TM Forum Specification

Federated Identity API User Guide

TMF691
Team Approved Date: 28-May-2020

Release Status: Pre-production	Approval Status: Team Approved
Version 4.0.0	IPR Mode: RAND

NOTICE

Direct inquiries to the TM Forum office:

4 Century Drive, Suite 100
Parsippany, NJ 07054, USA
Tel No. +1 973 944 5100
Fax No. +1 973 998 7196
TM Forum Web Page: www.tmforum.org

Table of Contents

List of Tables

N/A

Introduction

The following document is the specification of the REST API for Federated ID Management. It includes the model definition as well as all available operations for SID userinfo entity.
This API covers the operations required to allow an application (for instance a selfcare mobile app) request identity information about the individual that is making use of the functionality provided by such application (the user), or in general to allow an application to request identity related information about an individual to the system holding such identity information. This API, instead of defining new operations, relies on the use of industry standard for identity information such as OpenID Connect (http://openid.net/specs/openid-connect-core-1_0.html) and
OAuth2.0 (RFC6749).

This API manages Federated Identity because it defines the operations that must be supported by any system in order to allow providing identity related information (i.e.: the set of attributes related to the individual, such as name, family name, primary phone number, gender, birthdate, …) to different requesting applications, provided they are authorized to perform such request. Authorization can be granted by providing a valid proof of authorization (e.g.: an OAuth2.0 token) granted by the individual whose identity is being requested.

It is up to each implementation to define how authorization can be provided (and confirmed), this API only defines the operations required to request identity related information by an authorized application. As indicated before industry standard mechanisms (OpenID Connect and OAuth2.0) are considered for the implementation of this API, therefore it is assumed in this specification that the request for user´s identity includes an Authorization header with a valid token.

This API relates with existing TM Forum PartyManagement API (TMF632) because a user is actually an individual (i.e.: a party) acting with the role of “user” when interacting with the application requesting the identity information, therefore the so called “userinfo” can be actually either an extension or a subset of the specific party data information, which typically encompasses identity related and any other additional information related to such individual (such as for instance the date when the individual registered in the system, the status or the list of other related parties which is not identity-specific information).

This API defines a set of extended claims over those standard claims defined in OpenID Connect, in order to provide not only the basic user identity information but also the so called “userAssets” or list of assets that can be managed by the individual whose identity information is being requested.

SAMPLE USE CASES

This section includes a set of main use cases that can be performed with this API. Additional use cases can be generated using the operations and resources defined in this specification.

- An application that is being used by an individual and provides functionality to that individual (i.e.: End user) based on his identity (for instance a selfCare application that greets the user displaying his name on the screen), needs to identify such individual.

  In order to obtain identity information of the individual, the app performs the following steps

  1. The application obtains a proof of authorization by the individual to request his identity information (e.g.: an OAUth2.0 token)

  2. The application requests the identity-related information of the user (i.e.: the userinfo) associated to the individual whose proof of authorization is provided

- An application that is being used by an individual and provides functionality to that individual (i.e.: End user) based on the information stored in a system (for instance a selfCare application that will request billing information about the billing accounts associated to the user), needs to identify such individual and know what assets that user can manage.

  In order to obtain identity information of the individual, the app performs the following steps

  1. The application obtains a proof of authorization by the individual to request his identity information (e.g.: an OAUth2.0 token)

