

AW-SCIMv2-Extended - ENTWURF

P20 IAM - Identity and Access Management

Exported on 12/12/2024

Table of Contents

1	Einleitung.....	6
2	Endpunkte.....	7
3	Benutzerattribute	10
4	Berechtigungen	15
4.1	Groups: Berechtigungen ohne Dienststellenbezug.....	15
4.2	OU-Permissions: Berechtigungen mit Dienststellenbezug.....	17
4.3	Details zu AW-Rechten	21
5	Beispielnachrichten	22
5.1	Abfrage der AW-Rechte ohne Dst-Bezug.....	22
5.2	Abfrage der AW-Rechte mit Dst-Bezug.....	23
5.3	Anlegen eines Benutzers	24
5.4	Ändern eines Benutzers.....	26
5.5	Zuweisen eines Rechts ohne Dst-Bezug	28
5.6	Entziehen eines Rechts ohne Dst-Bezug	29
5.7	Zuweisen eines Rechts mit Dst-Bezug	29
5.8	Entziehen eines Rechts mit Dst-Bezug.....	30
5.9	Benutzerabfragen für Abgleich	31
5.9.1	Neue Benutzer.....	31
5.9.2	Geänderte Benutzer	31
5.9.3	Neue und geänderte Benutzer.....	31
5.9.4	Alle Benutzer, erste Anfrage.....	31
5.9.5	Alle Benutzer, zweite Anfrage (Pagination).....	31
5.9.6	Antwort	32
6	Fehlermeldungen	34
7	Authentifizierung.....	42


Status	VORGELEGT
Zielgruppe	AW-Entwickler
Dokumenteneigner	DI-PG-IAM
Gültig ab	
Version	0.4


Zusammenfassung	Das vorliegende Dokument beinhaltet Spezifikation der AW-SCIMv2-Extended Schnittstelle.
Einstufung der Geheimhaltung	KEINE



Inhaltsverzeichnis

Änderungsverzeichnis

Änderungsverzeichnis

Datum	Version	Beschreibung	Autor
 30 Oct 2024	0.1	Initiale Dokumentenerstellung	Dr. Patrik Stellmann (HH Extern)

 15 Nov 2024	0.2	<p>Korrektur nach Feedback von IGVP:</p> <ul style="list-style-type: none"> • Filter auf Users nach startIndex, nicht ID • PATCH-Operationen enthalten immer nur eine Attributänderung • Weitere Beispiele für Benutzeränderungen (Eintrag in Liste, Custom-Attribut, Löschen) • Korrektur: details einheitlich für Rechte-Details verwendet • Korrektur: id statt value im Schema für OuPermission, analog zu Group • Korrektur: displayName statt display im Schema von OuPermission, analog zu Group, Beispiele waren schon korrekt (in Referenz-Listen wird bereits in den Core-Schemata einheitlich display verwendet, so dass die Extension-Schemata hier analog aufgebaut sind.) • Korrektur: Referenzen einheitlich als "\$ref" (statt manchmal "ref") • "IGVP" als Anwendungsbezeichnung ersetzt durch "Anwendung" • noch offen: Fehlermeldung, wenn temporär an einem Benutzer keine Änderungen vorgenommen werden können (weil er gerade angemeldet ist) <p>Korrektur nach Feedback von Artus:</p> <ul style="list-style-type: none"> • excludeAttributes=members bei OuPermissions erfordert Schema als Prefix, da es kein Core-Attribut ist • Analog angepasst beim Abfragen von Groups mit Custom-Schema für details 	Dr. Patrik Stellmann (HH Extern)
---	-----	--	--

 22 Nov 2024	0.3	Anpassungen nach Feedback von IGVP: <ul style="list-style-type: none"> • Korrektur: Referenz als "\$ref" (statt "ref") beim Groups-Schema • Hinweis ergänzt, dass beim Abfragen von Groups je nach AW auch das Core-Schema genutzt werden kann 	Dr. Patrik Stellmann (HH Extern)
 06 Dec 2024	0.4	Anpassungen nach Feedback von IGCP und Artus: <ul style="list-style-type: none"> • Erklärung zum Schema-Prefix vor <code>members</code> bei <code>excludeAttributes</code> für /Groups und /OuPermissions • Korrektur des Schema-Prefix (urn: fehlte) 	Dr. Patrik Stellmann (HH Extern)

Prüfverzeichnis**Prüfverzeichnis**

Datum	Version	Beschreibung	Prüfer

1 Einleitung

Der Basisdienst IAM definiert gemäß [F-IAM-Gesamtkonzepte](#)¹ eine einheitliche SCIMv2-Schnittstelle für polizeiliche Fachanwendungen, die möglichst von sämtlichen Anwendungen mit einer IDM-Anbindung an das F-IAM genutzt werden soll. Dabei ist die Schnittstelle als Obermenge aller üblichen Anforderungen zu verstehen, von denen jede Anwendung nur den Teil umsetzt, den sie konkret benötigt.

¹ <https://confluence.bka.extrapol.de/pages/viewpage.action?pageId=129107669#IAMP20Dokumenteübersicht-F-IAM-Gesamtkonzept>

2 Endpunkte

Die von der Anwendung zu unterstützenden Endpunkte hängen davon ab, ob sie AW-Rechte mit oder ohne Dienststellenbezug (oder auch beides) unterstützen.

