder sind deaktiviert
- Reiter „Anwenderberechtigung“
 - Unverändert, da Rechte in Stufe 2b noch über Artus vergeben werden
- Reiter „Blockverbund“
 - Bleibt unverändert.

Anmerkung: Amtsbezeichnung soll über IAM/BV pflegbar sein, siehe 14.1. Wurde als Anforderung eingebracht. Sofern sie dort umgesetzt wird, soll die Amtsbezeichnung nicht mehr pflegbar sein.

Anwendungsfall: „@rtus-Admin Anwender Bearbeiten“

- Folgende Felder bleiben aktiv änderbar
 - „Pflege Hilfe“
 - PIAV-OZ-Berechtigung
- Alle anderen Felder werden deaktiviert und sind nur noch lesend einsehbar
- Folgende Aktionen werden deaktiviert:
 - Global sperren
 - Deaktivieren

4.14 [ANF-030] [Stufe 2b] Deaktivierung der internen Benutzerverwaltung für externe Provisionierung

Für Stufe 2b gelten zunächst alle Änderungen, wie diese bereits unter 4.13 beschrieben sind. Ab der Stufe 2b können nun auch Zuordnung zu Dienststellen und Berechtigungen vergeben werden. Auch dieses soll über die Artus-Konfiguration eingestellt werden können.

Hinweis: Es gibt bereits einen Konfigurationswert für einen Modus der internen/externen Berechtigungsverwaltung, der um den Kontext IAM erweitert werden könnte: Siehe „Client-remote-config.properties -> anwenderverwaltung.modus = ?“

Anwendungsfall: „VBS Anwenderliste“

- Aktion „Hinzufügen“ deaktivieren
- Aktion „Dst-Zuordnung aufheben“ deaktivieren
- Aktion „Rollen ändern“ deaktivieren

Anwendungsfall: „VBS Anwender Hinzufügen“

- Entfällt und ist nicht mehr aufrufbar

Anwendungsfall: „VBS Anwender Bearbeiten“

- Reiter „Anwenderdaten“
 - Nur noch folgende Felder dürfen editiert werden können:
 - Amtsbezeichnung
 - Alle weiteren Felder sind deaktiviert
 - Zuordnung aufheben ist deaktiviert
- Reiter „Anwenderberechtigung“
 - Nur Feld „Anwender auf dieser Dienststellesperren“ ist editierbar und aktiv
 - Alle Felder und Aktionen sind deaktiviert, aber lesbar
- Reiter „Blockverbund“
 - Bleibt unverändert

Anwendungsfall: „VBS Dienststellenverwaltung“

- Reiter „Dienststellenleiter“
 - An diesem Reiter sind keine Änderungen mehr erlaubt
 - Nur Anzeige erlaubt

Anwendungsfall: „@rtus-Admin Anwender Bearbeiten“

- Folgende Felder bleiben aktiv änderbar
 - „Pflege Hilfe“
 - PIAV-OZ-Berechtigung
- Alle anderen Felder werden deaktiviert und sind nur noch lesend einsehbar
- Folgende Aktionen werden deaktiviert:
 - Dienststelle hinzufügen
 - Zuordnung aufheben
 - Global sperren

- Deaktivieren
- Es wird ein Konfigurationswert eingeführt, der standardmäßig zur oben beschriebenen Deaktivierung von Feldern und Aktionen führt. Wird der Konfigurationswert geändert, werden die Felder und Aktionen wieder aktiv gesetzt, damit diese bei Bedarf genutzt werden können
- Die Aktivierung bzw. Deaktivierung über einen Konfigurationswert soll es im Konflikt- bzw. Fehlerfall ermöglichen, manuelle Korrekturen in @rtus zum Angleich in Bezug auf F-IAM bzw. BV über die Fachanwendung durchführen zu können

Anwendungsfall: „Admin Dienststellenliste/Hinzufügen“

- Dst-Leiter ist nicht mehr auswählbar und wird vorbelegt mit Superuser Artus-Admin
- Eine Änderung der Dienststellenleitung erfolgt dann über F-IAM

4.15 [ANF-031] [Stufe 2a] Protokollierung und Nachvollziehbarkeit

Log-Einträge in Logdatei und Protokolltabelle

Bereits in den Anforderungsbeschreibungen der vorherigen Abschnitte wurde jeweils beschrieben, dass Einträge in die Protokolltabelle und Log-Dateien vorgenommen werden. Diese werden dann im Abschnitt der Umsetzung jeweils konkretisiert werden. Es gilt die Loggingrichtlinie von Artus (A6).

Speicherung und Verwertung der Nachrichten vom F-IAM

Die Speicherung der Nachrichten vom F-IAM erfolgt in der Artus-Datenbank in einer Tabelle, dabei sollen mindestens folgende Bedarfe berücksichtigt werden:

- Technischer Schlüssel
- Wann wurde die Nachricht vom F-IAM angenommen (Datum, Uhrzeit, sekundengenau)
- Wann wurde die Nachricht von Artus verarbeitet (Datum, Uhrzeit, sekundengenau)
- Inhalt der Nachricht (JSON/SCIMv2 Nachrichten, ggf. komprimiert)
- Art der Nachricht (User, Permission, Operation)
- Protokollverlauf der Verarbeitung (Fließtext)
- Status der Verarbeitung (Erfolg, Fehler)

Ein Eintrag soll bei Bedarf über die Administrationskonsole (Hawtio) vom Applikationsserver abrufbar sein. Diese ist nur dem Verfahrensbetrieb zugänglich. Hierzu wird ein weiterer JMX-Service für IAM hinzugefügt, welche über den technischen Schlüssel die oben genannten Daten und die Nachricht anzeigt.

Für ein fachliches Verfahrensmanagement wird in @rtus-Admin ein Usecase zur Übersicht der IAM-Nachrichten erstellt. Dieser beinhaltet im Wesentlichen:

- Statistische Übersicht zu den Nachrichten
- Auflistung von Nachrichten über Suche von/bis Datum/Uhrzeit
- Suche über Nachrichten-ID von IAM
- Ansicht explizit Nachrichten und deren Verarbeitung
- Nachricht erneut als Kopie einstellen und erneute Verarbeitung anstoßen

Zur Löschung dieser Protokolldaten soll ein Service umgesetzt werden. Dieser Service soll die Nachrichten nach X-Tagen nach Eingangsdatum löschen. Die Anzahl der Tage soll konfigurierbar sein.

Status- und Monitoringdaten für das ULS

Für das ULS sollen die Einträge aus der „Nachrichtentabelle“ mit folgenden Informationen unter dem ULS Abschnitt „Application Server/IAM/Nachrichten“ bereitgestellt werden:

- Technischer Schlüssel
- Wann wurde die Nachricht vom F-IAM angenommen (Datum, Uhrzeit, sekundengenau)
- Wann wurde die Nachricht von Artus verarbeitet (Datum, Uhrzeit, sekundengenau)
- Art der Nachricht (User, Permission, Operation)
- Status der Verarbeitung (Erfolgreich, Fehler)

4.16 [ANF-032] Lesende Zugriffe für F-IAM: Abfrage von Benutzerdaten

Die SCIMv2-Spezifikation der PG IAM (A1.1) gibt zwei GET-Operationen, um durch das F-IAM abfragen auf den Bestand der Benutzer im iVBS @rtus durchzuführen.