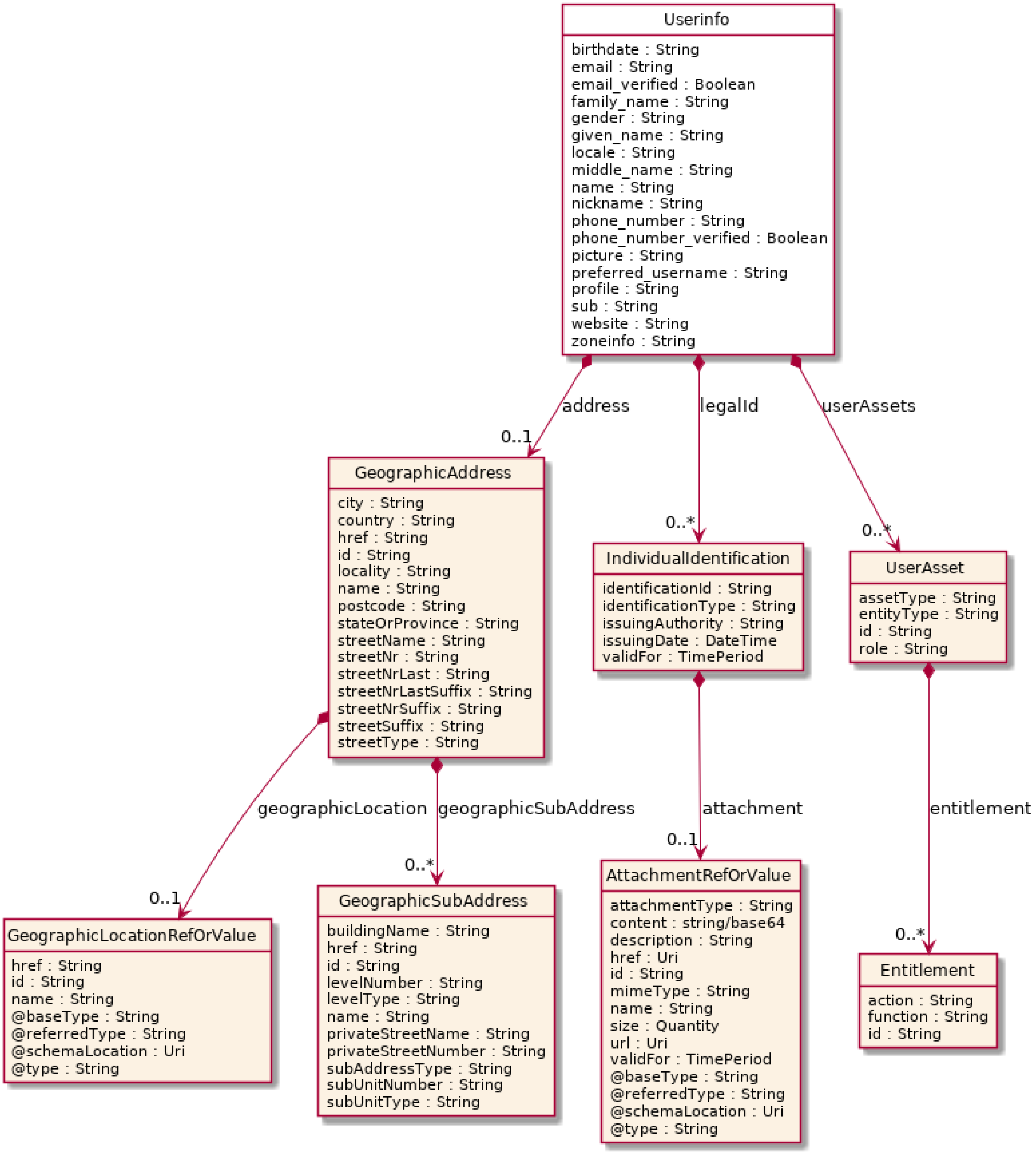
  2. The application requests the identity-related information of the user (i.e.: the userinfo and userAssets) associated to the individual whose proof of authorization is provided

Reader will find additional example of use cases using Usage API in “Open Digital Business Scenarios and Use Cases” document.

RESOURCE MODEL

Userinfo resource

Resource model



Field descriptions

Userinfo fields

address

A geographic address (GeographicAddress). Structure including the End-User's preferred postal address.

birthdate

A string. End-User's birthday, represented as an [ISO8601-2004] YYYY-MM-DD format. The year MAY be 0000, indicating that it is omitted. To represent only the year, YYYY format is allowed. Note that depending on the underlying platform's date related function, providing just year can result in varying month and day, so the implementers need to take this factor into account to correctly process the dates.

email

A string. End-User's preferred e-mail address. Its value MUST conform to the [RFC5322] addr-spec syntax.

email_verified

A boolean. True if the user's email has been verified.

family_name

A string. Surname(s) or last name(s) of the End-User. Note that in some cultures, people can have multiple family names or no family name; all can be present, with the names being separated by space characters.

gender

A string. End-User's gender. Values defined by this specification are female and male. Other values MAY be used when neither of the defined values are applicable.

given_name

A string. Given name(s) or first name(s) of the End-User. Note that in some cultures, people can have multiple given names; all can be present, with the names being separated by space characters.

legalId

A list of individual identifications (IndividualIdentification [*]). Identification documentation of the contact.