Endpunkt	Operation	Beschreibung	relevant für AWs
/ResourceTypes	GET	Schemas, Users, Groups, OuPermissions liefert auch die URLs der Endpunkte	immer
/Schemas	GET	Abfrage der Schemata	immer
/Users	GET	Abfrage aller Benutzer Es müssen mindestens die folgenden Filter unterstützt werden: <ul style="list-style-type: none"> • erzeugt ab • geändert ab • startIndex ab (für Pagination) 	immer
	POST	Erstellen eines neuen Benutzers <i>Beim Anlegen werden nie initialen Berechtigungszuweisungen angegeben. Die Pflege der Berechtigungszuweisungen erfolgt ausschließlich über die Endpunkte Groups und OuPermissions.</i>	immer
/Users/{User-ID}	GET	Abfrage eines konkreten Benutzers, ID wird von AW vergeben <i>Liefert auch die Liste aller Berechtigungszuweisungen (auch mit Dst-Bezug), sofern es nicht über Query- Parameter unterbunden wird.</i>	immer
	PUT	Entfällt, Änderungen werden per PATCH vorgenommen	

Endpunkt	Operation	Beschreibung	relevant für AWs
	PATCH	Ändern von Benutzerattributen <i>Pro Nachricht wird immer nur ein Attribut geändert.</i>	
	DELETE	Löschen eines Benutzers	
/Groups	GET	Abfrage aller AW-Rechte ohne Dienststellenbezug. <i>Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)</i>	für AW mit Berechtigungen ohne Dienststellenbezug
/Groups/{Group-ID}	GET	Abfrage eines konkreten AW-Rechts ohne Dienststellenbezug. <i>Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)</i>	
	PATCH	Berechtigungszuweisung hinzufügen/entfernen <i>Pro Nachricht vom F-IAM wird immer nur eine einzelne Operation enthalten sein.</i>	
/OuPermissions	GET	Abfrage aller AW-Rechte mit Dienststellenbezug. <i>Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)</i>	für AW mit Berechtigungen mit Dienststellenbezug
/OuPermissions/{OU-Permission-ID}	GET	Abfrage eines konkreten AW-Rechtes mit Dienststellenbezug. <i>Es kann implizit davon ausgegangen werden, dass die Liste der Zuweisungen unterdrückt wird. (Das F-IAM wird die Liste immer ignorieren.)</i>	

Endpunkt	Operation	Beschreibung	relevant für AWs
	PATCH	<p>Berechtigungszuweisung mit Dienststellenbezug hinzufügen/entfernen</p> <p><i>Pro Nachricht vom F-IAM wird immer nur eine einzelne Operation enthalten sein. (Zuweisen/Entziehen eines einzelnen Rechts für einen einzelnen Benutzer für eine konkrete Dienststelle</i></p>	

3 Benutzerattribute

Die Anwendung darf nur die Benutzerattribute speichern, für die es einen fachlichen Bedarf gibt. Das F-IAM kann dabei nur die Benutzerattribute liefern, die auch von den TN bereitgestellt wurden. Die mögliche Obermenge ist separat beschrieben: [Benutzerattribute im F-IAM](#)²

Es werden so weit wie möglich die Attribute des Standard-Schemas (`urn:ietf:params:scim:schemas:core:2.0:User`) verwendet.

Für die Attribute zum Referenzieren der hierarchischen Entität des Benutzers wird das Schema `urn:ietf:params:scim:schemas:extension:enterprise:2.0:User` (gemäß RFC7643) verwendet, wobei nur die Attribute `organization`, `division` und `department` unterstützt werden. Diese Attribute sind veraltet und sollten möglichst durch den P20-Dienststellenschlüssel ersetzt werden.

JSON-Schema "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"

```
{
  "id": "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
  "name": "EnterpriseUser",
  "description": "Enterprise User",
  "attributes": [
    {
      "name": "employeeNumber",
      "type": "string",
      "multiValued": false,
      "description": "Numeric or alphanumeric identifier assigned to a person, typically based on order of hire or association with an organization.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "costCenter",
      "type": "string",
      "multiValued": false,
      "description": "Identifies the name of a cost center.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    }
  ]
}
```

² <https://confluence.bka.extrapol.de/x/46DMD>

```

    "name": "organization",
    "type": "string",
    "multiValued": false,
    "description": "Identifies the name of an organization.",
    "required": false,
    "caseExact": false,
    "mutability": "readWrite",
    "returned": "default",
    "uniqueness": "none"
  },
  {
    "name": "division",
    "type": "string",
    "multiValued": false,
    "description": "Identifies the name of a division.",
    "required": false,
    "caseExact": false,
    "mutability": "readWrite",
    "returned": "default",
    "uniqueness": "none"
  },
  {
    "name": "department",
    "type": "string",
    "multiValued": false,
    "description": "Identifies the name of a department.",
    "required": false,
    "caseExact": false,
    "mutability": "readWrite",
    "returned": "default",
    "uniqueness": "none"
  },
  {
    "name": "manager",
    "type": "complex",
    "multiValued": false,
    "description": "The user's manager. A complex type that optionally allows
service providers to represent organizational hierarchy by referencing the 'id'
attribute of another User resource.",
    "required": false,
    "subAttributes": [
      {
        "name": "value",
        "type": "string",
        "multiValued": false,
        "description": "The 'id' of the SCIM resource representing the user's
manager.",
        "required": false,
        "caseExact": false,
        "mutability": "readWrite",
        "returned": "default",
        "uniqueness": "none"
      }
    ]
  }
]

```

```

    },
    {
      "name": "$ref",
      "type": "reference",
      "referenceTypes": ["User"],
      "multiValued": false,
      "description": "The URI of the SCIM resource representing the user's
manager.",
      "required": false,
      "caseExact": false,
      "mutability": "readWrite",
      "returned": "default",
      "uniqueness": "none"
    },
    {
      "name": "displayName",
      "type": "string",
      "multiValued": false,
      "description": "The displayName of the user's manager.",
      "required": false,
      "caseExact": false,
      "mutability": "readOnly",
      "returned": "default",
      "uniqueness": "none"
    }
  ]
}

```

Alle weiteren, P20-spezifischen Attribute sind in einem eigenen Extension-Schema `urn:ietf:params:scim:schemas:extension:p20:2.0:User` gesammelt.