/Users	GET	Abfrage aller Benutzer	immer
	POST	Erstellen eines neuen Benutzers	immer
/Users/{User-ID}	GET	Abfrage eines konkreten Benutzers, ID wird von AW vergeben Liefert auch die Liste aller Berechtigungszuweisungen (auch mit OU-Bezug), sofern es nicht über Query-Parameter unterbunden wird.	immer

Die Abfragen müssen nach Vorgaben der Spezifikation unter 1.4.3 Suchen (Search) und 1.4.4 Abfragen (WellKnown) (A1.1.) umgesetzt werden. Die Abfragen liefern Informationen über den Bestand der Benutzer, sowie im Detail alle Attribute, Dienststellenzuordnungen und Rechte mit dem Umfang, wie sie unter Abschnitt 3.2, 3.3 und 3.4 beschrieben sind.

Diese Abfragen können dann nicht nur vom F-IAM genutzt werden, sie können dann auch im Rahmen einer Migration von einer Artus-internen Benutzerverwaltung auf einer (neuen) BV des Teilnehmers genutzt werden.

4.17 [ANF-033] Lesende Zugriffe für F-IAM: Abfrage von VBS-Rechten

/OU-Permissions	GET	Abfrage von Rechten mit OE-Bezug, die für die AW zugewiesen werden können Liefert auch die Liste der Zuweisungen, sofern es nicht über Query-Parameter unterbunden wird.	für AW mit Berechtigungen mit OE-Bezug
/OU-Permissions/{OU-Permission-ID}	GET	Liefert auch die Liste der Zuweisungen, sofern es nicht über Query-Parameter unterbunden wird.	

Die Abfragen müssen nach Vorgaben der Spezifikation unter „1.1.2 Berechtigungsdefinitionen Abfragen“ und „1.1.3 Berechtigungszuweisungen Abfragen“ (A1.1.) umgesetzt werden. Die erste liefert eine Liste der möglichen Rechte mit OE-Bezug (Dienststellenbezug), die im VBS momentan vergeben werden können. Diese Liste ergibt sich aus den aktuellen Rollen, die im iVBS konfiguriert sind.

Die zweite Abfrage liefert eine Liste mit Benutzern, die ein angefragtes Recht zugewiesen bekommen haben.

Diese Abfragen können dann nicht nur vom F-IAM genutzt werden, sie können dann auch im Rahmen einer Migration von einer Artus-internen Benutzerverwaltung auf eine (neue) BV des Teilnehmers genutzt werden.

Hinweis: Die Operationen sind beide zwar in der Spezifikation aufgeführt, aber inhaltlich noch nicht beschrieben und mit Beispielen versehen.

5 Umsetzung Allgemein

Die folgenden Abschnitte beschreiben die Umsetzung des zuvor skizzierten Lösungsansatzes und die Anforderungen aus den Abschnitten 3 und 4.

Da die vorangegangenen Abschnitte teilweise bereits auch detaillierte Vorgaben zur Umsetzung gemacht haben, werden die Ausführungen in den nächsten Abschnitten nur Ergänzungen vornehmen und notwendige sowie offene Vorgaben zur Umsetzung vervollständigen, um redundante Ausführungen zu vermeiden. Ziel der nächsten Abschnitte ist es, eine gemeinsame Vorstellung von der Umsetzung der Anforderungen darzustellen, ohne zu kleinteilig zu werden.

Da dieses Konzept vor allem die Anforderungen und Umsetzung einer technischen Schnittstelle beschreibt, lässt es sich auch nicht ganz vermeiden, im Folgenden auch einige technische Aspekte der Umsetzung zu beschreiben.

5.1 Technische Komponentenübersicht

Die nachfolgende Komponentenübersicht lehnt sich an der Darstellung aus Abschnitt 3 (Abbildung 10) an, wobei in dieser Ansicht die wesentlichen technische Umsetzungskomponenten vom iVBS dargestellt werden. Diese Komponenten werden dann im Folgenden kurz tabellarisch beschrieben. Die notwendigen Umsetzungsdetails der beteiligten Komponenten werden in den nachfolgenden Abschnitten weiter ausgeführt.

