FAG IAM Provisionierung @rtus-Kooperation, Jan Rüth

Zusammenfassung

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

konzept

**Nutzer und   
Berechtigungsverwaltung über P20 IAM**

|  |  |  |
| --- | --- | --- |
| Stand Datum |  | 19.04.2024 |
| Version |  | 0.5 |
| Konzeptverantwortlich |  |  |
| Status |  | In Bearbeitung |
| Jira-Ticketnummer |  |  |
| Beteiligte Akteure   |  |  |  | | --- | --- | --- | | Rolle | Name | Organisation | | Weitere Konzeption | Jan Rüth | Dataport | | Verantwortlich Formulare | - | - | | Verantwortlich Kataloge | - | - | | Verantwortlich Dataport | Jan Rüth  Matthias Oppermann | Dataport | | Verantwortlich Fachlichkeit @rtus | Maren Tietgen (SH) | Dataport | | Fachlichkeit extern | Alberto Blinckmann (HH)  Denis Völkers (HH)  Torben Busse (HB)  Carsten Bauck (NI)  Jens Häupl (AN)  Thomas Reiser (AN)  Matthias Voltmer (SL)  Christian Grim (SL)  Paul Klemm (RP)  Christian Schwan (RP)  Moritz Rubel (RP)  Thomas Müller (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 Organisationeinheiten / 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 neuen 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 |
|  |  |  |  |  |
|  |  |  |  |  |

Inhaltsverzeichnis

[1 Problembeschreibung 6](#_Toc164419920)

[*1.1* *Vorwort* 6](#_Toc164419921)

[*1.2* *Einleitung und Problemstellung* 6](#_Toc164419922)

[2 Abhängigkeiten / Rahmenbedingungen 8](#_Toc164419923)

[*2.1* *Übersicht Objekt: Anwender* 8](#_Toc164419924)

[*2.2* *Übersicht Objekt: Dienststelle* 11](#_Toc164419925)

[*2.3* *Übersicht Objekt: Rollen- und Funktionsberechtigung* 14](#_Toc164419926)

[*2.4* *Planungsübersicht und stufiges Vorgehen* 16](#_Toc164419927)

[*2.5* *Übersicht „P20 F-IAM“ Benutzerverwaltung* 16](#_Toc164419928)

[*2.6* *Übersicht über SCIMv2 (Schnittstellen F-IAM)* 18](#_Toc164419929)

[3 Lösungsansatz 20](#_Toc164419930)

[*3.1* *[Stufe 2b] Verwaltung von Organisationeinheiten / Dienststellen* 20](#_Toc164419931)

[*3.2* *[Stufe 2a] Verwaltung von Anwendern* 21](#_Toc164419932)

[*3.3* *[Stufe 2b] Verwaltung Dienststellenzugehörigkeiten* 25](#_Toc164419933)

[*3.4* *[Stufe 2b] Verwaltung von Berechtigungen* 25](#_Toc164419934)

[*3.5* *[Stufe 2a] Protokollierung und Nachvollziehbarkeit* 30](#_Toc164419935)

[*3.6* *[Stufe 2a] Vorgehen bei der Transition von interner auf externer Provisionierung für Bestandskunden* 31](#_Toc164419936)

[*3.7* *[Stufe 2b] Vorgehen bei der Transition von bestehender externer Provisionierung mittels Webservice „Benutzerverwaltung“ auf F-IAM für Bestandskunden* 31](#_Toc164419937)

[4 Anforderung 32](#_Toc164419938)

[*4.1* *[ANF-001][Stufe 2a] Anlage neuer Dienststellen* 32](#_Toc164419939)

[*4.2* *[ANF-002] [Stufe 2b] Pflege und Aktualisierung der Dienststellenstammdaten* 32](#_Toc164419940)

[*4.3* *[ANF-003] [Stufe 2b] Deaktivierung (Löschung) von Dienststellen* 33](#_Toc164419941)

[*4.4* *[ANF-010] [Stufe 2a] Anlage neuer Anwender* 33](#_Toc164419942)

[*4.5* *[ANF-011] [Stufe 2a] Deaktivierung (logische Löschung) von Anwendern* 34](#_Toc164419943)

[*4.6* *[ANF-012] [Stufe 2a] Pflege und Aktualisierung der Anwenderstammdaten* 37](#_Toc164419944)

[*4.7* *[ANF-020] [Stufe 2b] Zuordnung von Anwender zu Dienststelle* 38](#_Toc164419945)

[*4.8* *[ANF-021] [Stufe 2b] Löschung einer Zuordnung von Anwender zu Dienststelle* 41](#_Toc164419946)

[*4.9* *[ANF-022] [Stufe 2b] Setzen von Berechtigungen auf Dienststellenebene* 41](#_Toc164419947)

[*4.10* *[ANF-023] [Stufe 2b] Löschen von Berechtigungen auf Dienststellenebene* 42](#_Toc164419948)

[*4.11* *[ANF-024] [Stufe 2a] Sperrung von Anwendern auf Dienststellen* 42](#_Toc164419949)

[*4.12* *[ANF-025] [Stufe 2a] Globale Sperrung von Anwender in @rtus* 43](#_Toc164419950)

[*4.13* *[ANF-030] [Stufe 2a] Deaktivierung der internen Benutzerverwaltung für externe Provisionierung* 43](#_Toc164419951)