JSON-Schema "urn:ietf:params:scim:schemas:extension:p20:2.0:User"

```

{
  "id": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
  "name": "P20User",
  "description": "Schema for P20-specific user attributes.",
  "attributes": [
    {
      "name": "idpUserName",
      "type": "string",
      "multiValued": false,
      "description": "TN-interner Nutzernamen",
      "required": true,
      "mutability": "readWrite",
      "returned": "default"
    },
    {

```

```

    "name": "idpUserId",
    "type": "string",
    "multiValued": false,
    "description": "TN-interne Nutzer-ID",
    "required": false,
    "mutability": "readWrite",
    "returned": "default",
    "uniqueness": "server"
  },
  {
    "name": "p20UId",
    "type": "string",
    "multiValued": false,
    "description": "P20-UID",
    "required": false,
    "mutability": "readWrite",
    "returned": "default"
  },
  {
    "name": "p20DepartmentNumber",
    "type": "string",
    "multiValued": false,
    "description": "P20-Dienststellenschlüssel, referenziert den TN-übergreifenden
Dienststellenkatalog",
    "required": false,
    "mutability": "readWrite",
    "returned": "default"
  },
  {
    "name": "nameSuffix",
    "type": "string",
    "multiValued": false,
    "description": "P20-Namenszusatz, zur Unterscheidung von Benutzern desselben TN
mit identischem Namen",
    "required": false,
    "mutability": "readWrite",
    "returned": "default"
  },
  {
    "name": "policeTitleKey",
    "type": "string",
    "multiValued": false,
    "description": "Schlüssel für Amtsbezeichnung, referenziert den Katalog XXX",
    "required": false,
    "mutability": "readWrite",
    "returned": "default"
  },
  {
    "name": "idp",
    "type": "string",
    "multiValued": false,
    "description": "TN-Kennung",

```

```
    "required": true,  
    "mutability": "immutable",  
    "returned": "default"  
  }  
]  
}
```

4 Berechtigungen

Bei Berechtigungen werden zwischen zwei Typen unterschieden. Dabei liegt es am Bedarf der jeweiligen Anwendung, welche davon sie verwendet (nur eine davon oder auch beide).

4.1 Groups: Berechtigungen ohne Dienststellenbezug

Berechtigungen ohne Dienststellenbezug werden durch den Resource-Typ "Group" abgebildet. Hierbei kann wahlweise der Standard-Endpoint mit dem Standard-

Schema `urn:ietf:params:scim:schemas:core:2.0:Group` verwendet werden.

Sofern der Bedarf besteht, weitere Details zu den Rechten über das F-IAM an die Benutzerverwaltung der TN zu übertragen, kann ein Extension-Schema

(`urn:ietf:params:scim:schemas:extension:p20:2.0:Group`) verwendet werden, in dem bei der Definition ein zusätzliche Attribut `details` enthalten ist.

JSON-Schema "urn:ietf:params:scim:schemas:extension:p20:2.0:Group"

```
{
  "id": "urn:ietf:params:scim:schemas:extension:p20:2.0:Group",
  "name": "CustomGroup",
  "description": "Custom schema for managing permission assignments without a scope
for the organizational unit.",
  "attributes": [
    {
      "name": "id",
      "type": "string",
      "multiValued": false,
      "description": "Unique identifier for the permission.",
      "required": true,
      "mutability": "readOnly",
      "returned": "always",
      "uniqueness": "server"
    },
    {
      "name": "displayName",
      "type": "string",
      "multiValued": false,
      "description": "A human-readable name for the permission.",
      "required": true,
      "mutability": "readWrite",
      "returned": "default"
    }
  ],
  {
```

```

"name": "members",
"type": "complex",
"multiValued": true,
"description": "Users who have been assigned to this permission.",
"mutability": "readWrite",
"returned": "default",
"subAttributes": [
  {
    "name": "value",
    "type": "string",
    "description": "The user's unique identifier.",
    "mutability": "immutable",
    "required": true
  },
  {
    "name": "display",
    "type": "string",
    "description": "A human-readable name of the member.",
    "mutability": "immutable"
  },
  {
    "name": "type",
    "type": "string",
    "description": "The type of member, always 'User'.",
    "mutability": "immutable"
  },
  {
    "name": "$ref",
    "type": "reference",
    "description": "A reference to the member resource.",
    "mutability": "immutable"
  }
],
{
  "name": "details",
  "type": "complex",
  "multiValued": false,
  "description": "Additional details about the permission.",
  "mutability": "readWrite",
  "returned": "default",
  "required": false,
  "subAttributes": [
    {
      "name": "desc",
      "type": "string",
      "description": "Description text for the permission.",
      "mutability": "readWrite",
      "required": false
    },
    {
      "name": "type",

```



```

        "type": "string",
        "description": "The type of permission.",
        "mutability": "readWrite",
        "required": false
    },
    {
        "name": "flags",
        "type": "string",
        "multiValued": true,
        "description": "List of flags related to the permission.",
        "mutability": "readWrite",
        "required": false
    }
]
}
}
}

```

4.2 OU-Permissions: Berechtigungen mit Dienststellenbezug

Berechtigungen mit Dienststellenbezug werden durch einen eigenen Resource-Type "OuPermission" abgebildet.