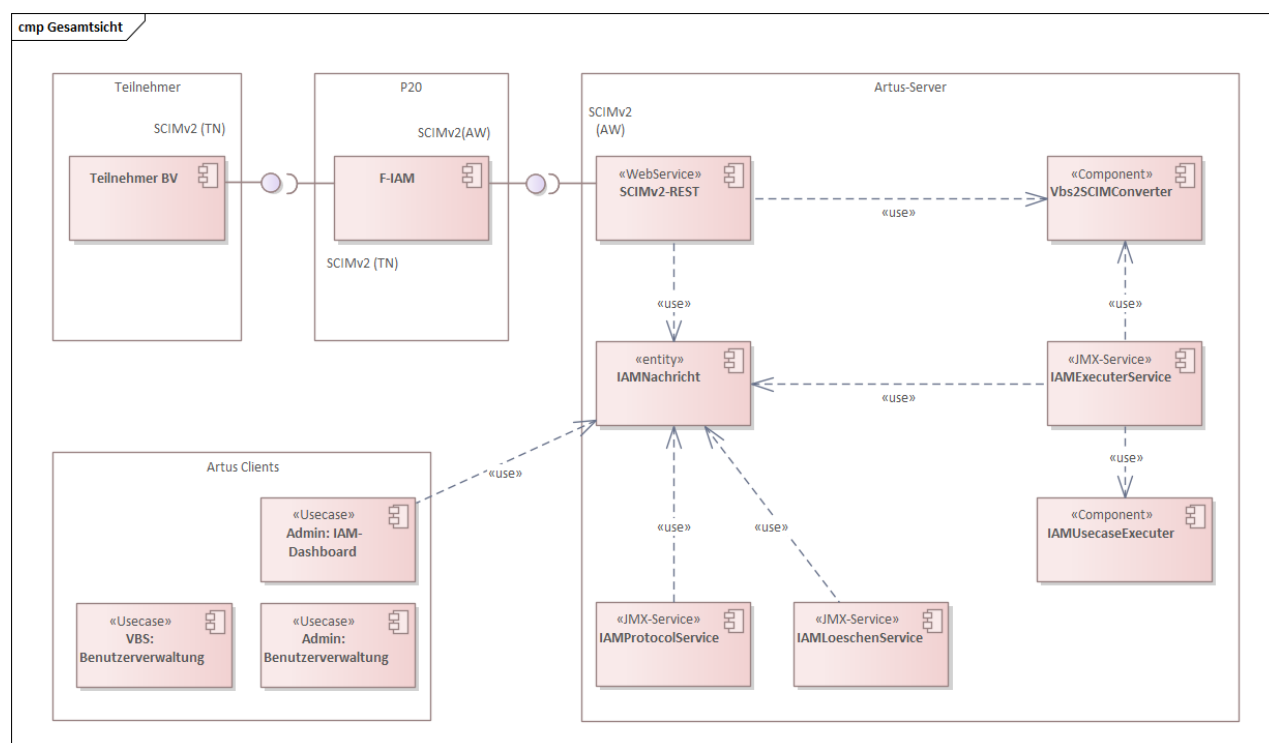


Abbildung 13: Technische Komponentenübersicht

Komponente	Umsetzungsmerkmale/-beschreibung
SCIMv2-REST-Service Webservice	<p>Diese Komponente setzt den SCIM-Webservice um. Sie stellt somit die Schnittstelle für das F-IAM zur Verfügung und basiert auf den Vorgaben der SCIM-Spezifikation der PG IAM (AW) (A1.1).</p> <p>Aufgaben:</p> <ul style="list-style-type: none"> Annahme von SCIM-Nachrichten von F-IAM. Umsetzung der Endpunkte Validierung und Konsistenzprüfung der Nachricht nach SCIMv2 und IAM-Spezifikation Vorprüfung nach Anforderungen @rtus Für <u>lesende</u> Operationen: Direkte synchrone Verarbeitung und Beantwortung <ul style="list-style-type: none"> Für Endpunkt Operation GET-Anfragen Führt Anfragen über Fachobjekte mittels Filter auf der DB aus, um Daten zu laden Nutzt den <i>VBS2SCIMConverter</i> für Konvertierung zum SCIM-Format Erzeugt die Ergebnismeldung und führt Sendung der Antwort aus Protokolliert das Ereignis als "<i>IAMNachricht</i>" Für <u>ändernde</u> Operationen: Asynchrone Verarbeitung durch "<i>IAMExecuterService</i>" <ul style="list-style-type: none"> Für Endpunkt Operation PATCH, POST, DELETE Aufgrund asynchroner Verarbeitung, sendet der Service positive Quittierung an F-IAM nach Speicherung der Nachricht Sollte später ein Fehler bei der Verarbeitung auftreten, werden die Zuständigen per Mail ans Postfach und über Admin-Client Ansicht und ULS benachrichtigt
IAMNachricht Entity/Fachobjekt	<p>Neues Fachobjekt in @rtus, um Nachrichten aus SCIM persistent zu speichern. Dieses neue Fachobjekt hält Metadaten zur Nachricht und Verarbeitung sowie die SCIM-Anfrage und eine mögliche Antwort bzw. Quittierung seitens @rtus vor. Es werden alle Nachrichten von jedem Endpunkt hier gespeichert.</p> <p>Für ändernde Operationen dienen diese Fachobjekte/Tabelle als Warteschlange, um die einzelnen Änderungen und notwendigen Anpassungen vorzuhalten, die dann asynchron von den anderen Komponenten verarbeitet werden.</p>
VBS2SCIMConverter SW-Komponente	Hilfskomponente zur Konvertierung von VBS-Zustand der Objekte Anwender, Dienststelle und Benutzerechte zur jeweiligen SCIM-Abbildung (User, OU-Permission).
IAMExecuterService JMX-Service	<p>Dieser serverseitige Dienst fragt zyklisch die unbearbeiteten IAM-Nachrichten ab. Die Abfrage erfolgt geordnet und stellt somit die korrekte Verarbeitungsreihenfolge sicher. Der Dienst analysiert anhand der Operation und Endpunkt die in Frage kommenden Anwendungsfälle und lässt diese dann ausführen. Der Dienst übernimmt hierbei die Transaktionssteuerung und Fehlerhandling.</p> <p>Der Dienst dokumentiert das Ergebnis und den Status in der <i>IAMNachricht</i>.</p>
IAMUsecaseExecuter SW-Komponente	<p>Diese Software-Komponente(n) setzt jeweils einen oder mehrere Anwendungsfälle aus den Anforderungen und Szenarien aus Abschnitt 4 um. Die Komponente wird vom <i>IAMExecuterService</i> aufgerufen. Zunächst werden bei Ausführung die Voraussetzungen geprüft und dann das besagte Szenario ausgeführt.</p> <p>Der Verlauf wird im einen Textprotokoll festgehalten und an den <i>IAMExecuterService</i> mit dem Gesamtergebnis (z.B. erledigt, Fehler) zurückgegeben.</p>
IAMProtocolService JMX-Service	<p>Dieser serverseitige JMX-Dienst ermittelt alle 5 Minuten die Erkenntnisse aus der Tabelle <i>IAMNachricht</i>. Der Dienst liefert dann alle Nachrichten mit den gewünschten Metadaten an das ULS. Mögliche Fehler werden als Emails laut Anforderung an konfigurierte Postfächer versandt. Der JMX-Service wird auch über einige Operationen verfügen, um Nachrichten bei Bedarf vollständig einsehen zu können.</p>
IAMLoeschenService JMX-Service	<p>Dieser serverseitige JMX-Dienst prüft alle 30 Minuten die Tabelle <i>IAMNachricht</i> und ermittelt alle Nachrichten, die gelöscht werden sollen und führt die physische Löschung aus. Die Ermittlung erfolgt wie in der Anforderung beschrieben, nach X-Tagen nach Nachrichteneingang.</p>
Admin: IAM-Dashboard Client-Usecase	<p>Das IAM-Dashboard ist ein neuer Usecase in @rtus-Admin. Dieser Usecase setzte die Anforderung [ANF-031] [Stufe 2a] Protokollierung und Nachvollziehbarkeit um. Der Usecase bietet dem Anwender der produktverantwortlichen Stelle @rtus die Möglichkeit, die Fachobjekte aus der Entität <i>IAMNachricht</i> abzufragen, zu filtern und im Detail einzusehen. Aus diesem Usecase heraus können auch Nachrichten inkl. Verlauf und Antwort als Mail zur weiteren Analyse versandt werden.</p>
Admin: Benutzerverwaltung Client-Usecase	<p>Dieser Usecase ist bereits in @rtus-Admin vorhanden und wird gemäß den Anforderungen [ANF-030] [Stufe 2a] und [ANF-030] [Stufe 2b] „Deaktivierung der internen Benutzerverwaltung für externe Provisionierung“ angepasst.</p>

VBS: Benutzerverwaltung Client-Usecase

Dieser Usecase ist bereits in @rtus-VBS vorhanden und wird gemäß den Anforderungen [ANF-030] [Stufe 2a] und [ANF-030] [Stufe 2b] „Deaktivierung der internen Benutzerverwaltung für externe Provisionierung“ angepasst.

Abbildung 14: Kurzbeschreibung der Umsetzungskomponenten

Der Entwicklung steht es frei, sowohl die Benennung der Komponenten anzupassen, als auch eine mögliche weitere Differenzierung der notwendigen Komponenten vorzunehmen.

6 Umsetzung Datenmodell und Schnittstelle

Dieser Abschnitt beschreibt die Umsetzungspunkte bezüglich der wesentlichen Software-Komponenten, wie sie bereits unter 5.1 vorgestellt worden sind und führt diese weiter aus.

6.1 Entität/Fachobjekt „IAMNachricht“

Dieses neue Fachobjekt dient dazu, die IAM-Nachrichten aus SCIM persistent zu speichern. Das Fachobjekt hält Metadaten zur Nachricht und zur Verarbeitung sowie die SCIM-Anfrage und eine mögliche Antwort (bzw. Quittierung) @rtus vor. Es werden alle Nachrichten von jedem Endpunkt hier gespeichert. Damit dient das Fachobjekt der Anforderung „[ANF-031] Protokollierung und Nachvollziehbarkeit“.

Für ändernde Operationen dienen diese Fachobjekte/Tabelle als Warteschlange, um die einzelnen Änderungen und notwendigen Anpassungen vorzuhalten, die dann asynchron von den anderen Komponenten verarbeitet werden.

Folgender Vorschlag wird für eine Umsetzung gemacht:

Attribut	Typ	Kardinalität	Beschreibung
oid	Number	1:1	ID der Entität (automatische Sequenz)
NID	String	1:1	Nachricht-ID aus SCIM-Nachricht
Version	String	1:1	Schnittstellen-Version
Endpunkt	String	1:1	Aufgerufener Endpunkt (User, OU-Permissions)
Operation	String	1:1	Auszuführende Operation (GET, POST, PATCH, DELETE)
Erzeugt	Datum/Uhrzeit	1:1	Eingangsdatum der Nachricht
Status	Enum	1:1	Ergebnis der Verarbeitung (Fehler, Pending, Finish)
Erledigt	Datum/Uhrzeit	0:1	Datum/Uhrzeit Ende der Verarbeitung
Anfragenachricht	Binary	1:1	SCIM-Nachricht, Zip
Anwender	Anwender	0:1	Betroffener Anwender
Dienststelle	Dienststelle	0:1	Betroffene Dienststelle
Verlaufslog	Text	0:1	Informationen zum Verlauf der Verarbeitung

Antwortnachricht	Binary	0:1	SCIM-Nachricht / Quittung als Antwort, Zip
------------------	--------	-----	--

Abbildung 15: Übersicht neues Fachobjekt IAMNachricht

Der Entwicklung steht es frei, hier erforderliche Anpassungen und Änderungen während der Umsetzung zu machen.