[*4.14* *[ANF-030] [Stufe 2b] Deaktivierung der internen Benutzerverwaltung für externe Provisionierung* 44](#_Toc164419952)

[*4.15* *[ANF-031] [Stufe 2a] Protokollierung und Nachvollziehbarkeit* 46](#_Toc164419953)

[5 Umsetzung VBS 48](#_Toc164419954)

[6 Umsetzung Datenmodell und Schnittstelle 48](#_Toc164419955)

[7 Umsetzung @rtus-Admin 48](#_Toc164419956)

[8 Umsetzung @rtus-Recherche 48](#_Toc164419957)

[9 Umsetzung @rtus-Mobile 48](#_Toc164419958)

[10 Umsetzung Kataloge 48](#_Toc164419959)

[11 Umsetzung Formulare 48](#_Toc164419960)

[12 Hinweise zur Abnahme 48](#_Toc164419961)

[13 Anlagen 49](#_Toc164419962)

[14 Sammlung offene Punkte 49](#_Toc164419963)

[*14.1* *Todo: Dataport: Verfolgung Aufnahme „Dienstgrad“ in SCIMv2 IAM* 49](#_Toc164419964)

[*14.2* *Todo: Dataport: Platzierung Thema „Rechte nur auf spezifischen Dienststellen gültig“* 50](#_Toc164419965)

[*14.3* *Todo: Dataport: Platzierung Thema „Recht nur einmal pro Dienststelle zu vergeben“* 50](#_Toc164419966)

# Problembeschreibung

## Vorwort

Dieses Dokument ist ein Grobkonzept, welches die Anforderungen und mögliche Lösungsansätze darstellt. In einigen Abschnitten werden auch mehrere alternative Lösungsvorschläge gemacht, welche dann in weiteren Austausch bewertet, ausgewählt und ggf. weiter ausgearbeitet werden müssen.

Dieses Dokument ist somit noch kein fertiges Fachkonzept, welches sich bereits zur Umsetzung eignet. Dieses kann sich aber daraus entwickeln.

## 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 werden und deshalb zeitnah konzeptioniert werden.

Im Zielbild von P20 sollen Fachanwendung 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**
   1. [ANF-001] Anlage neuer Dienststellen
   2. [ANF-002] Pflege und Aktualisierung der Dienststellenstammdaten
   3. [ANF-003] Deaktivierung (Stilllegung) von Dienststellen
2. **Anwenderverwaltung** 
   1. [ANF-010] Anlage neuer Anwender
   2. [ANF-011] Deaktivierung (logische Löschung) von Anwendern
   3. [ANF-012] Pflege und Aktualisierung der Anwenderstammdaten
3. **Berechtigungsverwaltung**
   1. [ANF-020] Zuordnung von Anwender zu Dienststelle
   2. [ANF-021] Löschung einer Zuordnung von Anwender zu Dienststelle
   3. [ANF-022] Setzen von Berechtigungen auf Dienststellenebene
   4. [ANF-023] Löschen von Berechtigungen auf Dienststellenebene
   5. [ANF-024] Sperrung von Anwendern auf Dienststellen
   6. [ANF-025] Globale Sperrung von Anwender in @rtus
4. **Sonstige Anforderungen**
   1. [ANF-030] Deaktivierung der internen Benutzerverwaltung für externe Provisionierung
   2. [ANF-031] Protokollierung und Nachvollziehbarkeit
   3. [ANF-032] Lesende Zugriffe für F-IAM

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 entfernet werden, wenn dieser noch offene Vorgänge auf der Dienststelle hat. Auch die bisherige Webservice-Schnittstelle zur internen Benutzerverwaltung (BPOL) unterliegt dieser Logik. Der Vorgang einer externen Provisionierung einer IT-Anwendung durch IAM verwenden hier eine andere Vorgehensweise: Sie teilen der Fachanwendung jeweils mit, wie der aktuelle Zustand der Verwaltung aussehen muss (ggf. auch durch Deltainformationen) und erwarten 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 auf asynchron und 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.

# 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.

## 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. Dieses erleichtert den Parallelbetrieb von interner und externer Benutzerverwaltung.

Für eine 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.