Mit "Dienststelle" ist hier maximal abstrakt gemeint und beschreibt eine beliebige hierarchische Entität in der Organisationsstruktur. Es kann auch ein Präsidium, eine Dienstgruppe o.ä. sein. Innerhalb des F-IAM wird nicht zwischen diesen Typen unterschieden.

Die Verwendung ist so weit wie möglich an Standard-Groups (Schema

`urn:ietf:params:scim:schemas:core:2.0:Group`) angelehnt und lediglich um folgende Attribute erweitert:

- Attribute `scope` für Berechtigungszuweisungen: Enthält den P20-Dienststellenschlüssel (Referenzieren des TN-übergreifenden Dienststellenkatalogs) zur Einschränkung der Berechtigung als Freitext.
- Attribute `inherit` für Berechtigungszuweisungen: Enthält optional die Information als Boolean, ob sich die Berechtigungszuweisung auch auf untergeordnete Dienststelle beziehen soll.
- Attribut `details` für die Berechtigungsdefinition, die durch das F-IAM an die TN durchgeleitet wird.

JSON-Schema "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"

```

{
  "id": "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission",
  "name": "OuPermission",
  "description": "Schema for managing OuPermission assignments with a scope for the organizational unit.",
  "attributes": [
    {

```

```

    "name": "id",
    "type": "string",
    "multiValued": false,
    "description": "Unique identifier for the OuPermission.",
    "required": true,
    "mutability": "readOnly",
    "returned": "always",
    "uniqueness": "server"
  },
  {
    "name": "displayName",
    "type": "string",
    "multiValued": false,
    "description": "A human-readable name for the OuPermission.",
    "required": true,
    "mutability": "readWrite",
    "returned": "default"
  },
  {
    "name": "members",
    "type": "complex",
    "multiValued": true,
    "description": "Users who have been assigned this OuPermission.",
    "mutability": "readWrite",
    "returned": "default",
    "subAttributes": [
      {
        "name": "value",
        "type": "string",
        "description": "The user's unique identifier.",
        "mutability": "immutable",
        "required": true
      },
      {
        "name": "display",
        "type": "string",
        "description": "A human-readable name of the member.",
        "mutability": "immutable"
      },
      {
        "name": "type",
        "type": "string",
        "description": "The type of member, always 'User'.",
        "mutability": "immutable"
      },
      {
        "name": "$ref",
        "type": "reference",
        "description": "A reference to the member resource.",
        "mutability": "immutable"
      }
    ]
  }
]

```

```

        "name": "scope",
        "type": "string",
        "description": "ID of the organizational unit (Dienststelle) to which this
permission applies.",
        "required": true,
        "mutability": "readWrite",
        "returned": "default"
    },
    {
        "name": "inherit",
        "type": "boolean",
        "description": "Indicates whether this permission is inherited by
subordinate organizational units (Dienststellen).",
        "mutability": "readWrite",
        "returned": "default"
    }
]
},
{
    "name": "details",
    "type": "complex",
    "multiValued": false,
    "description": "Additional details about the permission, including description,
type, and flags.",
    "mutability": "readWrite",
    "returned": "default",
    "required": false,
    "subAttributes": [
        {
            "name": "desc",
            "type": "string",
            "description": "Description text for the permission.",
            "mutability": "readWrite",
            "required": false
        },
        {
            "name": "type",
            "type": "string",
            "description": "The type of permission.",
            "mutability": "readWrite",
            "required": false
        },
        {
            "name": "flags",
            "type": "string",
            "multiValued": true,
            "description": "List of flags related to the permission.",
            "mutability": "readWrite",
            "required": false
        }
    ]
}
]
}

```

```
]
}
```

Die Liste der Zugewiesenen OU-Permissions wird als zusätzliches Attribut `OuPermissions` am Benutzer aufgeführt, wobei die Entitäten referenziert werden und dabei jeweils die konkrete Dienststelle (als `scope`) sowie optional die Angabe zur Vererbung (als `inherit`) angegeben wird.

JSON-Schema-Erweiterung am Benutzer für `OuPermissions`

```
{
  "name": "OuPermissions",
  "type": "complex",
  "multiValued": true,
  "description": "List of assigned OuPermissions for the user.",
  "required": false,
  "mutability": "readOnly",
  "subAttributes": [
    {
      "name": "id",
      "type": "string",
      "description": "Unique identifier for the OuPermission.",
      "required": true
    },
    {
      "name": "displayName",
      "type": "string",
      "description": "Human-readable name for the OuPermission.",
      "required": false
    },
    {
      "name": "$ref",
      "type": "reference",
      "description": "Reference to the OuPermission resource.",
      "required": false,
      "referenceTypes": ["OuPermission"]
    },
    {
      "name": "scope",
      "type": "string",
      "description": "Scope (Dienststelle) reference for the assigned OuPermission.",
      "required": true
    },
    {
      "name": "inherit",
      "type": "boolean",
      "description": "Indicates if the permission applies to subordinate units (Dienststellen).",
      "required": false
    }
  ]
}
```

```
]
}
```

4.3 Details zu AW-Rechten

Das Attribut `details` kann bei der Definition von Berechtigungen durch die AW angegeben werden, um Informationen zur Pflege an die Benutzerverwaltung der TN durch das F-IAM durchleiten zu lassen. Ziel ist es, einen parallelen Informationsfluss (beispielsweise Excel-Tabellen per EMail) von den AWs zu den TNs zu vermeiden. Der Inhalt dieser Struktur wird von dem F-IAM nicht ausgewertet sondern blind durchgereicht. Es kann also prinzipiell ein beliebiges JSON-Objekt beinhalten. Um aber die Kompatibilität der AWs mit allen TNs zu ermöglichen, wird der Aufbau zentral dokumentiert. AWs sind angehalten, neue Inhalte mit der PG-IAM abzustimmen, um Mehrdeutigkeiten zu vermeiden.