6.2 Webservice „SCIMv2-REST-Service“

Diese Komponente setzt den SCIMv2-Webservice um. Es setzt somit die Schnittstelle für das F-IAM um und basiert auf den Vorgaben der SCIMv2-Spezifikation der PG IAM für Anwendungen (A1.1).

Der Webservice übernimmt im Wesentlichen zwei Aufgaben: Zunächst nimmt er alle lesenden Operationen der SCIMv2-Schnittstelle an, führt diese synchron aus und liefert das Ergebnis synchron an das F-IAM zurück.

Des Weiteren nimmt der Webservice auch alle verändernden Operationen an, validiert diese soweit wie zu diesem Zeitpunkt möglich und speichert diese für die asynchrone Abarbeitung durch die Komponente „IAMExecutorService“.

Die nachfolgende Tabelle gibt eine Aufschlüsselung, welche SCIM-Endpunkte und Operationen wie vom Webservice verarbeitet werden sollen und welche Anwendungsfälle aus Abschnitt 4 betroffen sind. In kursiv sind die Erläuterungen aus der Spezifikation der PG IAM (A1.1) enthalten.

Endpunkt	Operation	Umsetzungsmerkmale/-beschreibung
/ServiceProvider-Config	GET	<ul style="list-style-type: none"> Spezifikation: Schemas, Users, Groups, +? liefert auch die URLs der Endpunkte Muss noch geklärt werden, wie die konkrete Antwort aussehen soll Umsetzung in <ul style="list-style-type: none"> SCIMv2-REST-Service
/ResourceTypes	GET	<ul style="list-style-type: none"> Spezifikation: Capabilities, AuthMechanismen, ... Muss noch geklärt werden, wie die konkrete Antwort aussehen soll Umsetzung in <ul style="list-style-type: none"> SCIMv2-REST-Service
/Schemas	GET	<ul style="list-style-type: none"> Spezifikation: relevant? Muss noch geklärt werden, wie die konkrete Antwort aussehen soll Umsetzung in <ul style="list-style-type: none"> SCIMv2-REST-Service
/Users	GET	<ul style="list-style-type: none"> Spezifikation: Abfrage aller Benutzer Auch mit Parameter GET /Users?startIndex=1&count=10 Siehe Spezifikation AW & TN 1.4.3 Suchen (Search) Wird genutzt im Anwendungsfall <ul style="list-style-type: none"> [ANF-032] Lesende Zugriffe für F-IAM: Abfrage von Benutzerdaten Umsetzung in/mit <ul style="list-style-type: none"> SCIMv2-REST-Service Konverter VBS2SCIMConverter
/Users	POST	<ul style="list-style-type: none"> Spezifikation: Erstellen eines neuen Benutzers Wird genutzt im Anwendungsfall <ul style="list-style-type: none"> [ANF-010] [Stufe 2a] Anlage neuer Anwender [ANF-025] [Stufe 2a] Globale Sperrung von Anwendern in @rtus und indirekt durch Mitgabe von Permissions [ANF-020] [Stufe 2b] Zuordnung von Anwender zu Dienststelle [ANF-022] [Stufe 2b] Setzen von Berechtigungen auf Dienststellenebene Umsetzung in/mit

		<ul style="list-style-type: none"> ◦ SCIMv2-REST-Service ◦ Konverter VBS2SCIMConverter ◦ Asynchroner "IAMExecutorService" ◦ IAMUsecaseExecutor
/Users/{User-ID}	GET	<ul style="list-style-type: none"> • Abfrage eines konkreten Benutzers, ID wird von AW vergeben. Liefert auch die Liste aller Berechtigungszuweisungen (auch mit OUBezug), sofern es nicht über QueryParameter unterbunden wird. • Auch 1.4.4.1 Parameter attributes/excludedAttributes notwendig • Wird genutzt im Anwendungsfall <ul style="list-style-type: none"> ◦ [ANF-032] Lesende Zugriffe für F-IAM: Abfrage von Benutzerdaten • Umsetzung in/mit <ul style="list-style-type: none"> ◦ SCIMv2-REST-Service ◦ Konverter VBS2SCIMConverter
/Users/{User-ID}	PATCH	<ul style="list-style-type: none"> • Spezifikation: Ändern von Benutzerattributen • Anwendungsfall <ul style="list-style-type: none"> ◦ [ANF-012] [Stufe 2a] Pflege und Aktualisierung der Anwenderstammdaten ◦ [ANF-025] [Stufe 2a] Globale Sperrung von Anwender in @rtus • Umsetzung in/mit <ul style="list-style-type: none"> ◦ SCIMv2-REST-Service ◦ Konverter VBS2SCIMConverter ◦ Asynchroner "IAMExecutorService" ◦ IAMUsecaseExecutor
/Users/{User-ID}	DELETE	<ul style="list-style-type: none"> • Spezifikation: Löschen eines Benutzers • Wird genutzt im Anwendungsfall <ul style="list-style-type: none"> ◦ [ANF-011] [Stufe 2a] Deaktivierung (logische Löschung) von Anwendern • Umsetzung in/mit <ul style="list-style-type: none"> ◦ SCIMv2-REST-Service ◦ Konverter VBS2SCIMConverter ◦ Asynchroner "IAMExecutorService" ◦ IAMUsecaseExecutor
/OU-Permissions	GET	<ul style="list-style-type: none"> • Spezifikation: Abfrage von Rechten mit OE-Bezug, die für die AW zugewiesen werden können Liefert auch die Liste der Zuweisungen, sofern es nicht über Query-Parameter unterbunden wird • Auch GET /Users?startIndex=1&count=10, Siehe Spezifikation AW&TN 1.4.3 Suchen (Search) • Wird genutzt im Entspricht Anwendungsfall <ul style="list-style-type: none"> ◦ [ANF-033] Lesende Zugriffe für F-IAM: Abfrage von VBS-Rechten • Umsetzung in/mit <ul style="list-style-type: none"> ◦ SCIMv2-REST-Service ◦ Konverter VBS2SCIMConverter
/OU-Permissions/{OU-Permission-ID}	GET	<ul style="list-style-type: none"> • Spezifikation: Liefert auch die Liste der Zuweisungen, sofern es nicht über Query-Parameter unterbunden wird. • Auch GET /Users?startIndex=1&count=10, Siehe Spezifikation AW&TN 1.4.3 Suchen (Search) • Auch 1.4.4.1 Parameter attributes/excludedAttributes notwendig? • Entspricht Anwendungsfall <ul style="list-style-type: none"> ◦ [ANF-033] Lesende Zugriffe für F-IAM: Abfrage von VBS-Rechten • Umsetzung in/mit <ul style="list-style-type: none"> ◦ SCIMv2-REST-Service ◦ Konverter VBS2SCIMConverter
/OU-Permissions	PATCH	<ul style="list-style-type: none"> • Spezifikation: Berechtigungszuweisung mit OE-Bezug hinzufügen/entfernen • Wird genutzt im Anwendungsfall <ul style="list-style-type: none"> ◦ [ANF-020] [Stufe 2b] Zuordnung von Anwender zu Dienststelle ◦ [ANF-021] [Stufe 2b] Löschung einer Zuordnung von Anwender zu Dienststelle ◦ [ANF-022] [Stufe 2b] Setzen von Berechtigungen auf Dienststellenebene ◦ [ANF-023] [Stufe 2b] Löschen von Berechtigungen auf Dienststellenebene ◦ [ANF-024] [Stufe 2a] Sperrung von Anwendern auf Dienststellen • Umsetzung in/mit <ul style="list-style-type: none"> ◦ SCIMv2-REST-Service ◦ Konverter VBS2SCIMConverter