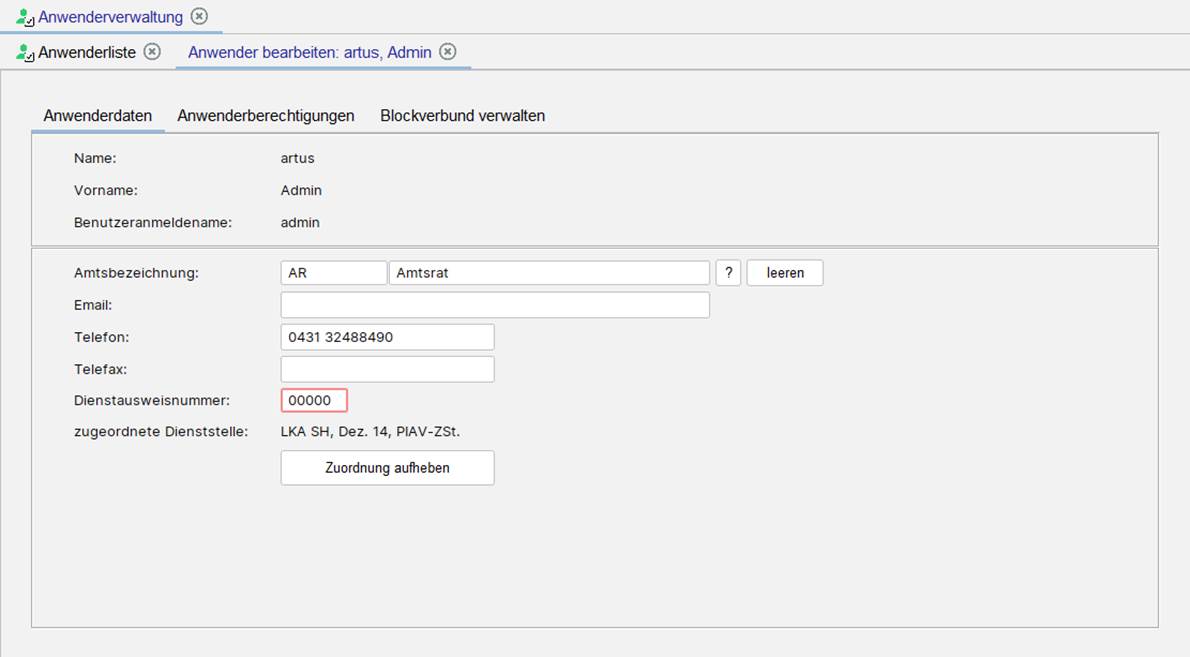


Abbildung : @rtus-Client: Anwenderverwaltung Maske Anwenderdaten

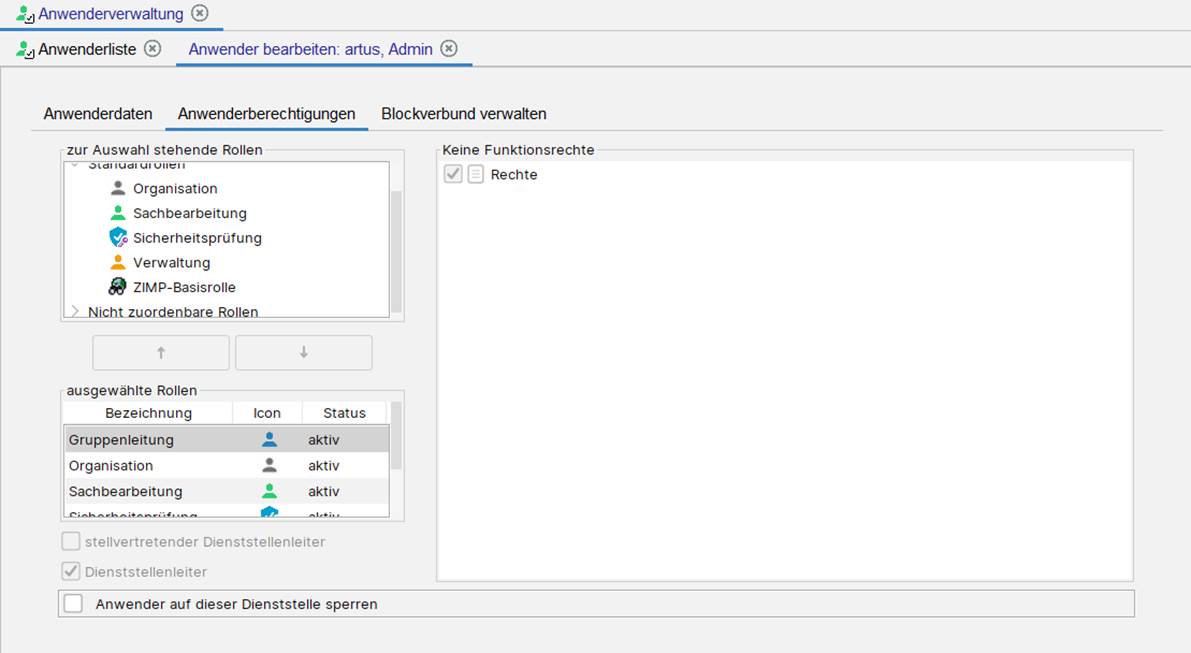


Abbildung : @rtus-Client: Anwenderverwaltung Maske Anwenderberechtigungen

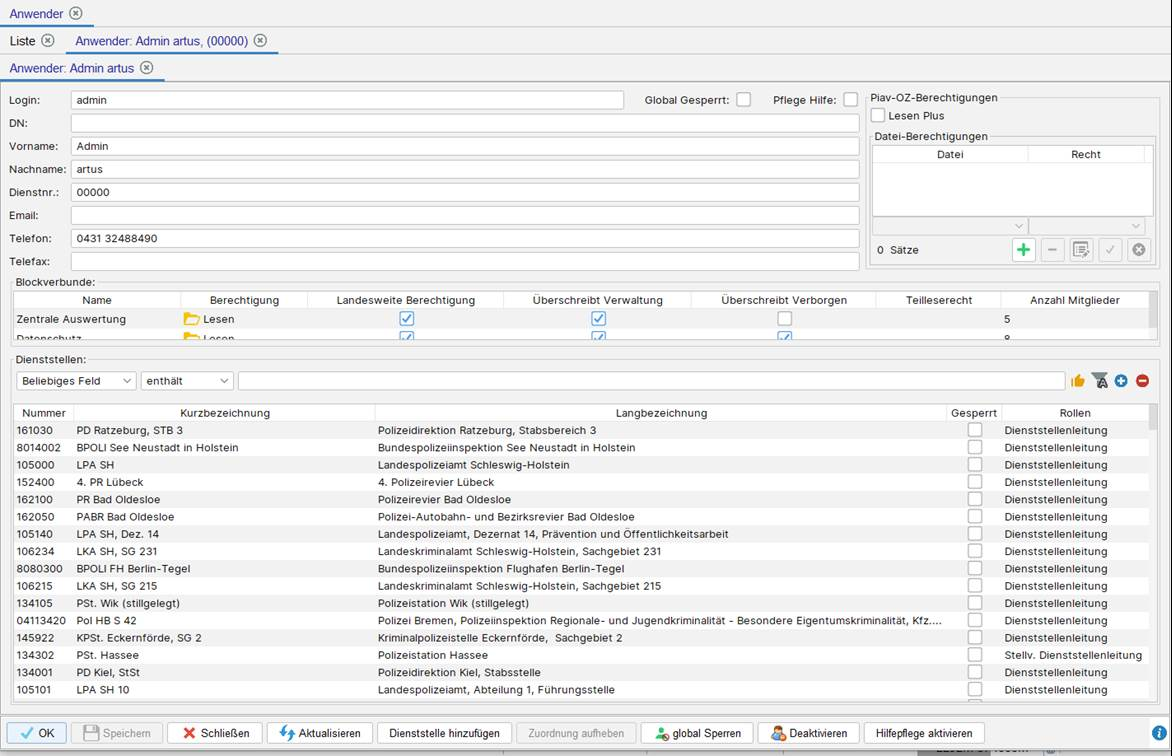


Abbildung : @rtus-Admin Maske Anwender Bearbeiten

|  |  |  |
| --- | --- | --- |
| **Attribut** | **Typ** | **Beschreibung** |
| Login/Benutzeranmeldename | 1..1, String 200 | Login Zeichenkette aus dem AD oder F-IAM. Entsprecht im AD den smAccountName. Muss eindeutig sein. |
| DN | 0..1, String 200 | DN-Zeichenkette, vollqaulifiziert 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 Bestandvorgänge 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? |  |

