

scim
Internet-Draft
Intended status: Standards Track
Expires: June 21, 2015

B. Greevenbosch
R. Sun
Huawei Technologies
December 18, 2014

SCIM and vCard mapping
draft-greevenbosch-scim-vcard-mapping-04

Abstract

This document defines a mapping between SCIM and vCard.

Note

Discussion and suggestions for improvement are requested, and should be sent to scim@ietf.org.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 21, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	4
2. Requirements notation	5
3. Mapping from SCIM to vCard	6
3.1. Mapping of SCIM attributes to vCard properties	6
3.2. Mapping of SCIM attributes to vCard parameters	13
4. Mapping from vCard properties to SCIM attributes	15
4.1. Mapping of vCard properties	15
4.2. Mapping of vCard parameters	20
5. Mapping between SCIM and vCard IDs	22
6. Differences between vCard and SCIM	23
7. Examples	24
7.1. Mapping from SCIM to vCard	24
7.2. Mapping from vCard to SCIM	28
8. Open issues	31
9. IANA Considerations	32
10. Security Considerations	33
11. Acknowledgements	34
12. References	35
12.1. Normative References	35
12.2. Informative References	35
Authors' Addresses	36

1. Introduction

The SCIM core schema [I-D.ietf-scim-core-schema] defines a platform neutral data and extension model for representing users of cloud services. SCIM core also defines XML and JSON serialisations of the abstract schema.

This document defines a mapping between SCIM and vCard [RFC6350]. The mapping may serve several purposes:

- o To provide a unified conversion mechanism between SCIM and vCard.
- o To identify properties that are defined in vCard, but are missing in SCIM.
- o To identify SCIM attributes that may be useful in vCard too.

2. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Mapping from SCIM to vCard

When mapping SCIM attributes to vCard, they may either become mapped to vCard properties or to vCard attributes associated with vCard properties. Section 3.1 defines the mappings to the vCard properties, whereas Section 3.2 defines mappings to vCard attributes.

In addition, in accordance to [RFC6350], the vCard representation MUST include the mandatory fields:

- o VERSION
- o FN

3.1. Mapping of SCIM attributes to vCard properties

Table 1 describes a mapping from SCIM attributes to the vCard properties.

In the table, the cardinality of the SCIM attribute is prefixed by an "S", whereas the cardinality of the vCard property is prefixed by a "v". The further notation has been adopted from [RFC6350] as follows:

1	Exactly one instance MUST be present.
*1	Exactly one instance MAY be present.
1*	One or more instances MUST be present.
*	One or more instances MAY be present.

SCIM fields that have no vCard equivalent MUST be omitted in the vCard result.

The reverse mapping from vCard to SCIM is defined in Section 4. The reason for having two tables is that some mappings are not invertible.

SCIM attribute	vCard property	Cardinality	Notes
active		S*1	

addresses	ADR	S* v*	See [RFC6350] for the internal coding of the ADR property.
addresses/country	ADR (country)	S* v*	Combined with other address attributes into a single ADR element.
addresses/formatted	ADR (LABEL)	S* v*	
addresses/locality	ADR (locality)	S* v*	Combined with other address attributes into a single ADR element.
addresses/postalCode	ADR (postal code)	S* v*	Combined with other address attributes into a single ADR element.
addresses/region	ADR (region)	S* v*	Combined with other address attributes into a single ADR element.

addresses/streetAddress	ADR (street address)	S* v*	Combined with other address attributes into a single ADR element.
costCenter		S*1	
department	ORG	S*1 v*	Use the hierarchical order defined in vCard.
displayName		S*1	
division	ORG	S*1 v*	Use the hierarchical order defined in vCard.
emails	EMAIL	S* v*	See Table 2 for the conversion of a possible "type" attribute.
employeeNumber		S*1	
entitlements		S*	Hard to map as it is proprietary by nature.
externalId		S*1	
groups/value		S*	ID of the group
groups/\$ref		S*	URI of the group

id	UID	S1 v*1	See Section 5 for conversion from SCIM id space to vCard UID space.
ims	IMPP	S* v*	
locale		S*1	
manager/displayName		S*1	This field is optional in SCIM, also when "manager" is included.
manager/id		S*1	SCIM specific ID, related to "id" attribute. The vCard RELATED property could be used, but a TYPE "manager" may need definition. In SCIM, "managerID" is mandatory if "manager" is included.
manager/\$ref		S*1	The URI of the SCIM resource representing the User's manager.

members/value	MEMBER	S* v*	Contains the IDs of the SCIM resources associated with the members of the group.
members/\$ref	MEMBER	S* v*	Contains the URIs of the SCIM resources associated with the members of the group.
meta/created	REV	S*1	No direct vCard equivalent. Candidates could be SOURCE and ORG-DIRECTOR Y.
meta/lastModified		S*1 v*1	
meta/location		S*1	
meta/resourceType		S*1	
meta/version	N (family names)	S*1	Combined with other name attributes in a single N element.
name/familyName		S*1 v*1	
name/formatted		S*1 v1*	

name/givenName	N (given names)	S*1 v*1	Combined with other name attributes in a single N element.
name/honorificPrefix	N (honorific prefixes)	S*1 v*1	Combined with other name attributes in a single N element.
name/honorificSuffix	N (honorific suffixes)	S*1 v*1	Combined with other name attributes in a single N element.
name/middleName	N (additional names)	S*1 v*1	
nickName	NICKNAME	S*1 v*	
organization	ORG	S*1 v*	Use the hierarchical order defined in vCard.
password		S*1	
phoneNumbers (no type)	TEL (no TYPE)	S* v*	
phoneNumbers (type="fax")	TEL (TYPE="fax")	S* v*	
phoneNumbers (type="home")	TEL (TYPE="voice,home")	S* v*	
phoneNumbers (type="mobile")	TEL (TYPE="voice,cell")	S* v*	

phoneNumbers (type="other")	TEL (no TYPE)	S* v*	
phoneNumbers (type="pager")	TEL (TYPE="pager")	S* v*	
phoneNumbers (type="work")	TEL (TYPE="voice,work")	S* v*	
photos	PHOTO	S* v*	URL of a web location where the photo can be retrieved.
preferredLanguage	LANG	S*1 v*	Language tag according to [RFC5646].
profileUrl	URL	S*1 v*	Multiple fields in SCIM better?
roles	ROLE	S* v*	Consider distinction with the "userType" attribute.
timezone	TZ	S*1 v*	
title	TITLE	S*1 v*	
userName		S1	
userType	ROLE	S*1 v*	Consider distinction with the "roles" attribute.
x509Certificates	KEY	S* v*	Care is required: keys may not have the same usage.