		<ul style="list-style-type: none"> ○ Asynchroner "IAMExecuterService " ○ IAMUsecaseExecuter
--	--	---

Abbildung 16: Gegenüberstellung SCIMv2-Endpunkte, Anforderungen und Umsetzung

Bei lesenden Operationen (GET) protokolliert der Webservice selber die Nachricht und das Ergebnis in Fachobjekt *IAMNachricht* und setzt den Status entsprechend als abgeschlossen oder auf Fehler. Das Mapping vom Fachmodell Artus (Anwender, Dienststelle, Rechte) wurde bereits in den Abschnitten 3.2 und 3.4 erörtert.

Der Webservice wird eine technische Validierung der Nachricht vornehmen (nach SCIMv2 der PG IAM A1.1). Des Weiteren wird der Webservice eine fachliche Validierung der Nachricht vornehmen, sofern diese bereits vor der eigentlichen Verarbeitung möglich ist. Ziel dieser fachlichen Validierung ist es, möglichst synchron bereits Fehlerzustände an das F-IAM melden zu können. Folgende Anwendungsfälle bzw. Szenarien sollten einer Validierung unterliegen:

- [ANF-011] [Stufe 2a][S1]
- [ANF-020] [Stufe 2b][S1]
- [ANF-020] [Stufe 2b][S2]
- [ANF-020] [Stufe 2b][S3]
- [ANF-020] [Stufe 2b][S4]
- [ANF-020] [Stufe 2b][S5]
- [ANF-020] [Stufe 2b][S8]

Die Schnittstelle soll über ein Konfigurationsdienst gestoppt werden können. Ist die Schnittstelle gestoppt, quittiert sie jede Anfrage mit Http 503 „Service Unavailable“. Der Dienst soll über einen Konfigurationswert in *artus-server.properties* gesteuert werden. Er soll auch direkt über den JMX-Dienst „*IAMExecuterService*“ gesetzt werden können.

6.3 JMX-Dienst „IAMExecuterService“

Dieser serverseitige Dienst wird als JMX-Dienst umgesetzt. Der Dienst fragt zyklisch die unbearbeiteten IAM-Nachrichten ab (Status „Pending/Wartend“). Die Abfrage erfolgt geordnet und stellt somit die korrekte Verarbeitungsreihenfolge sicher. Dieses kann über die Sortierung mittels Eingangsdatums bzw. OID erreicht werden.

Der Dienst analysiert aufgrund von Operation und Endpunkt die in Frage kommenden Anwendungsfälle und lässt diese dann über die jeweiligen SW-Komponente „*IAMUsecaseExecuter*“ ausführen. Der Dienst übernimmt hierbei die Transaktionssteuerung und das Fehlerhandling.

Der Dienst dokumentiert das Ergebnis und Status in der *IAMNachricht*.

Als JMX-Dienst ist er entsprechend über die JMX-Konsole „Hawtio“ zu starten und zu stoppen. Der Dienst wird mit Start des Artus-Server gestartet. Es gibt nur eine laufende Instanz vom Service, damit Nachrichten in der richtigen Reigenfolge der Eingänge verarbeitet werden. Der Dienst läuft permanent und macht nach jedem Durchlauf eine konfigurierbare Zeit in Millisekunden Pause (voreingestellt 30 Sekunden). Ein Durchlauf arbeitet am Stück eine konfigurierbare Menge an Nachrichten ab (voreingestellt 50). Beide Werte können über *artus-server.properties* konfiguriert oder am JMX-Dienst direkt gesetzt werden.

Der Dienst bietet auch eine JMX-Operation an, um auch den Webservice zu starten bzw. zu stoppen.

6.4 Komponente „IAMUsecaseExecuter“

Die Software-Komponente „IAMUsecaseExecuter“ repräsentiert die Umsetzung einer oder mehrerer der Anforderungen bzw. Szenarien aus Abschnitt 4, die durch ändernde Operation (POST, PATCH, DELETE) durch das F-IAM ausgelöst werden. Konkret sind folgende Anforderungen (Use-case) betroffen:

- [ANF-010] Anlage neuer Anwender
- [ANF-011] Deaktivierung (logische Löschung) von Anwendern
- [ANF-012] Pflege und Aktualisierung der Anwenderstammdaten
- [ANF-020] Zuordnung von Anwender zu Dienststelle
- [ANF-021] Löschung einer Zuordnung von Anwender zu Dienststelle
- [ANF-022] Setzen von Berechtigungen auf Dienststellenebene
- [ANF-023] Löschen von Berechtigungen auf Dienststellenebene
- [ANF-025] Globale Sperrung von Anwender in @rtus

Der jeweilige Usecase wird entsprechend in einer SW-Komponente umgesetzt und beim *IAMExecuterService* für einen bestimmten Endpunkt und Operation registriert. Wird eine entsprechende Operation am entsprechenden Endpunkt ausgelöst und über die Warteschlange als *IAMNachricht* bezogen, führt der *IAMExecuterService* die registrierten *IAMUsecaseExecuter* aus.

Bei der Ausführung protokolliert der *IAMUsecaseExecuter* den Verlauf der Ausführung und meldet das Ergebnis als Erfolg oder Fehler inklusive des Verlaufs zurück.

Die Aufteilung der Anwendungsfälle und Szenarien wird hier nicht vorgegeben.

Ein *IAMUsecaseExecuter* muss auch eine Möglichkeit anbieten, um bei der Annahme der Nachricht durch den *SCIMv2-REST-Service* eine Validierung durchzuführen. Hierzu wendet sich der *SCIMv2-REST-Service* an den *IAMExecuterService*, der wiederum die Validierung an die passenden *IAMUsecaseExecuter* delegiert. Hierdurch bleibt die gesamte Geschäftslogik für den Anwendungsfall bzw. das Szenario in der jeweiligen Software-Komponente vom *IAMUsecaseExecuter* gekapselt.

6.5 JMX-Dienst „IAMProtocolService“

Der *IAMProtocolService* setzt Teile der Anforderung „[ANF-031] [Stufe 2a] Protokollierung und Nachvollziehbarkeit“ Abschnitt 4.15 um. Der *IAMProtocolService* wird als serverseitige JMX-Dienst umgesetzt. Er ermittelt alle 5 Minuten (per Job über JMX-Scheduler, konfigurierbar über Scheduler-Service) die Erkenntnisse aus der Tabelle *IAMNachricht*. Der Dienst liefert dann alle Nachrichten mit den gewünschten Metadaten aus der Anforderung [ANF-031] an das ULS.

Mögliche Fehler werden als Emails laut Anforderung an konfigurierte Postfächer versandt. Die Postfächer werden in *artus-server.properties* als Parameter hinterlegt und es können auch mehrere Postfächer als komma-separierte Liste hinterlegt werden.

Der JMX-Service wird auch über einige Operationen verfügen, um Nachrichten bei Bedarf vollständig einsehen zu können.