## 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.

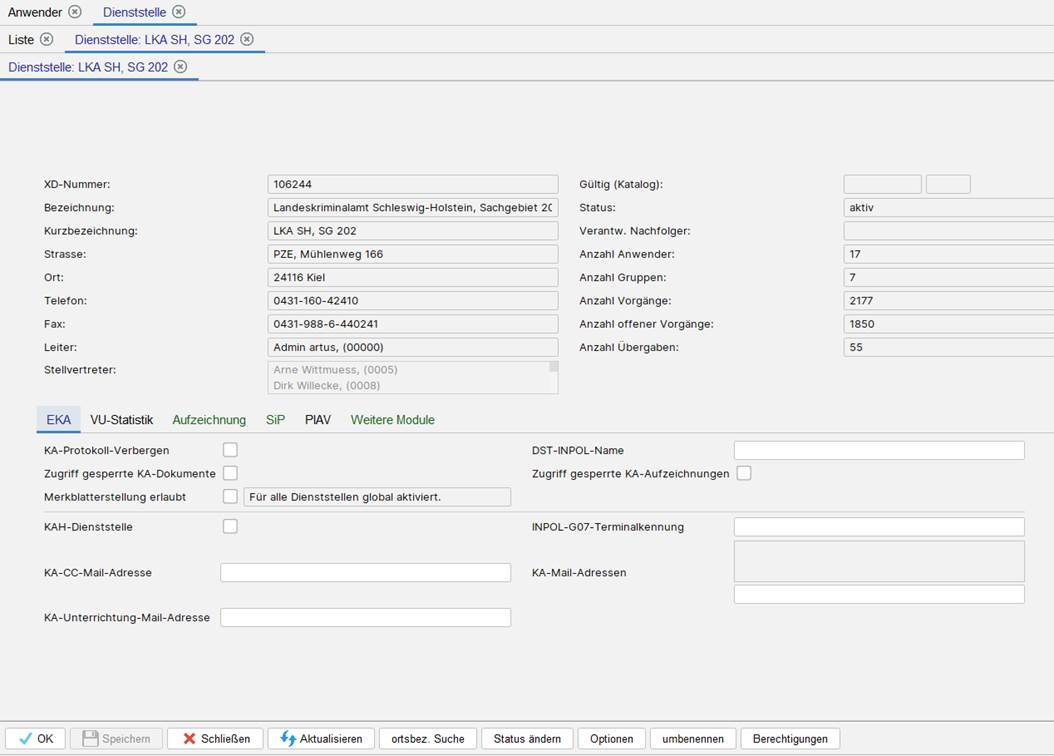


Abbildung : @rtus-Admin Maske Dienststellenverwaltung

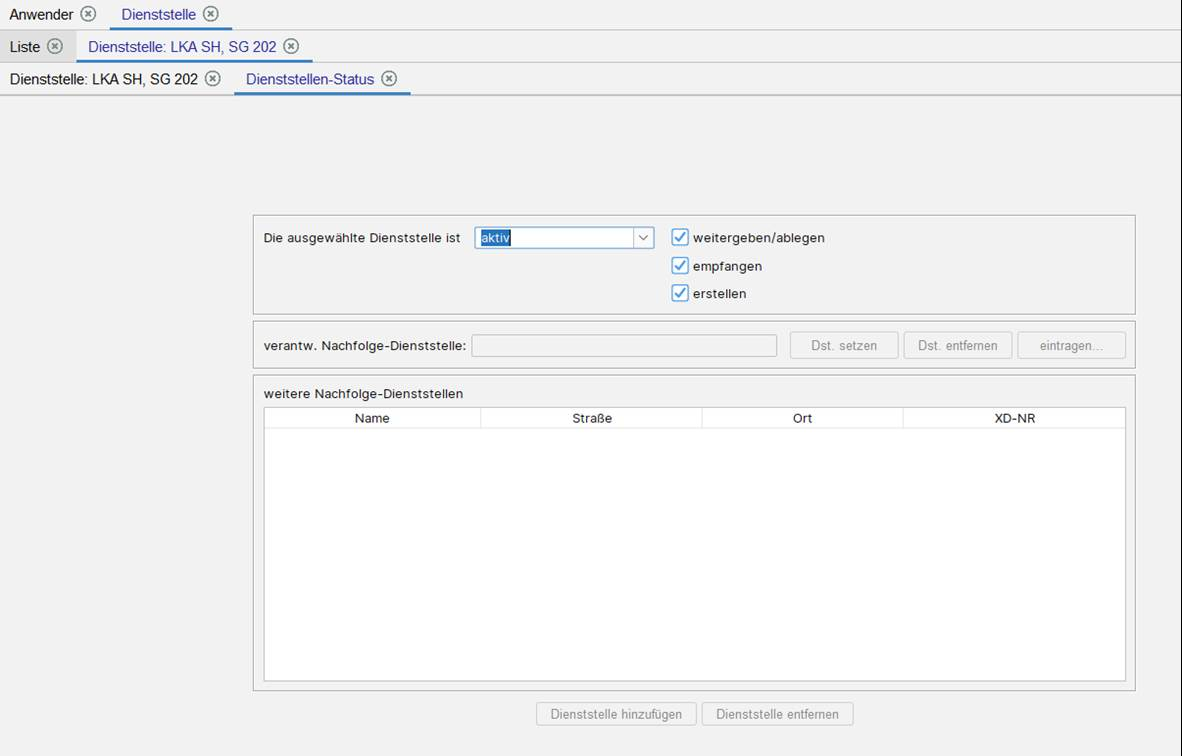


Abbildung : @rtus-Admin Maske Dienststellenverwaltung Dienststellen-Status

|  |  |  |
| --- | --- | --- |
| **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  Passiv  Reorganisation | Definiert den Status der Dienststelle.  Aktiv:  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 wir 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.

## 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 zusammengefasst. 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, Verborgen) 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 horizontale 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 eine oder mehrere 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 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:

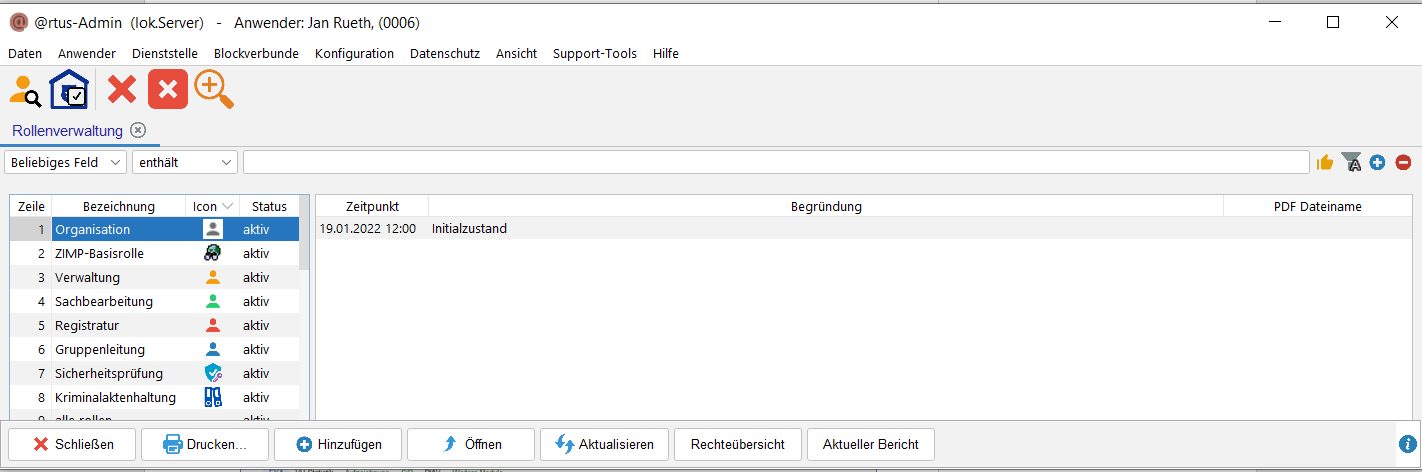


Abbildung : Rollenverwaltung in @rtus-Admin

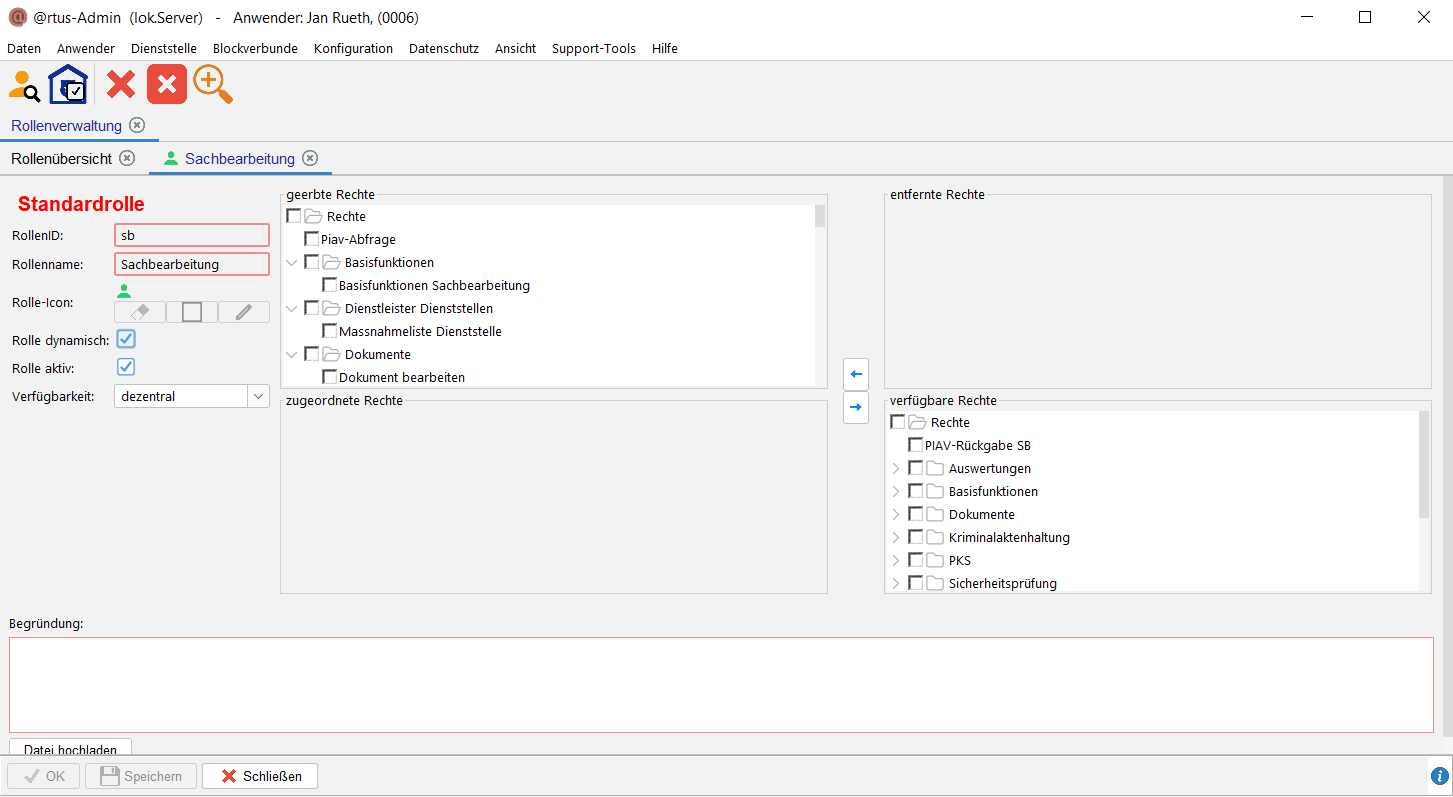


Abbildung : Rollenansicht und -bearbeitung in @rtus-Admin

## Planungsübersicht und stufiges Vorgehen

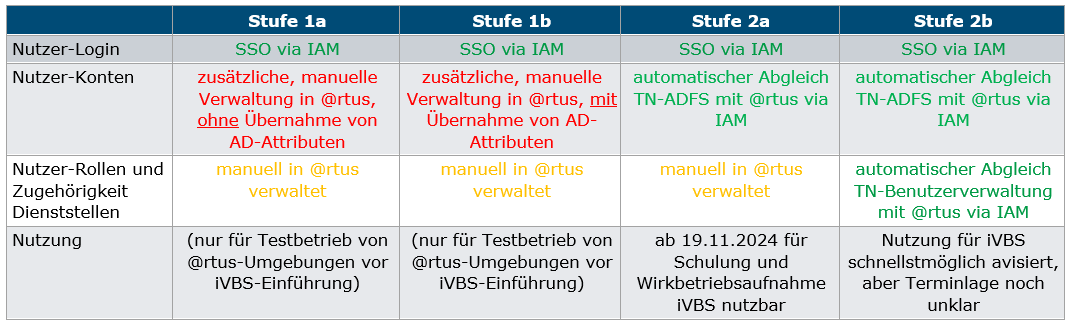


Abbildung : Ausbaustufen Anbindung Artus (Quelle Workshop 06.12.23 KTT/BKA/RP/SL/Dataport)

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 beim Teilnehmer 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.

## 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 der @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 könnend 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.