locale

A string. End-User's locale, represented as a [RFC5646] language tag. This is typically an [ISO639-1] language code in lowercase and an [ISO3166-1] country code in uppercase, separated by a dash. For example, en-US or fr-CA. As a compatibility note, some implementations have used an underscore as the separator rather than a dash, for example, en_US.

middle_name

A string. Middle name(s) of the End-User. Note that in some cultures, people can have multiple middle names; all can be present, with the names being separated by space characters. Also note that in some cultures, middle names are not used.

name

A string. End-User's full name in displayable form including all name parts, possibly including titles and suffixes, ordered according to the End-User's locale and preferences.

nickname

A string. Casual name of the End-User that may or may not be the same as the given_name. For instance, a nickname value of Mike might be returned alongside a given_name value of Michael.

phone_number

A string. End-User's preferred telephone number. [E.164] is RECOMMENDED as the format of this Claim, for example, +1 (425) 555-1212 or +56 82) 687 2400. If the phone number contains an extension, it is RECOMMENDED that the extension be represented using the [RFC3966] extension syntax, for example, +1 (604) 555-1234;ext=5678.

phone_number_verified

A boolean. True if the user's phone number has been verified.

picture

A string. URL of the End-User's profile picture. This URL MUST refer to an image file (for example, a PNG, JPEG, or GIF image file), rather than to a Web page containing an image. Note that this URL SHOULD specifically reference a profile photo of the End-User suitable for displaying when describing the End-User, rather than an arbitrary photo taken by the End-User.

preferred_username

A string. Shorthand name by which the End-User wishes to be referred to at the RP, such as janedoe or j.doe. This value MAY be any valid JSON string including special characters such as @, /, or whitespace.

profile

A string. URL of the End-User's profile page. The contents of this Web page SHOULD be about the End-User.

sub

A string. Subject - Unique Identifier for the End-User.

userAssets

A list of user assets (UserAsset [*]). List of additional profile information.

website

A string. URL of the End-User's Web page or blog. This Web page SHOULD contain information published by the End-User or an organization that the End-User is affiliated with.

zoneinfo

A string. String from zoneinfo time zone database representing the End-User's time zone. For example, Europe/Paris or America/Los_Angeles.

AttachmentRefOrValue sub-resource

An attachment by value or by reference. An attachment complements the description of an element, for example through a document, a video, a picture.

@referredType

A string. The actual type of the target instance when needed for disambiguation.

description

A string. A narrative text describing the content of the attachment.

href

An uri (Uri). URI for this Attachment.

id

A string. Unique identifier for this particular attachment.

url	An uri (Uri). Uniform Resource Locator, is a web page address (a subset of URI).
name	A string. The name of the attachment.
@baseType	A string. When sub-classing, this defines the super-class.
@schemaLocation	An uri (Uri). A URI to a JSON-Schema file that defines additional attributes and relationships.
@type	A string. When sub-classing, this defines the sub-class Extensible name.
attachmentType	A string. Attachment type such as video, picture.
content	A base 6 4 (Base64). The actual contents of the attachment object, if embedded, encoded as base64.
mimeType	A string. Attachment mime type such as extension file for video, picture and document.
size	A quantity (Quantity). The size of the attachment.
validFor	A time period. The period of time for which the attachment is valid.

Entitlement sub-resource

An Entitlement defines access levels to operate over a given function that can be included in an asset.

action	A string. Level of access granted as part of the permission.
function	A string. Specific function that can be managed over a given asset.
id	A string. Identifier of the entitlement.

GeographicAddress sub-resource

Structured textual way of describing how to find a Property in an urban area (country properties are often defined differently).
Note : Address corresponds to SID UrbanPropertyAddress.

href	A string. Unique reference of the place.
id	A string. Unique identifier of the place.
name	A string. A user-friendly name for the place, such as [Paris Store], [London Store], [Main Home].
city	A string. City that the address is in.
country	A string. Country that the address is in.
geographicLocation	A geographic location ref or value (GeographicLocationRefOrValue). A GeographicLocation is a pure-virtual super-class to the GeoJSON-aligned

geometries of Point (addresses and locations), MultiPoint, LineString (streets, highways and boundaries), MultiLineString and Polygon (countries, provinces, tracts of land). Use the @type attribute to specify which of these is being specified by the geometry attribute.