6.6 JMX-Dienst „IAMLoeschenService“

Der *IAMLoeschenService* setzt die Anforderung der Löschung aus [ANF-031] [Stufe 2a] „Protokollierung und Nachvollziehbarkeit“ (Abschnitt 4.15) um. Dieser serverseitige JMX-Dienst prüft alle 30 Minuten die Tabelle *IAMNachricht* und ermittelt alle Nachrichten, die gelöscht werden sollen

und führt die Löschung aus. Die Ermittlung erfolgt wie in der Anforderung beschrieben, nach X-Tagen (voreingestellt auf 90 Tage) nach Nachrichteneingang.

Die Anzahl der Löschungen wird der Log-Datei und im ULS vermerkt.

7 Umsetzung VBS

7.1 [ANF-030] [Stufe 2a][Stufe 2b] - Umsetzung VBS-Client

Dieser Abschnitt beschreibt die Umsetzung der Anforderung [ANF-030] [Stufe 2a][Stufe 2b] aus Abschnitt 4.13 und 4.14 zur „Deaktivierung der internen Benutzerverwaltung für externe Provisionierung“ im iVBS-Client.

Derzeit gibt es in der „client-remote-config.properties“ drei Modi für die Anwenderverwaltung:

normal	Anwenderverwaltung ist schreibend und uneingeschränkt nutzbar (default, SH, HB)
hbv	Anwenderverwaltung wird schreibend geöffnet. Rollen und Funktionsberechtigungen werden ausgeblendet. Blockverbunde können aber zugewiesen werden. (BPOL)
readonly	Anwenderverwaltung wird nur lesend geöffnet (ST)

Diese Modi werden um folgende erweitert:

iam_hbv	Anwenderverwaltung ist im IAM-Modus. Die HBV bleibt weiterhin den Client nutzbar. Es werden die Felder gemäß Anforderung [ANF-030] [Stufe 2a/b] umgesetzt, sofern sie durch diesen Modus überhaupt sichtbar sind. (BPOL)
iam_2a_normal	Es werden die Felder gemäß Anforderung [ANF-030] [Stufe 2a] umgesetzt. HBV bleibt änderbar. (SH, HB, RP, SL)
iam_2b_normal	Es werden die Felder gemäß Anforderung [ANF-030] [Stufe 2b] umgesetzt. HBV bleibt änderbar. (SH, HB, RP, SL)
iam_readonly	Anwenderverwaltung ist im IAM-Modus. Anwenderverwaltung wird nur lesend geöffnet. Weder HB, Rechte noch Attribute vom Anwender sind änderbar. Dieser Modus deckt damit automatisch [ANF-030] [Stufe 2a/2b] ab. (ST)

Abbildung 17: Neue Konfigurationswerte für Anwenderverwaltung

Entsprechend sind die Usecases Anwenderverwaltung und Dienststellenverwaltung entsprechend den Vorgaben aus [ANF-030] anzupassen.

8 Umsetzung @rtus-Admin

8.1 [ANF-030] [Stufe 2a][Stufe 2b] - Umsetzung Admin-Client

Dieser Abschnitt beschreibt die Umsetzung der Anforderung aus Abschnitt 4.13 und 4.14 zur „Deaktivierung der internen Benutzerverwaltung für externe Provisionierung“ im Admin-Client. Dort ist der Usecase „Anwender Bearbeiten“ betroffen.

In der „client-remote-config.properties“ wird ein neuer Parameter „anwenderverwaltung.admin.modus“ eingeführt. Dieser kann folgende Werte annehmen:

iam_off	IAM ist abgeschaltet. Alle Felder und Funktionen sind aktiv (voreingestellt).
iam_2a	Es werden die Felder gemäß Anforderung [ANF-030] [Stufe 2a] umgesetzt. HBV bleibt änderbar.
iam_2b	Es werden die Felder gemäß Anforderung [ANF-030] [Stufe 2b] umgesetzt. HBV bleibt änderbar.
iam_changemode	IAM ist eigentlich aktiv, aber für notwendige Korrekturen im VBS werden in diesem Modus gemäß Anforderung [ANF-030] [Stufe 2a/b] „@rtus-Admin Anwender Bearbeiten“ die Felder und Aktionen aktiviert, wenn dieser Konfigurationswert gesetzt ist.

Abbildung 18: Neue Konfigurationswerte für @rtus-Admin

Entsprechend sind die Usecases ist entsprechend den Vorgaben aus [ANF-030] anzupassen.

8.2 [ANF-031] [ANF-031][Stufe 2a] Protokollierung und Nachvollziehbarkeit

Das Dashboard für @rtus-Admin soll hier nicht im Detail vorgegeben werden. Das Dashboard soll eine Abfrageleiste im oberen Bereich bekommen, welche eine Suche über Datum von/bis über die IAM-Nachrichten ermöglicht.

Die Trefferanzeige wird als Trefferliste direkt unter der Suchleiste dargestellt. Sie enthält, bis auf die eigentlichen Nachrichteninhalte, alle fachlich informativen Attribute vom Fachobjekt IAM-Nachricht.

Mit Doppelklick kann man die IAM-Nachricht vollständig einsehen in einer weiteren Maske oder in einem Dialog.

In der Buttonleiste der Suchmaske wird ebenfalls angeboten, eine ausgewählte IAM-Nachricht an eine einzugeben Emailadresse auszuleiten. Der Inhalt sind dann die jeweiligen Nachrichten als Anhänge sowie die Attribute der IAM-Nachricht. Die Ausleitung kann über den vorhandenen SMTP-Zugang von dem Artus-Server erfolgen.

9 Umsetzung @rtus-Recherche

Dieses Fachkonzept hat keine Auswirkung auf die @rtus-Recherche.

Anmerkung: Die Berechtigung für die Nutzung der @rtus-Recherche wird wie bisher weiterhin über die Einrichtung eines Horizontalen Blockverbund in @rtus-Admin realisiert bleiben.

10 Umsetzung @rtus-Mobile

Dieses Fachkonzept hat keine Auswirkung auf @rtus-Mobile.

Anmerkung: Die Berechtigung für die Nutzung der @rtus-Mobile wird weiterhin über @rtus-Admin vergeben. Dies eist auch nicht anwenderbezogen, sondern es kann global freigegeben werden oder auf für die Nutzung eine ausgewählte Dienststelle. Weiterhin muss der Anwender selbst auch Mitglied auf der Dienststelle sein. Dieses wird dann durch die Anforderung in diesem Konzept nun über die Provisionierung durch das F-IAM zukünftig umgesetzt werden.

11 Umsetzung Kataloge

Dieses Fachkonzept hat keine Auswirkung auf die Kataloge.

12 Umsetzung Formulare

Dieses Fachkonzept hat keine Auswirkung auf die Formulare.