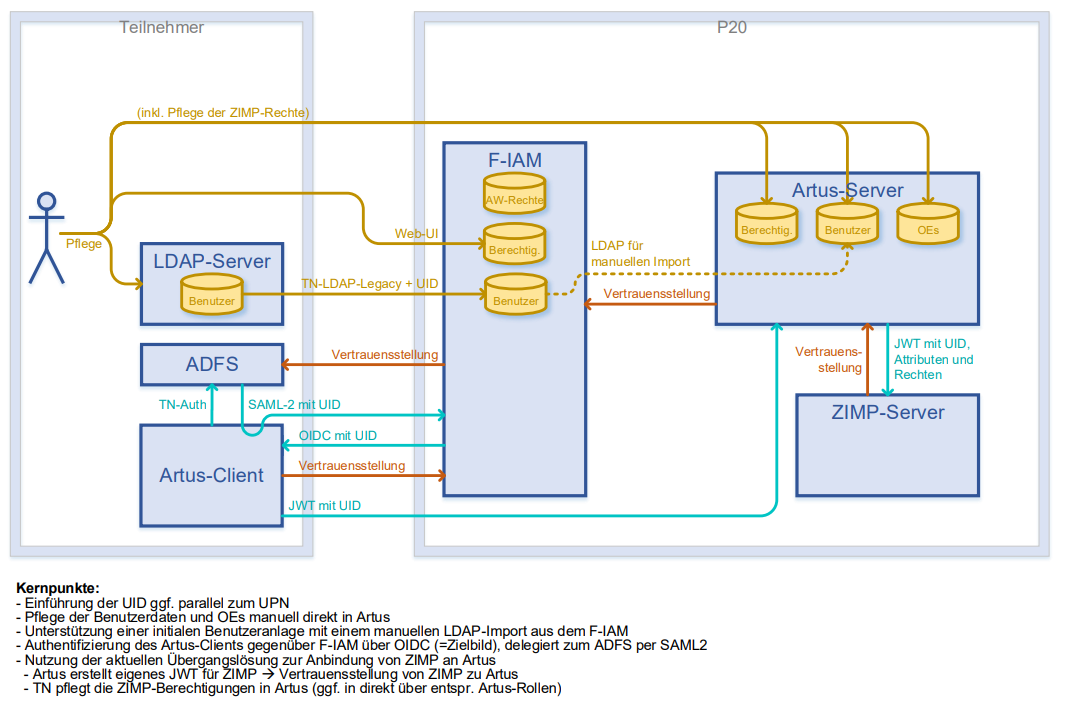


Abbildung : Schematische Darstellung interne Benutzerverwaltung ohne externe Provisionierung

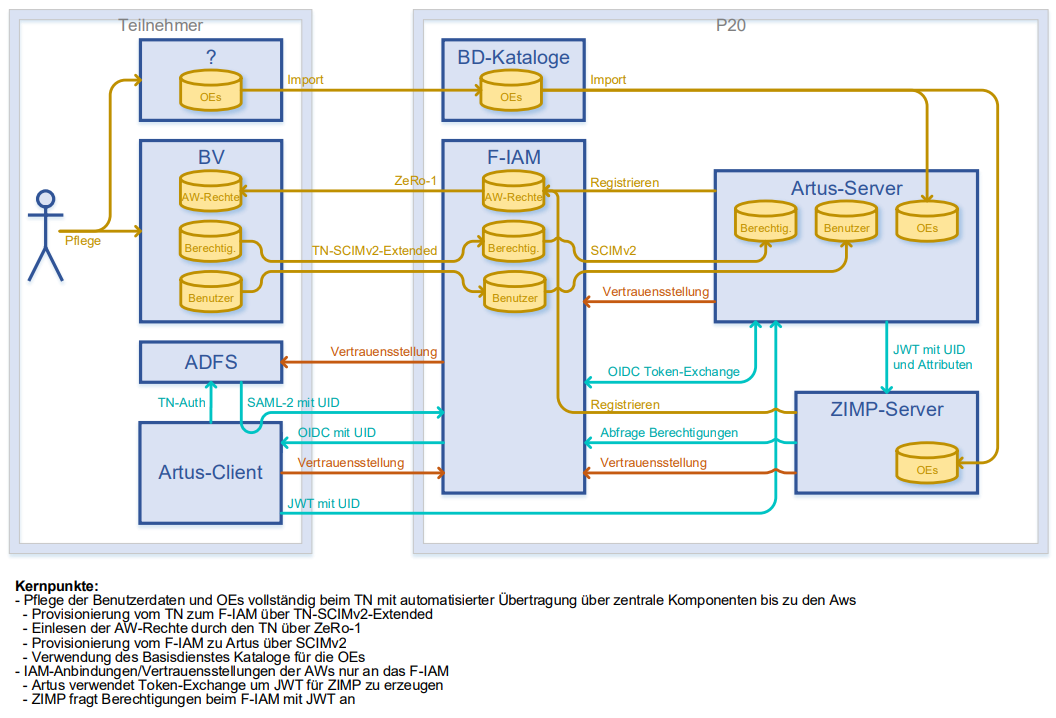


Abbildung : Provisionierung über F-IAM von P20

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

## 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“, und Version 2 (SCIM 2) 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 (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.

# 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.

## [Stufe 2b] Verwaltung von Organisationeinheiten / 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, aber wie die Zuordnung zwischen IAM und Katalog sichergestellt wird und wie diese Prozesse ablaufen, ist derzeit vollkommen offen[[1]](#footnote-2).

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 vorhanden 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 Dienststellennummer (Hierarchienummer, XD-Nummer) verwendet werden, da diese Erfahrungsgemäß eben nicht für immer konstant und eindeutig bleibt und damit sich 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 techn. 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 Schnitt 4 verwenden.

