Review AW-SCIMv2-Extended – ENTWURF-v21-20241212_115951-2

Abschnitt Einleitung

Keine Findings

Abschnitt Endpunkte

Endpunkt Schemas

Finding:
Die Relevanz diese Endpunkt ergibt sich aus der Prüfung der Deklaration gegen die Implementierung, zumindest auf Basis eine Sichtkontrolle.
Der Verzicht auf die Bereitstellung diese Endpunkt führt zu erhöhten Aufwenden während der Implementierung.
Der Konnektor im IAM setzt die Existenz diese Endpunkt voraus.

Abschnitt 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"
    }
  ]
}
```


Finding:
p20DepartmentNumber und policeTitleKey Ist das nicht das Gleiche?
Ich habe die Befürchtung, wir erfinden immer weiter Organisationselement.
Mittlerweile habe wir bereits 5:

Attribute	SCIM Attribute	
organizationalUnit	urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:User:organizationalUnit	The organizational unit which the user belong to. This is for delegated-administration

		purposes. Should be sourced from the participant source system. e.g. if ou=organizationName, value here is "organizationName"
division	urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:User:division	The organizational divison which the user belong to.
department	urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:User:department	The organizational department which the user belong to.
genericOU	urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:User:genericOU</scimAttribute>	The generic organizational unit which the user belong to. Mainly used only within the PLX-LDAP scope.
xcatalogOU	urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:User:xcatalogOU	The X-Polizei catalog organizational unit which the user belong to.

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 Ausspielen 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 Ausspeilen dieser Daten gegenüber den Teilnehmern vorgenommen wird.

Details zu AW-Rechten

Das Ziel ist verständlich, nur entsprechend der beiden 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.

Abschnitt 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
    }
  ]
}
```


Finding:
Das gibt der RFC Standard so nicht her, zumindest nicht mit der Schema-Definition `urn:ietf:params:scim:api:messages:2.0:Error`.
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.

Abschnitt 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"
  }
}
```

Finding:
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User
Das müsste eigentlich `organization` heißen.

Abschnitt 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
      }
    ]
  },
  ...
]
```

```
}
```

Finding:
Response Metadaten

```
  "totalResults": 3,
   "itemsPerPage": 3,
   "startIndex": 1,
```

ItemsPerPage ist nur dann 0 wenn außerhalb des Result Sets navigiert wurde
Startindex kann niemals kleiner 1 sein.

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User
Das müsste eigentlich `organization` heißen.

Bezüglich der Daten zu Organisationen allgemein, 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.

```
{
  "type": "cnp",
  "value": "7-123-4567"
}
```

RFC:
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

Abschnitt 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).

Zur Authentifizierung wird das F-IAM ein selbst ausgestelltes JWT als Bearer-Token übergeben. Die Signatur ist also gegen den JSON-WebKey (JWK) des F-IAM zu prüfen (siehe Access Manager Zugangsdaten).