13 Hinweise zur Abnahme

Offen

14 Glossar Thema IAM

Begriff	Erläuterung
IAM	Identity and Access Management (IAM) ist ein Rahmenwerk aus Richtlinien, Prozessen und Technologien, das sicherstellt, dass die richtigen Personen innerhalb einer Organisation Zugriff auf die richtigen Ressourcen zur richtigen Zeit und aus den richtigen Gründen haben. Es umfasst die Verwaltung von Benutzeridentitäten und deren Authentifizierung sowie die Kontrolle des Zugriffs auf Netzwerke, Systeme und Daten. Das IAM kann durch diverse Softwareprodukte umgesetzt werden, wie z.B. Microsoft Azure Active Directory oder Keycloak als Open Source Lösung. P20 setzt ein Oracle Produkt ein.
SCIM	SCIMv2 (System for Cross-Domain Identity Management Version 2) ist ein offener Standard, der die Verwaltung von Benutzeridentitäten in Cloud-basierten Anwendungen und Diensten vereinfacht. SCIMv2 definiert ein einheitliches API-Protokoll sowie ein Schema zur Automatisierung des Austauschs von Identitätsinformationen zwischen unterschiedlichen Domains und Systemen. SCIMv2 ist von der PG IAM als Schnittstellenprotokoll zwischen Teilnehmer-BV, F-IAM und den P20-Fachverfahren ausgewählt worden. Das Protokoll wird an den Bedürfnissen von F-IAM angepasst und deshalb separat mit einer eigenen Spezifikation versehen.
F-IAM	Als Förderatives-IAM wird das zentrale IAM von P20 bezeichnet, welches alle Benutzer und Rechte für P20 Anwendungen vorhält und auch die Authentifizierung der Nutzer durchführen kann.
BV	Als Benutzerverwaltung (auch teilweise als Teilnehmer-IAM bezeichnet), ist die jeweilige Software vom Teilnehmer, in dem die Benutzer, Dienststellenzuordnung und Rechte der Anwender zentral vom Teilnehmer gepflegt werden. Diese Daten werden mittels SCIMv2 an das F-IAM übermittelt, welches wiederum die Provisionierung der Fachanwendungen vornimmt.
JMX-Service	Java JMX (Java Management Extensions) ist ein Framework zur Verwaltung und Überwachung von Java-Anwendungen. Der JMX-Service ermöglicht die Interaktion mit MBeans (Managed Beans), die zur Überwachung und Steuerung von Ressourcen wie Anwendungen, Geräten und Diensten, verwendet werden. Beim Artus-Server (Wildfly) ermöglicht eine JMX-Web-Konsole (Hawtio) den Zugriff auf diese JMX-Service und ermöglicht somit eine Dienststeuerung und Konfiguration durch das fachliche bzw. technische Verfahrensmanagement.
REST	Ein REST Service ist eine webbasierte Schnittstelle, die auf dem REST-Architekturstil basiert. REST (Representational State Transfer) nutzt HTTP-Methoden wie GET, POST, PUT und DELETE, um Ressourcen über URLs zu adressieren und zu manipulieren.
REST-Operation	Operationen sind HTTP-Methoden wie GET, POST, PUT und DELETE, die an einem REST-Endpunkt aufgerufen werden können und dort mit der Semantik der HTTP-Methoden verarbeitet werden sollen.
REST-Endpunkt	Ein REST-Endpunkt ist eine spezifische URL (Uniform Resource Locator) innerhalb eines RESTful Web Service, über die bestimmte Ressourcen oder Funktionen zugänglich sind. Jeder Endpunkt repräsentiert eine Adresse, an die HTTP-Anfragen (wie GET, POST, PUT, DELETE) gesendet werden können, um mit der Ressource zu interagieren.

15 Anlagen

Kürzel	Titel	Quelle	Version Datum
A1	Anbindung von Anwendungen an das F-IAM	P20 F-IAM Confluence	V1.5 15.08.23
A1.1	P20 AW-SCIMv2 Spezifikation	AW-SCIMv2 IAM P20	Letzter Zugriff 10.06.2024
A2	SCIMv2 Spezifikation	SCIM: System for Cross-domain Identity Management	Letzter Zugriff 10.06.2024
A3	Rollen- und Rechtekonzept @rtus	200421 Entwurf - FK Rechte und Rollen BPOL.docx (Link)	V1.4 2020
A4	Datenberechtigungskonzept @rtus	FK_Koop_artus_Berechtigungen.doc (Link) FK_Koop_artus_Anpassung_Berechtigungskonzept.doc (Link) FK_artus_Vorgänge_verbergen.docx (Link)	V3.07 2009 V1.1 2009 V1.0 2018
A5	20231206_IAM_Zeitplanung_und_Arbeitspakete.pptx	Workshop 06.12.23 KTT/BKA/PG IAM/RP/SL/dataport	06.12.2023
A6	Loggingrichtlinie Artus	Logging Richtlinie @rtus v1.0.pdf	31.03.2022
A7	Änderungsantrag CR-IAM Stufe 2	2023-11-29_iVBS-Antragsänderung_artus_IAM_v1.1_PMO-SH.docx	08.12.2023

16 Sammlung offene Punkte

16.1 Todo: Dataport: Verfolgung Aufnahme „Dienstgrad“ in SCIMv2 IAM

Der Dienstgrad kann derzeit bei der BPOL und ST über den Webservice gepflegt werden. Daher sollte das auch mit IAM und SCIM gehen (siehe 2.1). Offen ist noch ob über Katalog oder String. Dataport muss das Thema bei PG IAM platzieren und weiterverfolgen.

Status:

22.03.2024: Mail an PG IAM und bilateraler Austausch vorab mit Patrik Stellmann.

16.2 Todo: Dataport: Platzierung Thema „Rechte nur auf spezifischen Dienststellen gültig“

Folgendes Thema soll über PG IAM besprochen und zu späteren Zeitpunkten aufgelöst werden:

Es gibt derzeit Rechte wie Kriminalaktenhaltung oder Sicherheitsüberprüfung, die nur auf spezifischen Dienststellen vergeben werden können. Ist die Dienststelle keine Kriminalaktenhaltung, können eben dort Anwendern auch keine Rechte für eine Kriminalaktenhaltung vergeben werden.

Momentan werden wir das als Fehlersituation behandeln (müssen), der dann wiederum in BV des Teilnehmers gelöst werden muss. Das F-IAM wird aber zwischenzeitlich diese Differenz auch feststellen können, da die BV das Recht vergeben und @rtus entsprechend die Vergabe abgelehnt hat und es bei Abfrage auch nicht gesetzt ist.

Perspektivisch sollte man bei dem neu zu schaffenden Repository mit den Anwendungsrechten die Anforderungen aufnehmen, dass Rechte auf eine Menge spezifischen Dienststellen vergeben werden dürfen.

Status:

05.04.2024 Per Mail an PG IAM gemeldet.

16.3 Todo: Dataport: Platzierung Thema „Recht nur einmal pro Dienststelle zu vergeben“

Folgendes Thema soll über PG IAM besprochen und zu späteren Zeitpunkten aufgelöst werden:

In VBS gibt es die Sonderrolle Dienststellenleitung. Diese kann nur einmal pro Dienststelle vergeben werden. Hat also ein Anwender bereits dieses Recht und wird einem zweiten dieses Recht vergeben, können wir derzeit nur dem ersten das Recht entziehen. Was wiederum dann eine Differenz zum IAM und zur BV darstellt. Das ein Recht vielleicht nur einmal zu vergeben ist, ist vielleicht gar nicht so außergewöhnlich und müsste dann auf BV Seite bereits geprüft und verhindert werden. Aber auch das muss die BV ja erst einmal wissen.

Daher stellt sich wie bei 1.) ggf. die Anforderung bei dem Repository mit Anwendungsrechten berücksichtigen. Dort könnten Rechte vielleicht gekennzeichnet werden, ob diese nur einmal global oder pro Dienststellen vergeben werden dürfen. So können die BV das bereits auf Teilnehmerseite sicherstellen.

Status:

05.04.2024 Per Mail an PG IAM gemeldet.

16.4 Todo: Dataport: Spezifikation und Beschreibung für GET bei OE-Permission fehlt

Die Spezifikation ist in den Abschnitten für GET-Abfragen Spezifikation unter „1.1.2 Berechtigungsdefinitionen Abfragen“ und „1.1.3 Berechtigungszuweisungen Abfragen“ auf Endpunkt „OE-Permission“ nicht beschrieben. Diese muss von der PG IAM noch vervollständigt werden. Betroffen sind (?) auch die Abschnitte 4.16, 4.17 und 6.2.