Table 1: SCIM to vCard mapping

3.2. Mapping of SCIM attributes to vCard parameters

In addition to SCIM properties, SCIM attributes may also need to be converted to vCard parameters. Table 2 contains the related mappings.

SCIM attribute	SCIM value	vCard parameter	vCard value	Notes
primary	true	PREF	1	
primary	false			Omitted in vCard.
type	aim	TYPE	x-aim	Only for "ims"
type	fax	TYPE	fax	May be combined with other types in vCard
type	gtalk	TYPE	x-gtalk	Only for "ims"
type	home	TYPE	home	May be combined with other types in vCard
type	icq	TYPE	x-icq	Only for "ims"
type	mobile	TYPE	cell	May be combined with other types in vCard
type	msn	TYPE	x-msn	Only for "ims"
type	other			Omitted in vCard
type	pager	TYPE	pager	May be combined with other types in vCard
type	photo			Only for "photo", vCard parameter can be omitted.
type	qq	TYPE	x-qq	Only for "ims"

type	skype	TYPE	x-skype	Only for "ims"
type	work	TYPE	work	May be combined with other types in vCard
type	xmpp	TYPE	x-xmpp	Only for "ims"
type	yahoo	TYPE	x-yahoo	Only for "ims"
type	yahoo	TYPE	x-thumbnail	Only for "thumbnail"

Table 2: Mapping of SCIM attributes to vCard parameters

4. Mapping from vCard properties to SCIM attributes

4.1. Mapping of vCard properties

Table 3 describes a mapping from vCard properties to SCIM attributes. For the cardinalities, the same notation from Section 3 is used.

Notice that the attributes "uid" and "userName" are mandatory in a SCIM representation, whereas they may not be available in the vCard. It is left to the application to generate sensible values for these fields.

vCard property	SCIM attribute	Cardinalit yin vCard/SCI M	Notes
ANNIVERSARY		v*1	
ADR (country)	addresses/country	v* S*	
ADR (extended address)		v*	
ADR (LABEL)	addresses/formatted	v* S*	
ADR (locality)	addresses/locality	v* S*	
ADR (post office box)	addresses/streetAddress	v* S*	
ADR (postal code)	addresses/postalCode	v* S*	
ADR (region)	addresses/region	v* S*	
ADR (street address)	addresses/streetAddress	v* S*	
BDAY		v*1	
BIRTHPLACE		v*1	Defined in [RFC6474].

CALADRURI		v*	Purpose: to specify the calendar user address to which a scheduling request should be sent for the object represented by the vCard.
CALURI		v*	Purpose: to specify the URI for a calendar associated with the object represented by the vCard.
CATEGORIES		v*	Contains not necessarily unified tags.
CLIENTPIDMAP		v*	Link between local PID and global URI.
DEATHDATE		v*1	Defined in [RFC6474].
DEATHPLACE		v*1	Defined in [RFC6474].
EMAIL	emails	v* S*	Can have TYPE="work", TYPE="home".
EXPERTISE		v*	Defined in [RFC6715].

FBURL		v*	Purpose: to specify the URI for the busy time associated with the object that the vCard represents.
FN	names/formatted	v1* S*1	
GENDER		v*1	Can have the values "M"ale, "F"emale, "O"ther, "N"one or not applicable or "U"nknown.
GEO		v*	GPS coordinates
HOBBY		v*	Defined in [RFC6715].
IMPP	ims	v* S*	
INTEREST		v*	Defined in [RFC6715].
KEY	x509Certificates?	v* S*	Care is required: keys may not have the same usage.

KIND		v*1	In vCard can have the values "individual", "group", "org" and "location". The value "application" was added by [RFC6473].
LANG	preferredLanguage	v* S*1	
LOGO		v*	
MEMBER	members/id	v* S*	Contains a vCard ID of a member of this group. The vCard MUST have KIND="group". ID must be converted.
N (additional names)	names/middleName	v*1 S*1	
N (family names)	names/familyName	v*1 S*1	
N (given names)	names/givenName	v*1 S*1	
N (honorific prefixes)	names/honorificPrefix	v*1 S*1	
N (honorific suffixes)	names/honorificSuffix	v*1 S*1	
NICKNAME	nickName	v* S*1	
NOTE		v*	Any text.
ORG	organization	v* S*1	
ORG-DIRECTORY		v*	Defined in [RFC6715].

PHOTO	photos	v* S*	URL of a web location where the photo can be retrieved.
PRODID		v*1	ID for producer of vCard.
RELATED		v*	Contains a vCard ID of another related vCard. Can have many TYPE values, such as "friend", "neighbor" and "spouse".
REV		v*1	Purpose: to specify revision information about the current vCard.
ROLE	roles	v* S*1	
SOUND		v*	
SOURCE		v*	Similar to SCIM meta/location.
TEL (TYPE="textphone")	phoneNumbers, type="other"	v* S*	See Table 4 for related type mapping.
TITLE	title	v* S*1	
TZ	timezone	v* S*1	

UID	externalId	v*1 S*1	See Section 5 for conversion from vCard UID space to SCIM id space.
URL	profileUrl	v* S*1	
VERSION		v1	Version of vCard specification.
XML		v*	Purpose: to include extended XML-encoded vCard data in a plain vCard.