geographicSubAddress
A list of geographic sub addresses (GeographicSubAddress [*]).
Representation of a GeographicSubAddress
It is used for addressing within a property in an urban area (country properties are often defined differently). It may refer to a building, a building cluster, or a floor of a multistory building.

locality
A string. An area of defined or undefined boundaries within a local authority or other legislatively defined area, usually rural or semi rural in nature. [ANZLIC-STREET], or a suburb, a bounded locality within a city, town or shire principally of urban character [ANZLICSTREET].

postcode
A string. descriptor for a postal delivery area, used to speed and simplify the delivery of mail (also know as zipcode).

stateOrProvince
A string. the State or Province that the address is in.

streetName
A string. Name of the street or other street type.

streetNr
A string. Number identifying a specific property on a public street. It may be combined with streetNrLast for ranged addresses.

streetNrLast
A string. Last number in a range of street numbers allocated to a property.

streetNrLastSuffix
A string. Last street number suffix for a ranged address.

streetNrSuffix
A string. the first street number suffix.

streetSuffix
A string. A modifier denoting a relative direction.

streetType
A string. alley, avenue, boulevard, brae, crescent, drive, highway, lane, terrace, parade, place, tarn, way, wharf.

GeographicLocationRefOrValue sub-resource

A GeographicLocation is a pure-virtual super-class to the GeoJSON-aligned geometries of Point (addresses and locations), MultiPoint, LineString (streets, highways and boundaries), MultiLineString and Polygon (countries, provinces, tracts of land). Use the @type attribute to specify which of these is being specified by the geometry attribute.

@referredType
A string. The actual type of the target instance when needed for disambiguation.

name
A string. A user-friendly name for the place, such as [Paris Store], [London Store], [Main Home].

href
A string. Unique reference of the place.

id	A string. Unique identifier of the place.
@baseType	A string. When sub-classing, this defines the super-class.
@schemaLocation	An uri (Uri). A URI to a JSON-Schema file that defines additional attributes and relationships.
@type	A string. The name of the GeoJSON structure used in the geometry attribute.

GeographicSubAddress sub-resource

Representation of a GeographicSubAddress
It is used for addressing within a property in an urban area (country properties are often defined differently). It may refer to a building, a building cluster, or a floor of a multistory building.

buildingName	A string. allows for buildings that have well-known names.
href	A string. Link to the subAddress.
id	A string. Unique Identifier of the subAddress.
levelNumber	A string. used where a level type may be repeated e.g. BASEMENT 1, BASEMENT 2.
levelType	A string. describes level types within a building.
name	A string. Name of the subAddress to identify it with a meaningful identification.
privateStreetName	A string. private streets internal to a property (e.g. a university) may have internal names that are not recorded by the land title office.
privateStreetNumber	A string. private streets numbers internal to a private street.
subAddressType	A string. Type of subAddress : it can be a subunit or a private street.
subUnitNumber	A string. the discriminator used for the subunit often just a simple number e.g. FLAT 5, may also be a range.
subUnitType	A string. the type of subunit e.g.BERTH, FLAT, PIER, SUITE, SHOP, TOWER, UNIT, WHARF.

IndividualIdentification sub-resource

Represents our registration of information used as proof of identity by an individual (passport, national identity card, drivers license, social security number, birth certificate).

attachment	An attachment ref or value (AttachmentRefOrValue). An attachment by value or by reference. An attachment complements the description of an element, for example through a document, a video, a picture.
identificationId	A string. Identifier.

identificationType A string. Identification type (passport, national identity card, drivers license, social security number, birth certificate).

issuingAuthority A string. Authority which has issued the identifier, such as: social security, town hall.

issuingDate A date time (DateTime). Date at which the identifier was issued.

validFor A time period. The period for which the identification information is valid.

Quantity sub-resource

An amount in a given unit.

amount A float. Numeric value in a given unit.

units A string. Unit.

UserAsset sub-resource

assetType A string. Second level to define the type of managed element for product/service/resource managed entities (e.g.: mobile line subscription, video platform license, mobile equipment, etc). Allows identifying the specific asset within the server referenced. Supported values are implementation and application specific. Other values can be added if those listed are not enough.

entitlement A list of entitlements (Entitlement [*]). information about individual entitlements to define access levels to operate over different functions that can be defined in an asset.

entityType A string. Type of managed entity (e.g.: product, resource, service, customer, account).

id A string. Unique identifier of referenced entity within the entity/asset pair (customerId, accountId, mobile line number, ...).

role A string. Represents the part played by an individual in relation to being granted a set of entitlements for manageable assets (e.g.: owner, user, viewer, ...).