Bisherige Inhalte:

- `desc` : Beschreibender Freitext – ausführlicher als der `DisplayName`
- `type` : Typ des Rechts, sofern die Anwendung verschiedene Typen unterscheidet.
- `flags` : Liste von Flags, wobei folgende Ausprägungen bekannt sind:
 - `alwaysInherits` : Eine Berechtigungszuweisung wirkt sich immer auch auf untergeordnete Dienststellen aus (nur bei `OuPermission`)
 - `neverInherits` : Eine Berechtigungszuweisung wirkt sich nie auch auf untergeordnete Dienststellen aus (nur bei `OuPermission`)
 - `hasInheritsAttribute` : Bei der Berechtigungszuweisung wird das Attribut `inherit` ausgewertet. (nur bei `OuPermission`)
 - `exactlyOncePerOu` : Die Berechtigung soll pro Dienststelle exakt einem Benutzer zugewiesen werden. Beim Entziehen, muss es also immer einem neuen Benutzer zugewiesen werden. (z.B. für die Dienststellenleitung)

5 Beispielnachrichten

5.1 Abfrage der AW-Rechte ohne Dst-Bezug



Sofern die Anwendung keine Rechte-Details überträgt, kann sie auch das Core-Schema `urn:ietf:params:scim:schemas:core:2.0:Group` verwenden. `excludeAttributes` würde in dem Fall ohne Schema-Präfix übergeben werden und die Antwort würde das Core-Schema referenzieren.

Hintergrund dieser Differenzierung ist, dass bei Attributen ein SCIMv2-Server davon ausgeht, dass es sich um ein Attribut aus einem Core-Schema handelt. In anderen Fällen (also auch bei /OuPermissions) muss bei `excludeAttributes` das konkrete Schema explizit angegeben werden. (Bei PATCH-Operationen ist das Schema-Prefix für die Attribute hingegen weder in der path- noch in der value-Angabe erforderlich, da die Endpunkte jeweils nur ein einzelnes Schema verwenden und die Attribute somit bereits über ihren Namen eindeutig sind.)

Anfrage

```
GET: https://.../aw/scim/Groups?
excludeAttributes=urn:ietf:params:scim:schemas:extension:p20:2.0:Group:members
```

Antwort

```
HTTP/1.1 200 OK
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ],
  "totalResults": 2,
  "Resources": [
    {
      "id": "RECHT_1",
      "schemas": [
        "urn:ietf:params:scim:schemas:extension:p20:2.0:Group"
      ]
    }
  ]
}
```

```

    "meta": {
      "resourceType": "Group",
      "created": "2024-10-09T15:00:00Z",
      "lastModified": "2024-10-09T15:00:00Z",
      "location": "https://.../aw/scim/Groups/RECHT_1"
    },
    "displayName": "Recht eins",
    "details": {
      "desc": "Beschreibung von Recht-1"
    }
  },
  {
    "id": "RECHT_2",
    "schemas": [
      "urn:ietf:params:scim:schemas:extension:p20:2.0:Group"
    ],
    "meta": {
      "resourceType": "Group",
      "created": "2024-10-09T15:00:00Z",
      "lastModified": "2024-10-09T15:00:00Z",
      "location": "https://.../aw/scim/Groups/RECHT_2"
    },
    "displayName": "Recht zwei",
    "details": {
      "desc": "Beschreibung von Recht-2"
    }
  }
]
}

```

5.2 Abfrage der AW-Rechte mit Dst-Bezug

Anfrage

```

GET: https://.../aw/scim/OuPermissions?
excludedAttributes=urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission:members

```

Antwort

```

HTTP/1.1 200 OK
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ],

```

```

"totalResults": 2,
"Resources": [
  {
    "id": "DST_RECHT_1",
    "schemas": [
      "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"
    ],
    "meta": {
      "resourceType": "OuPermission",
      "created": "2024-10-09T15:00:00Z",
      "lastModified": "2024-10-09T15:00:00Z",
      "location": "https://.../aw/scim/OuPermissions/DST_RECHT_1"
    },
    "displayName": "Recht mit Dst-Bezug eins",
    "details": {
      "desc": "Beschreibung von Dst-Recht-1",
      "flags": ["HasInheritsAttribute"]
    }
  },
  {
    "id": "DST_RECHT_2",
    "schemas": [
      "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission"
    ],
    "meta": {
      "resourceType": "OuPermission",
      "created": "2024-10-09T15:00:00Z",
      "lastModified": "2024-10-09T15:00:00Z",
      "location": "https://.../aw/scim/OuPermissions/DST_RECHT_2"
    },
    "displayName": "Recht mit Dst-Bezug zwei",
    "details": {
      "desc": "Beschreibung von Dst-Recht-2",
      "flags": []
    }
  }
]
}

```

5.3 Anlegen eines Benutzers

Anfrage

```

POST: https://.../aw/scim/Users
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8.....
Content-Length: ...