Table 3: vCard to SCIM mapping

4.2. Mapping of vCard parameters

Table 4 describes how vCard parameters are mapped to SCIM.

vCard parameter	vCard parameter value	SCIM representation	Notes
TYPE	cell	"type": "mobile"	
TYPE	fax	"type": "fax"	
TYPE	pager	"type": "pager"	
TYPE	text	"type": "other"	
TYPE	textphone	"type": "other"	
TYPE	video	"type": "video"	
TYPE	voice		Omitted in SCIM

Table 4: Mapping of vCard parameters

5. Mapping between SCIM and vCard IDs

A SCIM specific prefix could be used to indicate the conversion from SCIM IDs to vCard UIDs. A "Service Provider" specific part would need to be included in the vCard UID, as the SCIM ID is unique within the Service Provider's space only. The following format is proposed:

```
UID:scim:[serviceProviderID]:123456789
```

Conversion from vCard to SCIM may be done similarly, i.e. by adding a prefix to the vCard UID. The SCIM schema document mentions for the SCIM ID: "This identifier MUST be unique across the Service Provider's entire set of Resources", so as long as the vCard UID indeed is globally unique, and the service provider uses the prefix for vCard acquired resources only, the rule should hold.

Notice that the above mechanism allows looping. For example, converting SCIM -> vCard -> SCIM would lead to another SCIM ID in the second representation as in the first. This indeed reflects the possible loss of information in the conversion process. It is RECOMMENDED to avoid this kind of chained conversion.

Because of the format of the vCard UID after conversion from SCIM, the SCIM service provider can detect above mentioned chained conversion, as well as the original vCard ID. The actions the service provider may take upon such detection may for example include using the original SCIM data instead, or using smarter mapping by analysing the original and the new import. This kind of mechanisms is left out of scope of this document.

6. Differences between vCard and SCIM

This section contains a non-exhaustive list of differences between vCard and SCIM.

- o In vCard, a group property can be established. This property contains the IDs of its members. In SCIM however, the group/membership relation can be signalled in two directions: just like vCard the group object can signal its members through the "members" attribute, but the member objects can also point to the groups they are part of, through the "groups" attribute.
- o In SCIM, relations between objects can be established either through their IDs or through their URIs. vCard only uses IDs to signal relationships between entities.

7. Examples

7.1. Mapping from SCIM to vCard

Figure 2 contains the result after converting the SCIM data from Figure 1 to vCard.

Notice that the following fields have been omitted during conversion:

- o userName
- o locale
- o active
- o password
- o groups
- o meta fields except for "lastModified"

```
{
  "schemas": ["urn:scim:schemas:core:2.0:User"],
  "id": "2819c223-7f76-453a-919d-413861904646",
  "externalId": "701984",
  "userName": "bjensen@example.com",
  "name": {
    "formatted": "Ms. Barbara J Jensen III",
    "familyName": "Jensen",
    "givenName": "Barbara",
    "middleName": "Jane",
    "honorificPrefix": "Ms.",
    "honorificSuffix": "III"
  },
  "displayName": "Babs Jensen",
  "nickName": "Babs",
  "profileUrl": "https://login.example.com/bjensen",
  "emails": [
    {
      "value": "bjensen@example.com",
      "type": "work",
      "primary": true
    },
    {
      "value": "babs@jensen.org",
      "type": "home"
    }
  ]
}
```



```
],
"addresses": [
  {
    "type": "work",
    "streetAddress": "100 Universal City Plaza",
    "locality": "Hollywood",
    "region": "CA",
    "postalCode": "91608",
    "country": "USA",
    "formatted": "100 Universal City Plaza\nHollywood, CA 91608 USA",
    "primary": true
  },
  {
    "type": "home",
    "streetAddress": "456 Hollywood Blvd",
    "locality": "Hollywood",
    "region": "CA",
    "postalCode": "91608",
    "country": "USA",
    "formatted": "456 Hollywood Blvd\nHollywood, CA 91608 USA"
  }
],
"phoneNumbers": [
  {
    "value": "555-555-5555",
    "type": "work"
  },
  {
    "value": "555-555-4444",
    "type": "mobile"
  }
],
"ims": [
  {
    "value": "someaimhandle",
    "type": "aim"
  }
],
"photos": [
  {
    "value": "https://photos.example.com/profilephoto/7293000000Ccne/F",
    "type": "photo"
  },
  {
    "value": "https://photos.example.com/profilephoto/7293000000Ccne/T",
    "type": "thumbnail"
  }
],
```

```

    "userType": "Employee",
    "title": "Tour Guide",
    "preferredLanguage": "en_US",
    "locale": "en_US",
    "timezone": "America/Los_Angeles",
    "active": true,
    "password": "tlmeMa$heen",
    "groups": [
      {
        "value": "e9e30dba-f08f-4109-8486-d5c6a331660a",
        "$ref": "https://example.com/v1/Groups/e9e30dba-f08f-4109-8486-d5c6a3316
60a",
        "display": "Tour Guides"
      },
      {
        "value": "fc348aa8-3835-40eb-a20b-c726e15c55b5",
        "$ref": "https://example.com/v1/Groups/fc348aa8-3835-40eb-a20b-c726e15c5
5b5",
        "display": "Employees"
      },
      {
        "value": "71ddacd2-a8e7-49b8-a5db-ae50d0a5bfd7",
        "$ref": "https://example.com/v1/Groups/71ddacd2-a8e7-49b8-a5db-ae50d0a5b
fd7",
        "display": "US Employees"
      }
    ],
    "x509Certificates": [
      {
        "value":
        "MIIDQzCCAqygAwIBAgICEAAwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
        EzARBgNVBAGMCKNhbgGmb3JuaWEeXFDASBgNVBAoMC2V4YW1wbGUuY29tMRQwEgYD
        VQQDDAtleGFtcGxlLmNvbTAeFw0xMTEwMjI0MzFaFw0xMjEwMDQwNjI0MzFa
        MH8xCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRQwEgYDVQQKDAU1
        eGFtcGxlLmNvbTEhMB8GA1UEAwwYTXMuIEJhcmJhcmEgSiBKZW5zZW4gSULJMSIw
        IAYJKoZIhvcNAQkBFhNiamVuc2VuQGV4YW1wbGUuY29tMIIIBIjANBgkqhkiG9w0B
        AQEFAAOCAQ8AMIIBCgKCAQEAA7Kr+Dcds/JQ5GwejJfcbIP682X3xpjis56AK02bc
        1FLgzdLI8auoR+cC9/Vrh5t66HkQIOdA4unHh0AaZ4xL5PhVbXIPMB5vAPKpzz5i
        PSi8x08SL7I7SDhcBVJhqVqr3HgllEG6UClddHO7nkLuwXq8HcISKkbT5WFTVfFZ
        zidPl8HZ7DhXkZIRtJwBweq4bvm3hM1Os7UQH05ZS6cVDgweKNwdLLrT5likSQG3
        DYrl+ft781UQRIqxgwgCfXEuDiinPh0kkvIi5jivVulZ9QiwlyEdRbLJ4zJQBmDr
        SGTMYn4lRc2HgHO4DqB/bnMVorHB0CC6AV1QoFK4GPe1LwIDAQABo3sweTAJBgNV
        HRMEAjaAMCwGCWCGSAGG+EIBDQQFfhlPcGVuU1NMIEdlbmVyYXRlZCBZDZlZC0aWZp
        Y2F0ZTAdBgNVHQ4EFgQU8pD0U0vsZIsaA16lL8En8bx0F/gwHwYDVR0jBBGwFoAU
        dGeKitcaF7gnzsNwDx708kqaVt0wDQYJKoZIhvcNAQEFBQADgYEAA81SsFnOdYJt
        Ng5Tcq+/ByEDrBgnusx0jloUhByPMEVkoMZ3J7j1ZgI8rAbOkNngX8+pKfTiDz1R
        C4+dx8oU6Za+4NJXUjll5CvV6BEYb1+QAEJwittTVvxB/A67g42/vzgAtoRUeDovl
        +GFibZ+GNF/cAYKcMtGcrs2i97ZkJMo="
      }
    ],
    "meta": {