Json representation sample

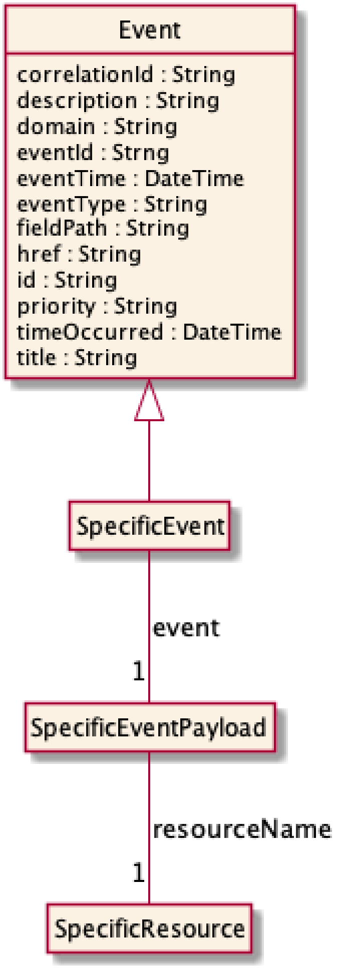
We provide below the json representation of an example of a 'Userinfo' resource object

```
{
  "address": {
    "id": "1a2b3c",
    "href": "https://host:port/location/geographicAddress/1a2b3c",
    "streetNr": "1",
    "streetName": "UnterDenLinden",
    "city": "Berlin",
    "country": "Germany",
    "postcode": "10117",
    "@type": "GeographicAddress",
    "geographicLocation": {
      "id": "afuih78g"
    }
  },
  "birthdate": "1970-11-02",
  "email": "jane.doe@email.com",
  "email_verified": true,
  "family_name": "Doe",
  "gender": "female",
  "given_name": "Jane",
  "legalId": [
    {
      "identificationType": "passport",
      "identificationId": "51DD1234",
      "issuingAuthority": "US Government",
      "issuingDate": "2017-10-22T07:49:25.246Z",
      "validFor": {
        "startDateTime": "2017-10-22T07:49:25.246Z",
        "endDateTime": "2027-10-21T07:49:25.246Z"
      },
      "attachment": [
        {
          "attachmentType": "passportCopy",
          "isRef": false,
          "name": "PassportCopy321.pdf",
          "description": "Scanned copy of the passport",
          "mimeType": "application/pdf",
          "url": "http://DocumentManager/321/PassportCopy321.pdf"
        }
      ]
    }
  ],
  "locale": "en",
  "middle_name": "Mary",
  "name": "Jane Mary Doe",
  "nickname": "JaneDoe",
  "phone_number": "+1 (425) 555-1212",
  "phone_number_verified": true,
  "picture": "https://some.url.com/janeDoe.jpg",
  "preferred_username": "janeDoe",
  "profile": "https://my.blog.com/janeDoe",
  "sub": "a066ffd5-f685-43bc-ad57-bfb7639decb0",
  "userAssets": [
    {
      "id": "2289c5f7-7e14-41a5-a71d-5ba811618ad0",
      "assetType": "landline",
      "entityType": "service",
      "role": "authorizedUser",
      "entitlement": [
        {
          "action": "string",
          "function": "string"
        }
      ],
      "href": "https://host:port/userInfo/userAssets/2289c5f7-7e14-41a5-a71d-5ba811618ad0",
      "@schemaLocation": "https://mycsp.com:8080/tmf-api/schema/Common/UserAsser.schema.json",
      "@type": "UserAsset"
    }
  ],
  "website": "https://janedoe.com",
  "zoneinfo": "America/Los_Angeles",
  "id": "a066ffd5-f685-43bc-ad57-bfb7639decb0",
  "href": "https://host:port/userInfo/a066ffd5-f685-43bc-ad57-bfb7639decb0",
  "@schemaLocation": "https://mycsp.com:8080/tmf-api/schema/Common/UserInfo.schema.json",
  "@type": "UserInfo"
}
```

Notification Resource Models

0 notifications are defined for this API

The notification structure for all notifications in this API follow the pattern depicted by the figure below. A notification event resource (depicted by "SpecificEvent" placeholder) is a sub class of a generic Event structure containing at least an id of the event occurrence (eventId), an event timestamp (eventTime), and the name of the resource (eventType).
This notification structure owns an event payload structure ("SpecificEventPayload" placeholder) linked to the resource concerned by the notification using the resource name as access field ("resourceName" placeholder).