```



```

{
  "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"
  ],
  "userName": "by04765432",
  "name": {
    "familyName": "Dampf",
    "givenName": "Hans"
  },
  "title": "Dr.",
  "emails": [
    {
      "primary": true,
      "type": "work",
      "value": "hans.dampf@polizei.bayern.de"
    }
  ],
  "phoneNumbers": [
    {
      "primary": true,
      "type": "work",
      "value": "+49 123 456789"
    },
    {
      "type": "fax",
      "value": "+49 987 654321"
    },
    {
      "type": "cnp",
      "value": "7-123-4567"
    }
  ],
  "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User": {
    "organizational": "123",
    "division": "456",
    "department": "789"
  },
  "urn:ietf:params:scim:schemas:extension:p20:2.0:User": {
    "idpUserName": "hans.dampf@polizei.bayern.de",
    "idpUserId": "04765432",
    "p20Uid": "T-36-9-09-9876543",
    "p20DepartmentNumber": "BY-123",
    "nameSuffix": "2",
    "policeTitleKey": "123",
    "idp": "BY"
  }
}

```

Antwort

```

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"
  ],
  "id": "1001",
  "meta": {
    "resourceType": "User",
    "created": "2011-08-01T21:32:44.882Z",
    "lastModified": "2011-08-01T21:32:44.882Z",
    "location": "https://.../aw/scim/Users/1001"
  },
  "userName": "by04765432"
  ...
}

```

5.4 Ändern eines Benutzers

Anfrage: Nachname ändern

```

PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8.....
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path": "name.familyName",
      "value": "Dampf2"
    }
  ]
}

```

Anfrage: Telefonnummer ändern

```

PATCH https://.../aw/scim/Users/1001

```

```

Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8.....
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path": "phoneNumbers[type eq \"work\"].value",
      "value": "+49 123 987654"
    }
  ]
}

```

Anfrage: P20-Dienststelle ändern

```

PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8.....
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path":
"urn:ietf:params:scim:schemas:extension:p20:2.0:User:p20DepartmentNumber",
      "value": "BY-456"
    }
  ]
}

```

Anfrage: Abteilung löschen

```

PATCH https://.../aw/scim/Users/1001
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8.....
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "replace",
      "path": "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department",

```

```
    "value": ""  
  }  
]  
}
```

Antwort

HTTP/1.1 204 No Content

5.5 Zuweisen eines Rechts ohne Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/Groups/RECHT_1  
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" : "1001"  
        }  
      ]  
    }  
  ]  
}
```

Antwort

HTTP/1.1 204 No Content

5.6 Entziehen eines Rechts ohne Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/Groups/RECHT_1
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8.....
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:PatchOp"],
  "Operations": [
    {
      "op"    : "remove",
      "path"  : "members[value eq \"1001\"]"
    }
  ]
}
```

Antwort

HTTP/1.1 204 No Content

5.7 Zuweisen eines Rechts mit Dst-Bezug

Anfrage

```
PATCH https://.../aw/scim/OuPermissions/DST_RECHT_1
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": "1001",

```

```

        "scope": "09_10_0900313400000_001",
        "inherit": false
    },
    {
        "type": "User",
        "value": "1001",
        "scope": "09_10_0900987600000",
        "inherit": true
    }
]
}
]
}

```

Antwort

HTTP/1.1 204 No Content

5.8 Entziehen eines Rechts mit Dst-Bezug

Anfrage

```

PATCH https://.../aw/scim/OuPermissions/DST_RECHT_1
Accept: application/scim+json
Content-Type: application/scim+json Authorization: Bearer h480djs93hd8.....
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "remove",
      "path": "members[value eq \"1001\" and scope eq \"09_10_0900313400000_001\"]"
    },
    {
      "op": "remove",
      "path": "members[value eq \"1001\" and scope eq \"09_10_0900987600000\"]"
    }
  ]
}

```

Antwort

HTTP/1.1 204 No Content

5.9 Benutzerabfragen für Abgleich

5.9.1 Neue Benutzer

Anfrage nach Nutzern, die seit dem 01.10.2024 00:00:00 erzeugt wurden.

```
GET https://.../aw/scim/Users?filter=meta.created gt "2024-10-01T00:00:00Z"
```

5.9.2 Geänderte Benutzer

Anfrage nach Nutzern, die seit dem 01.10.2024 00:00:00 geändert wurden.

```
GET https://.../aw/scim/Users?filter=meta.lastModified gt "2024-10-01T00:00:00Z"
```

5.9.3 Neue und geänderte Benutzer

Anfrage nach Nutzern, die seit dem 01.10.2024 00:00:00 erzeugt oder geändert wurden.

```
GET https://.../aw/scim/Users?filter=meta.created gt "2024-10-01T00:00:00Z" or  
meta.lastModified gt "2024-10-01T00:00:00Z"
```

5.9.4 Alle Benutzer, erste Anfrage

Anfrage nach allen Benutzern für einen Komplettabgleich, wobei lediglich 100 Treffer erwartet werden.

```
GET https://.../aw/scim/Users?count=100
```

5.9.5 Alle Benutzer, zweite Anfrage (Pagination)

Anfrage nach allen Benutzern für einen Komplettabgleich, wobei lediglich 100 Treffer erwartet werden, aber beginnend ab dem Benutzer nach der ersten Abfrage.

```
GET https://.../aw/scim/Users?startIndex=101&count=100
```