```

```

    "resourceType": "User",
    "created": "2010-01-23T04:56:22Z",
    "lastModified": "2011-05-13T04:42:34Z",
    "version": "W\\/\\"a330bc54f0671c9\\\"",
    "location": "https://example.com/v1/Users/2819c223-7f76-453a-919d-41386190
4646"
  }
}

```

Figure 1: Original SCIM data

```

BEGIN:VCARD
VERSION:4.0
UID:"scim:provider.example.org:2819c223-7f76-453a-919d-413861904646"
FN:Ms. Barbara J Jensen III
N:Jensen;Barbera;Jane;Ms.;III
NICKNAME:Babs
URL:"https://login.example.com/bjensen"
EMAIL;TYPE=work;PREF=1:bjensen@example.com
EMAIL;TYPE=home:babs@jensen.org
ADR;LABEL="100 Universal City Plaza\nHollywood, CA 91608 USA";TYPE=work
:;;100 Universal City Plaza;Hollywood;CA;91608;USA
ADR;LABEL="456 Hollywood Blvd\nHollywood, CA 91608 USA";type=home:;;456
Hollywood Blvd;Hollywood;CA;91608;USA
TEL;TYPE=voice,work:555-555-5555
TEL;TYPE=cell:555-555-4444
IMPP;TYPE=x-aim:someaimhandle
PHOTO:"https://photos.example.com/profilephoto/7293000000Ccne/F"
PHOTO;TYPE=x-thumbnail:"https://photos.example.com/profilephoto/7293000
0000Ccne/T"
ROLE:Employee
TITLE:Tour Guide
LANG:en-US
TZ:America/Los_Angeles
KEY:...MIIDQzCCAqygAwIBAgICEAAwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
EzARBgNVBAGMCkNhbgGlb3JuaWExFDASBgNVBAoMC2V4YW1wbGUuY29tMRQwEgYD
VQQDDAtleGFtcGxlLmNvbTAeFw0xMTEwMjI0MzFaFw0xMjEwMDQwNjI0MzFa
MH8xCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRQwEgYDVQQKDAU1
eGFtcGxlLmNvbTEhMB8GA1UEAwYTXMuIEJhcmJhcmEgSiBkZW5zZW4gSULJMSIw
IAYJKoZIhvcNAQkBFhNiamVuc2VuQGV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAA7Kr+Dcds/JQ5GweJjFfCBIP682X3xpjis56AK02bc
1FLgzdLI8auoR+cC9/Vrh5t66HkQIOdA4unHh0AaZ4xL5PhVbXIPMB5vAPKpzz5i
PSi8x08SL7I7SDhcBVJhqVqr3Hgl1EG6UC1DdH07nkLuwXq8HcISKkbT5WFTVfFZ
zidPl8HZ7DhXkZIRtJwBweq4bvm3hM1Os7UQH05ZS6cVDgweKNwdLLrT51ikSQG3
DYrl+ft781UQRIqxgwqCfXEuDiinPh0kkvIi5jivVulZ9QiwlyEdRbLJ4zJQBmDr
SGTMYn4lRc2HgHO4DqB/bnMVorHB0CC6AV1QoFK4GPelLwIDAQABO3sweTAJBgNV
MIIDQzCCAqygAwIBAgICEAAwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
EzARBgNVBAGMCkNhbgGlb3JuaWExFDASBgNVBAoMC2V4YW1wbGUuY29tMRQwEgYD