Event
correlationId : String
description : String
domain : String
eventId : Strng
eventTime : DateTime
eventType : String
fieldPath : String
href : String
id : String
priority : String
timeOccurred : DateTime
title : String
SpecificEvent
event
1
SpecificEventPayload
resourceName
1
SpecificResource

API OPERATIONS

Remember the following Uniform Contract:

Operation on Entities	Uniform API Operation	Description
Query Entities	GET Resource	GET must be used to retrieve a representation of a resource.
Create Entity	POST Resource	POST must be used to create a new resource
Partial Update of an Entity	PATCH Resource	PATCH must be used to partially update a resource
Complete Update of an Entity	PUT Resource	PUT must be used to completely update a resource identified by its resource URI
Remove an Entity	DELETE Resource	DELETE must be used to remove a resource
Execute an Action on an Entity	POST on TASK Resource	POST must be used to execute Task Resources
Other Request Methods	POST on TASK Resource	GET and POST must not be used to tunnel other request methods.

Filtering and attribute selection rules are described in the TMF REST Design Guidelines.

Notifications are also described in a subsequent section.

Operations on Userinfo

List userinfos

GET /userinfo?fields=...&{filtering}

Description

This operation list userinfo entities.
Attribute selection is enabled for all first level attributes.
Filtering may be available depending on the compliance level supported by an implementation.

Usage Samples

This example details how userinfo is retrieved for a user. In this example a valid Authorization token must be present in the header

Request

```
GET /tmf-api/openid/v4/userinfo
Accept: application/json
```

Response

```
200

{
  "address": {
    "id": "1a2b3c",
    "href": "https://host:port/location/geographicAddress/1a2b3c",
    "streetNr": "1",
    "streetName": "UnterDenLinden",
    "city": "Berlin",
    "country": "Germany",
    "postcode": "10117",
    "@type": "GeographicAddress",
    "geographicLocation": {
      "id": "afuih78g"
    }
  },
  "birthdate": "1970-11-02",
  "email": "jane.doe@email.com",
  "email_verified": true,
  "family_name": "Doe",
  "gender": "female",
  "given_name": "Jane",
  "legalId": [
    {
      "identificationType": "passport",
      "identificationId": "51DD1234",
      "issuingAuthority": "US Government",
      "issuingDate": "2017-10-22T07:49:25.246Z",
      "validFor": {
        "startDateTime": "2017-10-22T07:49:25.246Z",
        "endDateTime": "2027-10-21T07:49:25.246Z"
      },
      "attachment": [
        {
          "attachmentType": "passportCopy",
          "isRef": false,
          "name": "PassportCopy321.pdf",
          "description": "Scanned copy of the passport",
          "mimeType": "application/pdf",
          "url": "http://DocumentManager/321/PassportCopy321.pdf"
        }
      ]
    }
  ],
  "locale": "en",
  "middle_name": "Mary",
  "name": "Jane Mary Doe",
  "nickname": "JaneDoe",
  "phone_number": "+1 (425) 555-1212",
  "phone_number_verified": true,
  "picture": "https://some.url.com/janeDoe.jpg",
  "preferred_username": "janeDoe",
  "profile": "https://my.blog.com/janeDoe",
  "sub": "a066ffd5-f685-43bc-ad57-bfb7639decb0",
  "userAssets": [
    {
      "id": "2289c5f7-7e14-41a5-a71d-5ba811618ad0",
      "assetType": "landline",
      "entityType": "service",
      "role": "authorizedUser",
      "entitlement": [
        {
          "action": "string",
          "function": "string"
        }
      ],
      "@baseType": "UserAsset",
      "href": "https://host:port/userInfo/userAssets/2289c5f7-7e14-41a5-a71d-5ba811618ad0",
      "@schemaLocation": "https://mycsp.com:8080/tmf-api/schema/Common/UserAsser.schema.json",
      "@type": "UserAsset"
    }
  ],
  "website": "https://janedoe.com",
  "zoneinfo": "America/Los_Angeles",
  "id": "a066ffd5-f685-43bc-ad57-bfb7639decb0",
  "href": "https://host:port/userInfo/a066ffd5-f685-43bc-ad57-bfb7639decb0",
  "@schemaLocation": "https://mycsp.com:8080/tmf-api/schema/Common/UserInfo.schema.json",
  "@type": "UserInfo"
}
```

Retrieve userinfo

GET /userinfo/{id}?fields=...&{filtering}

Description

This operation retrieves an userinfo entity.
Attribute selection is enabled for all first level attributes.
Filtering on sub-resources may be available depending on the compliance level supported by an implementation.