Status:

19.06.2024 Mail an PG IAM:

Hallo Julia,

einen zweiten Punkt aus dem heutigen Workshop mit der FAG IAM Provisionierung möchte ich ebenfalls separat bei euch einsteuern und um eine Rückmeldung bitten.

Die Spezifikation SCIMv2 IAM ist in den Abschnitten für GET-Abfragen Spezifikation unter „1.1.2 Berechtigungsdefinitionen Abfragen“ und „1.1.3 Berechtigungszuweisungen Abfragen“ auf Endpunkt „OE-Permission“ nicht beschrieben. Diese muss noch aus unserer Sicht von der PG IAM noch vervollständigt werden.

Link: [https://confluence.bka.extrapol.de/pages/viewpage.action?pageId=244553450#AWSCIMv2ENTWURF-Abrufen\(WellKnown\)](https://confluence.bka.extrapol.de/pages/viewpage.action?pageId=244553450#AWSCIMv2ENTWURF-Abrufen(WellKnown))

/OU-Permissions	GET	Abfrage von Rechten mit OE-Bezug, die für die AW zugewiesen werden können Liefert auch die Liste der Zuweisungen, sofern es nicht über Query-Parameter unterbunden wird.	für AW mit Berechtigungen mit OE-Bezug
/OU-Permissions/{OU-Permission-ID}	GET	Liefert auch die Liste der Zuweisungen, sofern es nicht über Query-Parameter unterbunden wird.	
	PATCH	Berechtigungszuweisung mit OE-Bezug hinzufügen/entfernen	

Könnt ihr sagen, wann ihr hier die Vervollständigung vornehmen könnt?

16.5 Todo: Dataport: Hinterfragen der asynchronen Verarbeitung schreibender Nachrichten

Rückmeldung am 17:06:2024 von Martin Nicolay, SL zum Abschnitt Webservice SCIMv2 zu 5.1:

„Folgenden Punkt sehe ich für die Arbeitsabläufe der Benutzeradministration als sperrig handhab-bar:

Asynchrone Verarbeitung von Ändernden Operationen.

Im Konzept unter 5.1 (Seite 53, Tabellezeile SCIMv2-REST-Service) wird beschrieben, dass ändernde IAM-Operationen durch @rtus asynchron umgesetzt werden. Es wird zur synchronen Quittierung der Operation eine Validierung durchgeführt, die jedoch bei Vorliegen von mehreren, voneinander abhängigen und noch nicht umgesetzten Operationen, fehlerhaft sein kann. Dadurch kann es vorkommen, dass Operationen, die die Validierung ohne Fehlermeldung passieren, bei Umsetzung der Operation einen Fehler erzeugen. Umgekehrt wäre auch möglich.

Beispiel: Operation 1: Deaktivierung der Dienststelle X; Operation 2: Zuordnung eines Benutzers für die Dienststelle X

Operation 1 validiert ohne Fehler und wird zur späteren Bearbeitung gespeichert. Operation 2 validiert ohne und wird gespeichert für spätere Bearbeitung → keine Fehlermeldung in F-IAM

Folgen: Operation 1 wird umgesetzt ohne Fehler. Operation 2 kann nicht umgesetzt werden, da Dienststelle X zuvor deaktiviert wurde. → Protokollierung des Fehlers in @rtus

Problem: Die Personen, die für die Berechtigungsverwaltung zuständig sind, gehen von korrekter Umsetzung da, das im F-IAM kein Fehler ersichtlich ist. Der Fehler läuft zeitversetzt bei Personen auf, die für die Verfahrensbetreuung @rtus zuständig sind. Die fehlerverursachende Stelle erhält erst zeitversetzt und über Umwege Kenntnis von dem Fehlerfall. Wesentlich einfacher wäre hier eine synchrone Bearbeitung durch @rtus und somit eine unmittelbare Fehlermeldung an die Stelle, die die fehlerverursachende Aktion ausgelöst hat."

Dataport erläuterte im Termin 19.06.2024 zum Abschnitt 5.1 Webservice SCIMv2 die Begründung, warum die schreibenden Operationen grundsätzlich asynchron sein müssen:

1. Einige Operationen können etwas länger dauern und das F-IAM darf nicht mit längeren Antworten blockiert werden. Beispiel ist hier das Umhängen und Statusänderungen von Vorgängen.
2. Noch wichtiger ist, dass die Schnittstelle zwischen BV und IAM bereits asynchron ist und daher selbst eine synchrone Verarbeitung auf der iVBS-Seite keine Vorteile bietet. Beim F-IAM ist der Hintergrund, dass hier mit einer Änderung durch eine BV zahlreiche Fachverfahren mit Nachrichten versehen werden müssen (Beispiel: Neuer Nutzer mit Recht auf zahlreiche Fachverfahren, Löschen von Anwendern). Da die Menge der Fachverfahren nicht sichergestellt werden kann, muss die Verarbeitung zwischen BV und F-IAM asynchron sein.

Dataport soll hier noch einmal den Sachverhalt mit einer Bitte um Stellungnahme zu den Bedenken an die PG IAM verfassen und die Rückmeldung in die FAG zurückführen.

Status:

19.06. Mail an die PG IAM versendet

Hallo Julia,

wir bearbeiten derzeit gerade in den finalen Zügen das Umsetzungskonzept für die Anbindung der F-IAM Provisionierung. Die aktuellste Version 0.8 stelle ich mit der Mail auch zur Verfügung.

Die Teilnehmer der FAG zeigten sich im heutigen Workshop aufgrund der asynchronen Verarbeitung der Nachrichten zwischen BV und F-IAM bzw. F-IAM und Fachverfahren (weiterhin) besorgt. Ich verweise hier auf den Abschnitt „16.5 Todo: Dataport: Hinterfragen der asynchronen Verarbeitung schreibender Nachrichten“. Ich habe dort auch noch mal die zwei Gründe für eine asynchrone Verarbeitung der schreibenden Nachrichten aufgeführt, so wie wir sie zumindest aus der Zusammenarbeit mit der PG IAM herleiten und begründen können.

Letztendlich ist die Sorge der Fachlichkeit, dass durch die asynchrone Verarbeitung Abweichungen produziert werden, die in einem manuellen Prozess aufgelöst werden müssen. Zwar sehen eure und unsere Anwendungsfälle im Fehlerfall eine Nachvollziehbarkeit und eine Benachrichtigung der betroffenen Stellen vor, aber die vorhandene Inkonsistenz muss trotzdem manuell aufgelöst werden. Je nach Menge solcher Problemfälle, kann das natürlich Aufwand für diese Stellen bedeuten. Keiner kann sagen, wie häufig solche Problemfälle auftauchen werden. Im Konzept sind bei 6 Fehlerszenarien, wo wir bereits beim Eingang der Nachricht ggf. eine Fehlermeldung an das F-IAM zurückgeben (Schlagwort im Dokument „Fehlerszenario“).

Die FAG wünscht sich eine Stellungnahme oder auch Rückmeldung, die zunächst noch einmal begründet, warum dieser Sachverhalt unvermeidbar ist bzw. ob es doch eine Alternative einer synchronen Verarbeitungskette zwischen BV, F-IAM und Fachverfahren geben kann. Vielleicht gibt es auch Erfahrungen im Austausch mit anderen Teilnehmern oder ggf. bei bestehenden Verfahren.

Viele Grüße

Jan