```

```

VQQDDAtleGFtcGx1LmNvbTAeFw0xMTEwMjIwNjI0MzFaFw0xMjEwMDQwNjI0MzFa
MH8xCzAJBgNVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRQwEgYDVQQKDatl
eGFtcGx1LmNvbTEhMB8GA1UEAwYTXMuIEJhcmJhcmEgSiBKZW5zZW4gSULJMSIw
IAYJKoZIhvcNAQkBFhNiamVuc2VuQGv4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEA7Kr+Dcds/JQ5GwejJFcBIP682X3xpjis56AK02bc
lFLgzdLI8auoR+cC9/Vrh5t66HkQIOdA4unHh0AaZ4xL5PhVbXIPMB5vAPKpzz5i
PSi8x08SL7I7SDhcBVJhqVqr3Hgl1EG6UC1DdH07nkLuwXq8HcISKkbT5WFTVfFZ
zidPl8HZ7DhXkZIRtJwBweq4bvm3hM10s7UQH05ZS6cVDgweKNwdLLrT51likSQG3
DYrl+ft781UQRIqxgwqCfXEuDiinPh0kkvIi5jivVu1Z9QiwlyEdRbLJ4zJQBmDr
SGTMYn4lRc2HgHO4DqB/bnMVorHB0CC6AV1QoFK4GPelLwIDAQABo3sweTAJBgNV
HRMEAjAAMCwGCWCGSAGG+EIBDQqFh1PcGVuU1NMIEdlbmVyYXRlZCBZDZXJ0aWZp
Y2F0ZTAdBgNVHQ4EFgQU8pD0U0vsZIsaA16lL8En8bx0F/gwHwYDVR0jBBgwFoAU
dGeKitcaF7gnzsNwDx708kqaVt0wDQYJKoZIhvcNAQEFBQADgYEA81SsFnOdYJt
Ng5Tcq+/ByEDrBgnusx0jloUhByPMEVkoMZ3J7j1ZgI8rAbOkNngX8+pKfTiDz1R
C4+dx8oU6Za+4NJXUj1L5CvV6BEYb1+QAEJwittVvxB/A67g42/vzgAtoRUeDov1
+GFibZ+GNF/cAYKcMtGcrs2i97ZkJMo=
REF:"2011-05-13T04:42:34Z"
END:VCARD

```

Figure 2: After conversion to vCard

7.2. Mapping from vCard to SCIM

Figure 4 contains the result after converting the vCard data from Figure 3 to SCIM.

The following vCard attributes have been omitted in the SCIM representation:

- o GENDER
- o BDAY

The mandatory "uid" and "userName" attributes have been added to the SCIM representation, although they have not been defined in the vCard.

```
BEGIN:VCARD
VERSION:4.0
FN:Vincent van Gogh
N:van Gogh;Vincent;;;
GENDER:M
BDAY:18530330
ROLE;LANGUAGE="en":painter
LANG;PREF=1:nl
LANG;PREF=2:fr
ADR;LABEL="Vincent van Gogh\n54 Rue Lepic\n75018 Paris\nFrance";LANGUAGE="fr";TYPE=home::3th floor;54 Rue Lepic;Paris;;75018;France
TEL;TYPE="work,voice";PREF=1:+33-1-123456
TEL;TYPE="home,voice";PREF=2:+33-1-654321
EMAIL;TYPE=home:vangogh@example.com
URL;TYPE=work:"http://www.vangogh.example.com"
TZ:+0100
END:VCARD
```

Figure 3: Original SCIM data

```
{
  "schemas": ["urn:scim:schemas:core:2.0:User"],
  "id": "xyz",
  "userName": "vangogh@example.com",
  "name": {
    "formatted": "Vincent van Gogh",
    "familyName": "van Gogh",
    "givenName": "Vincent",
  },
  "roles": [
    {
      "value": "painter"
    }
  ],
  "preferredLanguage": "nl",
  "adresses": [
    {
      "type": "home",
      "streetAddress": "54 Rue Lepic",
      "locality": "Paris",
      "postalCode": "75018",
      "country": "France",
      "formatted": "Vincent van Gogh\n54 Rue Lepic\n75018 Paris\nFrance"
    }
  ],
  "phoneNumbers": [
    {
      "value": "+33-1-123456",
      "type": "work"
    },
    {
      "value": "+33-1-654321",
      "type": "home"
    }
  ],
  "emails": [
    {
      "value": "vangogh@example.com",
      "type": "home"
    }
  ],
  "timezone": "+0100"
}
```

Figure 4: Original SCIM data

8. Open issues

The following issues require further consideration:

- o It may be feasible to leave out the conversion between SCIM ids and vCard UUIDs, as they may be dependent on the particular application that is importing the information.
- o It is unclear on whether the SCIM ID can include alphanumeric characters or is restricted to numeric characters only. The examples in [I-D.ietf-scim-core-schema] seem to indicate that they consist of hexadecimal numbers, with dashes at appropriate places. If this is the case, then during the conversion from vCard UUIDs to SCIM IDs would include conversion of alphanumeric characters to hexadecimal values.
- o For SCIM fields that have no equivalent vCard attributes, vCard attributes of the form "x-..." could be defined. Alternatively, vCard attributes could be defined, and registered with IANA.
- o The "id" and "userName" fields are mandatory in SCIM. However, a vCard does not have to contain similar information. Creating a sensible value of these fields may be left to the SCIM application that is importing the vCard, or guidelines could be defined.

9. IANA Considerations

A "manager" TYPE for the RELATED vCard property may need registration.

10. Security Considerations

The mapping between vCard and SCIM may be useful for easily transferring data for one system towards another. However, it also has privacy implications. Therefore, it is important that user consensus is acquired where applicable.

For this document, some decisions were made concerning mapping between attributes and properties with similar, but not equal, semantics. This was done in a best effort manner. However one should realise that during the mapping process some accuracy from the original data may be lost.

Conversion from SCIM to vCard and subsequently back to SCIM, as well as conversion from vCard to SCIM and subsequently back to vCard SHOULD be avoided.

11. Acknowledgements

Thanks to Kepeng Li for providing feedback and suggestions. Thanks to Paul Madsen and Phil Hunt for providing similar mapping drafts [draft-scim-saml2-binding] and [I-D.hunt-scim-directory], which have served as inspiration for this document. Michael Angstadt and Dany Cauchie provided valuable review comments.