5.9.6 Antwort

```
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ],
  "totalResults": 3,
  "itemsPerPage": 0,
  "startIndex": 0,
  "Resources": [
    {
      "id": "1001",
      "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"
      ],
      "meta": {
        "resourceType": "User",
        "created": "2011-08-01T21:32:44.882Z",
        "lastModified": "2011-08-01T21:32:44.882Z",
        "location": "https://.../aw/scim/Users/1001"
      },
      "userName": "by04765432",
      "name": {
        "familyName": "Dampf",
        "givenName": "Hans"
      },
      "title": "Dr.",
      "emails": [
        {
          "primary": true,
          "type": "work",
          "value": "hans.dampf@polizei.bayern.de"
        }
      ],
      "phoneNumbers": [
        {
          "primary": true,
          "type": "work",
          "value": "+49 123 456789"
        },
        {
          "type": "fax",
          "value": "+49 987 654321"
        }
      ]
    }
  ]
}
```



```

    {
      "type": "cnp",
      "value": "7-123-4567"
    }
  ],
  "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User": {
    "organizational": "123",
    "division": "456",
    "department": "789"
  },
  "urn:ietf:params:scim:schemas:extension:p20:2.0:User": {
    "idpUserName": "hans.dampf@polizei.bayern.de",
    "idpUserId": "04765432",
    "p20Uid": "T-36-9-09-9876543",
    "p20DepartmentNumber": "BY-123",
    "nameSuffix": "2",
    "policeTitleKey": "123",
    "idp": "BY"
  },
  "groups": [
    {
      "value": "RECHT_1",
      "display": "Recht eins",
      "$ref": "https://.../aw/scim/Groups/RECHT_1",
    }
  ],
  "OuPermissions": [
    {
      "value": "DST_RECHT_1",
      "display": "Recht mit Dst-Bezug eins",
      "$ref": "https://.../aw/scim/OuPermissions/DST_RECHT_1",
      "scope": "09_10_0900313400000_001",
      "inherit": false
    },
    {
      "value": "DST_RECHT_1",
      "display": "Recht mit Dst-Bezug eins",
      "$ref": "https://.../aw/scim/OuPermissions/DST_RECHT_1",
      "scope": "09_10_0900987600000",
      "inherit": true
    }
  ]
},
...
]
}

```

6 Fehlermeldungen

Der AW-SCIMv2-Server soll in den folgenden Fehlerfällen die entsprechenden Fehlermeldungen zurückgeben.

Liste der Fehlermeldungen

- Benutzer anlegen:
 - Obligatorische Daten im User fehlen (familyName, givenName, idpUserId, p20DepartmentNumber)

```
HTTP/1.1 400 Bad Request
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request failed due to invalid syntax.",
  "status": "400",
  "scimType": "invalidValue",
  "resourceType": "User",
  "errors": [
    {
      "status": "400",
      "detail": "The required attribute 'givenName' is missing.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
      "value": null
    },
    {
      "status": "400",
      "detail": "The required attribute 'familyName' is missing.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
      "value": null
    },
    {
      "status": "400",
      "detail": "The required attribute 'idpUserId' is missing.",
      "schema": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
      "value": null
    },
    {
      "status": "400",
      "detail": "The required attribute 'p20DepartmentNumber' is
missing.",
      "schema": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
      "value": null
    }
  ]
}
```

- Benutzer besteht schon (idpUserId einen aktiven anderen Benutzer zugewiesen, falls eine idpUserId transferiert werden soll, dann muss erst die ID beim alten Benutzer gelöscht und dann beim neuen Benutzer angelegt werden)

```
HTTP/1.1 409 Conflict
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request could not be completed due to a conflict with
the current state of the resource.",
  "status": "409",
  "scimType": "uniqueness",
  "resourceType": "User",
  "errors": [
    {
      "status": "409",
      "detail": "The attribute 'idpUserId' must be unique. The provided
value is already in use.",
      "schema": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
      "value": "existing_idp_user_id"
    }
  ]
}
```

- Benutzer über SCIM aktualisieren:
 - Benutzer ist in Anwendung nicht vorhanden (technische ID in Anwendung nicht vorhanden)

```
HTTP/1.1 404 Not Found
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The requested resource was not found.",
  "status": "404",
  "scimType": "resourceNotFound",
  "resourceType": "User",
  "errors": [
    {
      "status": "404",
      "detail": "The User with id 'unknown_user_id' does not exist.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
      "value": "unknown_user_id"
    }
  ]
}
```

- Benutzererkennung ist doppelt (neue idpUserId ist bereits einem anderen Benutzer zugewiesen, siehe oben)

HTTP/1.1 409 Conflict

Content-Type: application/json

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request could not be completed due to a conflict with
the current state of the resource.",
  "status": "409",
  "scimType": "uniqueness",
  "resourceType": "User",
  "errors": [
    {
      "status": "409",
      "detail": "The attribute 'idpUserId' must be unique. The provided
value is already in use by another user.",
      "schema": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
      "value": "existing_idp_user_id"
    }
  ]
}
```

- Obligatorische Datenfelder verletzt (remove oder replace mit LEER-Wert wird auf obligatorische Daten - siehe oben - ausgeführt)

HTTP/1.1 400 Bad Request

Content-Type: application/json

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request failed due to invalid syntax.",
  "status": "400",
  "scimType": "invalidValue",
  "resourceType": "User",
  "errors": [
    {
      "status": "400",
      "detail": "The required attribute 'givenName' cannot be set to an
empty value.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
      "value": ""
    },
    {
      "status": "400",
      "detail": "The required attribute 'familyName' cannot be set to an
empty value.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
      "value": ""
    },
    {
      "status": "400",