Usage Samples

The Userinfo entity is not a list and therefore there is no operation to retrive userinfo by ID. Userinfo is retrieved for the user specified in the header token.

Request

```
GET /tmf-api/openid/v4/userinfo/42
Accept: application/json
```

Response

```
200

{
  "address": {
    "id": "1a2b3c",
    "href": "https://host:port/location/geographicAddress/1a2b3c",
    "streetNr": "1",
    "streetName": "UnterDenLinden",
    "city": "Berlin",
    "country": "Germany",
    "postcode": "10117",
    "@type": "GeographicAddress",
    "geographicLocation": {
      "id": "afuih78g"
    }
  },
  "birthdate": "1970-11-02",
  "email": "jane.doe@email.com",
  "email_verified": true,
  "family_name": "Doe",
  "gender": "female",
  "given_name": "Jane",
  "legalId": [
    {
      "identificationType": "passport",
      "identificationId": "51DD1234",
      "issuingAuthority": "US Government",
      "issuingDate": "2017-10-22T07:49:25.246Z",
      "validFor": {
        "startDateTime": "2017-10-22T07:49:25.246Z",
        "endDateTime": "2027-10-21T07:49:25.246Z"
      },
      "attachment": [
        {
          "attachmentType": "passportCopy",
          "isRef": false,
          "name": "PassportCopy321.pdf",
          "description": "Scanned copy of the passport",
          "mimeType": "application/pdf",
          "url": "http://DocumentManager/321/PassportCopy321.pdf"
        }
      ]
    }
  ],
  "locale": "en",
  "middle_name": "Mary",
  "name": "Jane Mary Doe",
  "nickname": "JaneDoe",
  "phone_number": "+1 (425) 555-1212",
  "phone_number_verified": true,
  "picture": "https://some.url.com/janeDoe.jpg",
  "preferred_username": "janeDoe",
  "profile": "https://my.blog.com/janeDoe",
  "sub": "a066ffd5-f685-43bc-ad57-bfb7639decb0",
  "userAssets": [
    {
      "id": "2289c5f7-7e14-41a5-a71d-5ba811618ad0",
      "assetType": "landline",
      "entityType": "service",
      "role": "authorizedUser",
      "entitlement": [
        {
          "action": "string",
          "function": "string"
        }
      ],
      "@baseType": "UserAsset",
      "href": "https://host:port/userInfo/userAssets/2289c5f7-7e14-41a5-a71d-5ba811618ad0",
      "@schemaLocation": "https://mycsp.com:8080/tmf-api/schema/Common/UserAsser.schema.json",
      "@type": "UserAsset"
    }
  ],
  "website": "https://janedoe.com",
  "zoneinfo": "America/Los_Angeles",
  "id": "a066ffd5-f685-43bc-ad57-bfb7639decb0",
  "href": "https://host:port/userInfo/a066ffd5-f685-43bc-ad57-bfb7639decb0",
  "@schemaLocation": "https://mycsp.com:8080/tmf-api/schema/Common/UserInfo.schema.json",
  "@type": "UserInfo"
}
```

Acknowledgements

Version History

Version Number	Date	Release led by:	Description
1.01	03-Jul-2018	Luis Velarde (Telefónica)	First Release of Draft Version of the Document.
1.0.2	29-Jun-2018	Adrienne Walcott	Formatting/style edits prior to R18 publishing.
1.0.3	10-Sep-2018	Adrienne Walcott	Updated to reflect TM Forum Approved Status
4.0.0	28-May-2020	Alan Pope	Alignment with Guidelines 4.0

Release History

Release Number	Date	Release led by:	Description
18.0.0	03-Jul-2018	Luis Velarde (Telefónica)	Initial Release
18.0.1	10-Sep-2018	Adrienne Walcott	Updated to reflect TM Forum Approved Status
Pre-production	28-May-2020	Alan Pope	Alignment with Guidelines 4.0