12. References

12.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC5646] Phillips, A. and M. Davis, "Tags for Identifying Languages", BCP 47, RFC 5646, September 2009.
- [RFC6350] Perreault, S., "vCard Format Specification", RFC 6350, August 2011.
- [RFC6473] Saint-Andre, P., "vCard KIND:application", RFC 6473, December 2011.
- [RFC6474] Li, K. and B. Leiba, "vCard Format Extensions: Place of Birth, Place and Date of Death", RFC 6474, December 2011.
- [RFC6715] Cauchie, D., Leiba, B., and K. Li, "vCard Format Extensions: Representing vCard Extensions Defined by the Open Mobile Alliance (OMA) Converged Address Book (CAB) Group", RFC 6715, August 2012.
- [I-D.ietf-scim-core-schema]
Hunt, P., Grizzle, K., Wahlstroem, E., and C. Mortimore,
"System for Cross-Domain Identity Management: Core
Schema", draft-ietf-scim-core-schema-14 (work in
progress), December 2014.

12.2. Informative References

- [I-D.hunt-scim-directory]
Hunt, P., "SCIM Directory Services",
draft-hunt-scim-directory-00 (work in progress),
September 2012.
- [draft-scim-saml2-binding]
Madsen, P., "SAML 2.0 Binding for SCIM",
draft-scim-saml2-binding-02 (work in progress),
April 2011.

Authors' Addresses

Bert Greevenbosch
Huawei Technologies Co., Ltd.
Huawei Industrial Base F1-8
Bantian, Longgang District
Shenzhen 518129
P.R. China

Phone: +86-755-28979133
Email: bert.greevenbosch@huawei.com

Ruinan Sun
Huawei Technologies Co., Ltd.
Huawei Industrial Base
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: sunruinan@huawei.com

SCIM WG
Internet-Draft
Intended status: Informational
Expires: February 27, 2014

P. Hunt
Oracle
B. Khasnabish
ZTE USA, Inc.
A. Nadalin
Microsoft
Z. Zeltsan
Individual
K. Li
Huawei
August 26, 2013

SCIM Use Cases
draft-zeltsan-scim-use-cases-02

Abstract

This document lists the user scenarios and use cases of System for Cross-domain Identity Management (SCIM).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 27, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
1.1. Terminology	3
2. SCIM User Scenarios	3
2.1. Background & Context	4
2.2. Model Concepts	4
2.2.1. Triggers	4
2.2.2. Actors	5
2.2.3. Modes & Flows	6
2.2.4. Bulk & Batch Operational Semantics	7
2.3. Cloud Service Provider to Cloud Service Provider Flows (CSP->CSP)	7
2.3.1. CSP->CSP - Create Identity (Push)	7
2.3.2. CSP->CSP - Update Identity (Push)	7
2.3.3. CSP->CSP - Delete Identity (Push)	7
2.3.4. CSP->CSP - SSO Trigger (Push)	8
2.3.5. CSP->CSP - SSO Trigger (Pull)	8
2.3.6. CSP->CSP - Password Reset (Push)	8
2.4. Enterprise Cloud Subscriber to Cloud Service Provider Flows(ECS->CSP)	9
2.4.1. ECS->CSP - Create Identity (Push)	9
2.4.2. ECS ->CSP - Update Identity (Push)	9
2.4.3. ECS ->CSP - Delete Identity (Push)	9
2.4.4. ECS ->CSP - SSO Pull	9
3. SCIM use cases	10
3.1. Change of the ownership of a file	10
3.2. Migration of the identities	11
3.3. Single Sign-On (SSO) Service	12
3.4. Provisioning of the user accounts for a Community of Interest (CoI)	13
3.5. Transfer of attributes to a relying party web site	14
3.6. Change notification	15
4. Security considerations	16
5. IANA considerations	16
6. Acknowledgements	16
7. References	16
7.1. Normative References	16
7.2. Informative References	16
Authors' Addresses	17

1. Introduction

This document describes the SCIM scenarios and use cases. It also provides a list of the requirements derived from the use cases. The document's objective is to help with understanding of the design and applicability of SCIM schema [I-D.ietf-scim-core-schema] and SCIM protocol [I-D.ietf-scim-api].

The following section provides the abbreviated descriptions of the scenarios and use cases.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] when they appear in ALL CAPS. These words may also appear in this document in lower case as plain English words, absent their normative meanings.

Here is a list of acronyms and abbreviations used in this document:

- o COI: Community Of Interest
- o CRM: Customer Relationship Management
- o CRUD: Create Read Update Delete
- o CSP: Cloud Service Provider
- o CSU: Cloud Service User
- o ECS: Enterprise Cloud Subscriber
- o IaaS: Infrastructure as a Service
- o JIT: Just In Time
- o PaaS: Platform as a Service
- o SaaS: Software as a Service
- o SAML: Security Assertion Markup Language
- o SCIM: System for Cross-domain Identity Management
- o SSO: Single-Sign On

2. SCIM User Scenarios

2.1. Background & Context

The System for Cross-domain Identity Management (SCIM) specification is designed to make managing user identity in cloud based applications and services easier. The specification suite seeks to build upon experience with existing schemas and deployments, placing specific emphasis on simplicity of development and integration, while applying existing authentication, authorization, and privacy models. It's intent is to reduce the cost and complexity of user management operations by providing a common user schema and extension model, as well as binding documents to provide patterns for exchanging this schema using standard protocols. In essence, make it fast, cheap, and easy to move users in to, out of, and around the cloud.

The SCIM scenarios are overview user stories designed to help clarify the intended scope of the SCIM effort.

2.2. Model Concepts

2.2.1. Triggers

Quite simply, triggers are actions or activities that start SCIM flows. Triggers may not be relevant at the protocol or the schema, they really serve to help identify the type or activity that resulted in a SCIM protocol exchange. Triggers make use of the traditional provisioning C.R.U.D (Create Read Update & Delete) operations but add additional use case contexts like "SSO" as it is designed to capture a class of use case that makes sense to the actor requesting it rather than to describe a protocol operation.

- o Create SCIM Identity Resource - Service On-boarding Trigger: A create SCIM resource trigger is a service on-boarding activity in which a business action such as a new hire or new service subscription is initiated by one of the SCIM Actors. In the protocol itself, service on-boarding may well be implemented via the same resource PUT method as a service change. This is particular to the implementation not to the use cases that drive that implementation.
- o Update SCIM Identity Resource - Service Change Trigger: An Update SCIM resource trigger is a service change activity as a result of an identity moving or changing its service level. An Update Identity trigger might be the result of a change in a service subscription level or a change to key identity data used to denote a service subscription level. Password changes are specifically called out from other more general identity attribute changes as they are considered to have specific use case differences.