```

```

    "detail": "The required attribute 'idpUserId' cannot be set to an
empty value.",
    "schema": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
    "value": ""
  },
  {
    "status": "400",
    "detail": "The required attribute 'p20DepartmentNumber' cannot be
set to an empty value.",
    "schema": "urn:ietf:params:scim:schemas:extension:p20:2.0:User",
    "value": ""
  }
]
}

```

- Berechtigung zuweisen:
 - Berechtigung ohne Dst-Bezug nicht bekannt

```

HTTP/1.1 404 Not Found
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The requested resource was not found.",
  "status": "404",
  "scimType": "resourceNotFound",
  "resourceType": "Group",
  "errors": [
    {
      "status": "404",
      "detail": "The Group with id 'unknown_group_id' does not exist.",
      "schema": "urn:ietf:params:scim:schemas:core:2.0:Group",
      "value": "unknown_group_id"
    }
  ]
}

```

- Berechtigung mit Dst-Bezug nicht bekannt

```

HTTP/1.1 404 Not Found
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The requested resource was not found.",
  "status": "404",
  "scimType": "resourceNotFound",
  "resourceType": "OuPermission",
  "errors": [

```

```
{
  "status": "404",
  "detail": "The OuPermission with id 'unknown_permission_id' does not exist.",
  "schema":
    "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission",
  "value": "unknown_permission_id"
}
```

- OU nicht bekannt

```
HTTP/1.1 404 Not Found
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The requested OU resource was not found.",
  "status": "404",
  "scimType": "resourceNotFound",
  "resourceType": "OuPermission",
  "errors": [
    {
      "status": "404",
      "detail": "The OU with id 'unknown_ou_id' does not exist.",
      "schema":
        "urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission",
      "value": "unknown_ou_id"
    }
  ]
}
```

- Berechtigung ohne Dst-Bezug ist schon zugewiesen

```
HTTP/1.1 409 Conflict
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request could not be completed due to a conflict with the current state of the resource.",
  "status": "409",
  "scimType": "conflict",
  "resourceType": "Group",
  "errors": [
    {
      "status": "409",
      "detail": "The group with id 'group_id' is already assigned to the user.",
    }
  ]
}
```

```

        "schema": "urn:ietf:params:scim:schemas:core:2.0:Group",
        "value": "group_id"
    }
]
}

```

- Berechtigung mit Dst-Bezug ist schon zugewiesen

```

HTTP/1.1 409 Conflict
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request could not be completed due to a conflict with
the current state of the resource.",
  "status": "409",
  "scimType": "conflict",
  "resourceType": "OuPermission",
  "errors": [
    {
      "status": "409",
      "detail": "The OuPermission with id 'ou_permission_id' for scope
'ou_id' is already assigned to the user.",
      "schema":
"urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission",
      "value": {
        "scope": "ou_id",
        "permissionId": "ou_permission_id"
      }
    }
  ]
}

```

- Berechtigung entziehen:
 - Berechtigung nicht bekannt
→ *identisch zum Zuweisen einer unbekannten Berechtigung*
 - Berechtigung ohne Dst-Bezug ist nicht zugewiesen

```

HTTP/1.1 409 Conflict
Content-Type: application/json

{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request could not be completed due to a conflict with
the current state of the resource.",
  "status": "409",
  "scimType": "conflict",
  "resourceType": "Group",
  "errors": [

```

```
{
  "status": "409",
  "detail": "The group with id 'group_id' is not assigned to the
user.",
  "schema": "urn:ietf:params:scim:schemas:core:2.0:Group",
  "value": "group_id"
}
]
```

- Berechtigung mit Dst-Bezug ist nicht zugewiesen

HTTP/1.1 409 Conflict

Content-Type: application/json

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The request could not be completed due to a conflict with
the current state of the resource.",
  "status": "409",
  "scimType": "conflict",
  "resourceType": "OuPermission",
  "errors": [
    {
      "status": "409",
      "detail": "The OuPermission with id 'ou_permission_id' for scope
'ou_id' is not assigned to the user.",
      "schema":
"urn:ietf:params:scim:schemas:extension:p20:2.0:OuPermission",
      "value": {
        "scope": "ou_id",
        "permissionId": "ou_permission_id"
      }
    }
  ]
}
```

- Benutzer über SCIM abfragen
 - Benutzer-ID nicht bekannt

HTTP/1.1 404 Not Found

Content-Type: application/json

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],
  "detail": "The requested user resource was not found.",
  "status": "404",
  "scimType": "resourceNotFound",
  "resourceType": "User",
}
```



```
"errors": [  
  {  
    "status": "404",  
    "detail": "The User with id 'unknown_user_id' does not exist.",  
    "schema": "urn:ietf:params:scim:schemas:core:2.0:User",  
    "value": "unknown_user_id"  
  }  
]  
}
```

7 Authentifizierung

Zur Authentifizierung wird das F-IAM ein selbst ausgestelltes JWT als Bearer-Token übergeben. Die Signatur ist also gegen das OIDC-Zertifikat des F-IAM zu prüfen (siehe [Access Manager Zugangsdaten](#)³).

Scope und erforderliches Recht (im groups-Claim des JWT) werden bei der Anbindung individuell abgestimmt. Aus Sicht des F-IAM handelt es sich hierbei um eine andere Anwendung als für die Authentifizierung von Benutzern, die die Anwendung verwenden wollen, da die Berechtigung zum Zugriff auf die SCIMv2-Schnittstelle nicht durch die TN vergeben werden darf.

³ <https://confluence.bka.extrapol.de/x/MzS-CQ>