## [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/Benutzeranmeldename | [1..1] userName | - |  |
| DN | - | - | Offen. Vorschlag entfall für Schnittstelle |
| 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@somwhere.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

## [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.

## [Stufe 2b] Verwaltung von Berechtigungen

@rtus unterscheiden wir bereits im Abschnitt 2.3 beschrieben 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 |  |
| Zugeorndet (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 entzogen[[2]](#footnote-3). 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):

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"

  , "policeTitleKey"      : "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 : 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 : Beispiel PATCH-Operation mit Vergabe SB-Rolle auf einer Dienststelle

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

## [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 Ablaufristen 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.

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

Offen

## [Stufe 2b] Vorgehen bei der Transition von bestehender externer Provisionierung mittels Webservice „Benutzerverwaltung“ auf F-IAM für Bestandskunden

Offen

# 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.

## [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

## [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.

## [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 Dienststelle wird 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 dem aktive Vorgänge endbearbeitet werden oder auf die Nachfolgerdienststelle Dienststelle 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.

## [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 werden 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 erfolgt 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.)

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

Ereignis:

Ein aktiver Anwender 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 werden.
  + 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 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 interimsweise 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 interimsweise Zuordnung des Superuser @rtus-Admin zeitnah durch eine weitere Zuordnung eines neuen Dienststellenleiters erfolgt.

Szenario 4: „Anwender existiert 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. Dienststellenleitung 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 Stellvertreter 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 ist 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

## [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

## [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 Teilnehmer-Verzeichnisdienst angelegt werden 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 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 werden dann erst beim neuen Leiter gesetzt werden. Hierdurch wird eine Inkonsistent vermieden, da hier die vorhandenen Szenarien durchgeführt werden.

Fehlerszenario 8: „Dienststellenbezogene Rolle nicht auf Dienststelle erlaubt“

* Vorbedingungen
  + Anwender und Dienststelle existiert
  + 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

## [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

## [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.

## [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 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 Zuordnung zu entfernen Anwender 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

## [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.

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

Ereignis:

Der gesamte VBS-Zugang für einen Anwender soll gesperrt werden, ohne den 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 Attribut active=false
* @rtus setzt die Sperrung am Objekt Anwender
* Artus protokolliert die Änderungen aus den Szenarien in der Protokoll-Tabelle

Die Sperrung entfernen ist identisch mit dem obigen Ablauf.

TODO Dataport: Hinweis, dass Lösung über F-IAM ein Sperrung auf alle Verfahren auslöst

## [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 folgende Anwendungsfälle sich 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: „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

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

Für Stufe 2b gelten zunächst alle Änderungen, wie 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: „Über @rtus-Admin Anwender Bearbeiten“

* Folgende Felder bleiben aktiv änderbar
  + „Pflege Hilfe“
  + PIAV-OZ-Berechtigung
* (A) Alle anderen Felder werden deaktiviert und sind nur noch lesend einsehbar
* (B) Folgende Aktionen werden deaktiviert:
  + Dienststelle hinzufügen
  + Zuordnung aufheben
  + Global sperren
  + Deaktivieren
* Es wird ein Konfigurationswert eingeführt, der standardmäßig zur oben beschriebenen Deaktivierung von A und B führt. Wird der Konfigurationswert deaktiviert, werden die Felder und Aktionen von A und B 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

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

Log-Einträge in Logdatei und Protokolltabelle

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

Speicherung und Verwertung der Nachrichten vom F-IAM

Für 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 (Erfolgreich, 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.

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 „Nachrichtetabelle“ 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)

Stand der FAG Sichtung bis 19.04.2024

# Umsetzung VBS

Offen

# Umsetzung Datenmodell und Schnittstelle

Offen

# Umsetzung @rtus-Admin

Offen

# Umsetzung @rtus-Recherche

Offen

# Umsetzung @rtus-Mobile

Offen

# Umsetzung Kataloge

Offen

# Umsetzung Formulare

Offen

# Hinweise zur Abnahme

Offen

# Anlagen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kürzel | Titel | Quelle | Version/Datum | Anmerkung |
| A1 | Anbindung von Anwendungen an das F-IAM | [P20 F-IAM Confluence](https://confluence.bka.extrapol.de/pages/viewpage.action?pageId=28642117) | 1.5 vom 15.08.23 |  |
| A1.1 | P20 AW-SCIMv2 Spezifikation | [AW-SCIMv2 IAM P20](https://confluence.bka.extrapol.de/pages/viewpage.action?pageId=244553450) |  |  |
| A2 | SCIMv2 Spezifikation | [SCIM: System for Cross-domain Identity Management](https://scim.cloud/) | Letzter Zugriff 29.11.23 |  |
| A3 | Rollen- und Rechtekonzept @rtus |  |  | TODO |
| A4 | Datenberechtigungskonzept @rtus |  |  | TODO |
| A5 | 20231206\_IAM\_Zeitplanung\_und\_Arbeitspakete.pptx | Workshop 06.12.23 KTT/BKA/PG IAM/RP/SL/dataport | 06.12.23 |  |
| 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 |  |

# Sammlung offene Punkte

## 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.

## 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 BV das Recht vergeben hat 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.

## 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.

1. Einzelne Teilnehmer wie Hamburg haben für sich einen vorhandenen Prozess basierend auf ihrer Benutzerverwaltung. [↑](#footnote-ref-2)
2. Siehe: [[ART-32100] Neues Rollenkonzept - Dienststellenleiter nach Umstellung - Artus JIRA (extrapol.de)](http://jira-artus.sh.extrapol.de/browse/ART-32100?filter=-3) [↑](#footnote-ref-3)