- o Delete SCIM Identity Resource - Service Termination Trigger: A delete SCIM resource trigger represents a specific and deliberate action to remove an identity from a given SCIM service point. At this stage it is unclear if the SCIM protocol needs to identify separate protocol exchange for a service suspension actions. This may be relevant as target services usually differentiate between these result and may require separate resource representations as a result.
- o Single-Sign On (SSO) Trigger - Real-time Service Access Request: A SSO trigger is a special class of activity in which a Create or Update trigger is initiated during an SSO operational flow. The implication here is that as the result of a real-time service access request by the end user (SSO), defined SCIM protocol exchanges can be used to initiate SCIM resource CRUD somewhere in the service cloud.

2.2.2. Actors

Actors are the operating parties that take part in both sides of a SCIM protocol exchange, and help identify the source of a given Trigger. So far, we have identified the following SCIM Actors:

- o Cloud Service Provider (CSP): A CSP is the entity operating a given cloud service. In a SaaS scenario this is simply the application provider. In an IaaS or PaaS scenario, the CSP may be the underlying IaaS/PaaS infrastructure provider or the owner of the application running on that platform. In all cases, the CSP is the thing that holds the identity information being operated upon. Put another way, the CSP really is the service that the end-end user interacts with.
- o Enterprise Cloud Subscriber (ECS): An ECS represents a middle-tier of aggregation for related identity records. In one of our sample enterprise SaaS scenarios, the ECS is "FooBar.Inc" that subscribes to a cloud based CRM service service "SaaS-CRM.Inc" (the CSP) for all of its sales staff. The actual Cloud Service Users (CSUs) are the FooBar.Inc. sales staff. The ECS actor is identified to help capture use cases in which a single entitle is given administrative responsibility for other identity accounts. SCIM may not address the configuration and setup of an ECS within the CSP, but it does address use cases in which SCIM identity resources are grouped together and administers as part of some broader agreement or operational exchange.
- o Cloud Service User (CSU): A CSU represents the real cloud service end-end user - the "person logging into and using the cloud service". As described above, and ECS will typically own or

manage multiple CSU identities where as the CSU represents the FooBar.Inc. employee using the cloud service to manage their CRM process.

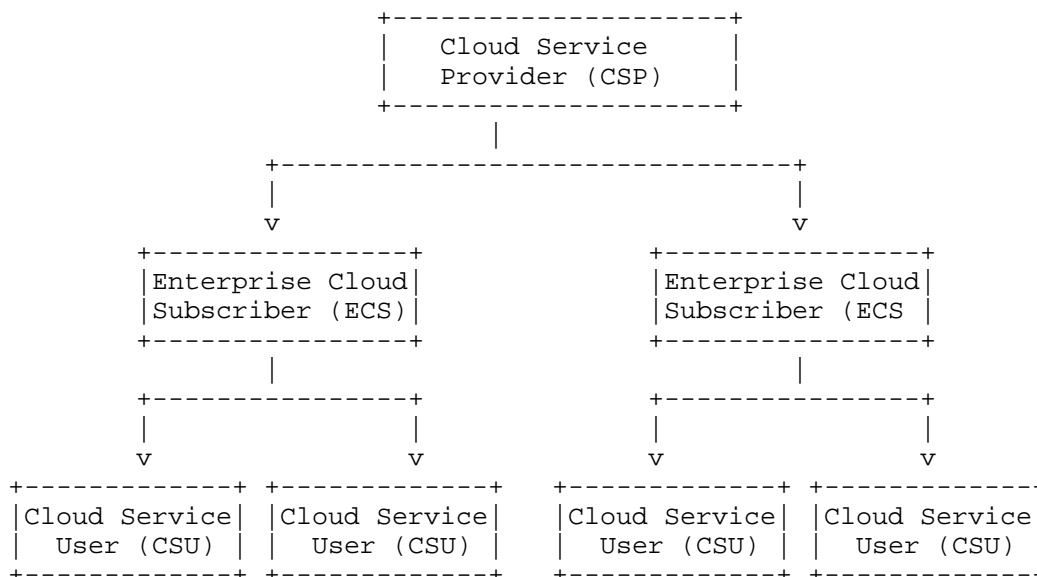


Figure 1: SCIM Actors

2.2.3. Modes & Flows

Modes identify the functional intent of a data-flow initiated in a SCIM scenario. The modes identified so far are 'push' and 'pull' referring to the fact of pushing data to, or pulling data from an authoritative identity data store.

In the SCIM scenarios, Modes are often used in the context of a flow between two Actors. For example, one might refer to a Cloud-to-Cloud Pull exchange. Here one Cloud Service Provider (CSP) is pulling identity information from another CSP. Commonly referenced flows are:

- o Cloud Service Provider to Cloud Service Provider (CSP->CSP)
- o Enterprise Cloud Subscriber to Cloud Service Provider (ECS-CSP)

Modes & flows simply help us understand what is taking place; they are likely to be technically meaningless at the protocol level, but again they help the reader follow the SCIM scenarios and apply them to real work use cases.

2.2.4. Bulk & Batch Operational Semantics

It is assumed that each of the triggers action outlined in this document may be part of the larger bulk or batch operation. Individual SCIM actions should be able to be collected together to create single protocol exchanges.

The initial focus of SCIM scenarios is on identifying base flows and single operations. The specific complexity of full bulk and batch operations is left to a later version of the scenarios or to the main specification.

2.3. Cloud Service Provider to Cloud Service Provider Flows (CSP->CSP)

These scenarios represent flows between two Cloud Service Providers (CSPs). It is assumed that each CSP maintains an Identity Data Store for its Cloud Service Users (CSUs). These scenarios address various joiner, mover, leaver and JIT triggers, resulting in push and pull data exchanges between the CSPs.

