## Benutzerattribute

### 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 Nutzername",

      "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"

    }

  ]

}

p20DepartmentNumber und policeTitleKey

Ist das nicht das Gleiche?

## Berechtigungen

### Groups: Berechtigungen ohne Dienststellenbezug

Das Schema entspricht weitgehend dem urn:ietf:params:scim:schemas:core:2.0:Group und wird um das Segment *details* erweitert.

Das erfordert Anpassungen im F-IAM, da hier eine Persistierung zu implementieren ist, die für das F-IAM selbst keine Relevanz hat und nur für das Auspielen dieser Daten gegenüber den Teilnehmern vorgenommen wird.

Das F-IAM wird das selbst in keiner Art und Weise verarbeiten.

### OU-Permissions: Berechtigungen mit Dienststellenbezug

Soweit Ok, bis auf das Segment details.  
Das erfordert Anpassungen im F-IAM, da hier eine Persistierung zu implementieren ist, die für das F-IAM selbst keine Relevanz hat und nur für das Auspeilen dieser Daten gegenüber den Teilnehmern vorgenommen wird.

### Details zu AW-Rechten

Das Ziel ist verständlich, nur entsprechend der belieben obigen Punkte bedenklich.

Eine Teilnehmer hat keine Kenntnis darüber auf welche Art und Weise eine Anwendung/Dienst angebunden ist. Weiterhin sind die angebunden System in ihrer Ausprägung sehr heterogen. Mit diesem Ansatz wird nun verfolgt mehr Informationen über exakt einen Typ vom System bereitzustellen, den andere Typen nicht in der Lage sein werden zu leisten.

## Anlegen eines Benutzers

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"

  }

}

Das müsste eigentlich organization heißen

Bezüglich der Daten zu Organisationen, wir explodieren mittlerweile in Organisation-Keys (siehe grüne Marker). Eine Konsoldierung scheint hier angebracht, auch unter der Berücksichtigung, das über alle Teilnehmer hinweg betrachtet, die Minorität einen diesbezüglichen Bedarf zu haben scheint.

## Benutzerabfragen für Abgleich

### Antwort (Response Metadaten)

{

  "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

        }

      ]

    },

    ...

  ]

}

  "totalResults": 3,

  "itemsPerPage": 3,

  "startIndex": 1,

ItemsPerPage ist nur dann 0 wenn außerhalb des ResultSets navigiert wurde

Startindex kann niemals Kleiner 1 sein

          "type": "cnp",

          "value": "7-123-4567"

        }

The sub-attribute "type" often has typical values of "work", "home", "mobile", "fax", "pager", and "other" and **MAY** allow more types to be defined by the SCIM clients.

Sollte also statthaft sein

Fehlermeldungen

{

  "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

    }

  ]

}

Das gibt der RFC Standard so nicht her.

Ob diese Fehler so eintreten ist zu prüfen. Bisher gehen wir nicht davon aus, das Bulk-Operationen zum Einsatz kommen. Innerhalb von PATCH wird versucht, dass singular zu halten.

## 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](https://confluence.bka.extrapol.de/x/MzS-CQ)).