2.3.1. CSP->CSP - Create Identity (Push)

In this scenario two CSPs (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. CSP-1 receives a Create Identity trigger action from its Enterprise Cloud Subscriber (ECS-1). CSP-1 creates a local user account for the new CSU. CSP-1 then pushes the new CSU joiner push request down-stream to CSP-2 and gets confirmation that the account was successfully created. After receiving the confirmation from CSP-2, CSP-1 sends an acknowledgement to the requesting ECS.

2.3.2. CSP->CSP - Update Identity (Push)

In this scenario two CSPs (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. The Enterprise Cloud Subscriber (ECS-1) has already created an account with CSP-1 and supplied a critical attribute "department" that is used by CSP-1 to drive service options. CSP-1 then receives an Update Identity trigger action from its Enterprise Cloud Subscriber (ECS). CSP-1 updates its local directory account with the new department value. CSP-1 then initiates a separate SCIM protocol exchange to push the mover change request down-stream to CSP-2. After receiving the confirmation from CSP-2, CSP-1 sends an acknowledgment to ECS-1.

2.3.3. CSP->CSP - Delete Identity (Push)

In this scenario two CSPs (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. CSP-1 receives a Delete Identity trigger action from its Enterprise Cloud Subscriber (ECS-1). CSP-1 suspends the local directory account for the specified CSU account. CSP-1 then pushes a termination request for the specified CSU account down-stream to CSP-2 and gets confirmation that the account was successfully removed. After receiving the confirmation from CSP-2, CSP-1 sends an acknowledgment to the requesting ECS.

This use case highlights how different CSPs may implement different operational semantics behind the same SCIM operation. Note CSP-1 suspends the account representation for its service where as CPS-2 implements a true delete operation.

2.3.4. CSP->CSP - SSO Trigger (Push)

In this scenario two CSPs (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. However, rather than pre-provisioning accounts from CSP-1 to CSP-2, CSP-1 waits for a service access request from the end Cloud Service User (CSU-1) before issuing account creation details to CSP-2. When the CSU completes a SSO transaction from CSP-1 to CSP-2, CSP-2 then creates an account for the CSU based on information pushed to it from CSP-1.

At the protocol level, this class of scenarios may result in the use of common protocol exchange patterns between CSP-1 & CSP-2.

2.3.5. CSP->CSP - SSO Trigger (Pull)

In this scenario two CSPs (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. However, rather than pre-provisioning accounts from CSP-1 to CSP-2, CSP-2 waits for a service access request from the Cloud Service User (CSU-1) before initiating a Pull request to gather information about the CSU sufficient to create a local account.

At the protocol level, this class of scenarios may result in the use of common protocol exchange patterns between CSP-2 & CSP-1.

2.3.6. CSP->CSP - Password Reset (Push)

In this scenario two CSPs (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. CSP-1 wants to change the password for a specific Cloud Service User (CSU-1). CSP-1 sends a request to CSP-2 to reset the password value for CSU-1.

At the protocol level, this scenario may result in the same protocol exchange as any other attribute change request.

2.4. Enterprise Cloud Subscriber to Cloud Service Provider Flows(ECS->CSP)

These scenarios represent flows between an Enterprise Cloud Subscriber (ECS) and a Cloud Service Providers (CSP). It is assumed that both the ECS and the CSP maintains an LDAP service for the relevant Cloud Service Users (CSUs). These scenarios address various joiner, mover, leaver and JIT triggers, resulting in push and pull data exchanges between the ECS and the CSP.

Many of these scenarios are very similar to those defined in the Cloud Service Provider to Cloud Service Provider section above. They are identified separately here so that we may explore any differences and might emerge.

2.4.1. ECS->CSP - Create Identity (Push)

In this scenario an Enterprise Cloud Subscriber (ECS-1) maintains a service with a Cloud Service Provider (CSP-1) that requires the sharing of various Cloud Service User (CSU) accounts. A new user joins ECS-1 and so ECS-1 pushes an account creation request to CSP-1, supplying all required base SCIM schema attribute values and additional extended SCIM schema values as required.

2.4.2. ECS ->CSP - Update Identity (Push)

In this scenario an Enterprise Cloud Subscriber (ECS-1) maintains a service with Cloud Service Provider (CSP-1) that drives service definition from a key account schema attribute called Department. ECS-1 wishes to move a given CSU from Department A to Department B and so it pushes an attribute update request to the CSP.

2.4.3. ECS ->CSP - Delete Identity (Push)

In this scenario an Enterprise Cloud Subscriber (ECS-1) maintains a service with a Cloud Service Provider (CSP-1). Upon termination of one of its employees' employment agreement, ECS-1 sends a suspend account request to CSP-1 (Figure 1.4.3-1). One week later the ECS wishes to complete the process by fully removing the Cloud Service User (CSU) account and so it sends a terminate account request to CSP-1.

2.4.4. ECS ->CSP - SSO Pull

In this scenario an Enterprise Cloud Subscriber (ECS-1) maintains a service with a Cloud Service Provider (CSP-1). No accounts are created or exchanged in advance. However, rather than pre-provisioning accounts from ECS-1 to CSP-1, CSP-1 waits for a service access request from the Cloud Service User (CSU-1) under the control domain of ECS-1, before issuing an account Pull request to CSP-1.

3. SCIM use cases

This section lists the SCIM use cases.

3.1. Change of the ownership of a file

Description:

Bob - an employee of the company SomeEnterprise - creates a file, which is located at the cloud provided by SomeCSP. After Bob leaves SomeEnterprise, SomeCSP on a request from SomeEnterprise terminates Bob's rights to the file and transfers his former rights to Bill - another employee of SomeEnterprise.

Pre-conditions:

- o SomeCSP is a cloud service provider for SomeEnterprise
- o With permission of SomeEnterprise, Bob had created a file at the cloud provided by SomeCSP
- o Bob has left SomeEnterprise
- o SomeEnterprise terminates Bob's rights to the file and, possibly, decommisions Bob's identity
- o SomeEnterprise communicates the changes to Bob's rights to SomeCSP
- o SomeCSP enforces the changes made by SomeEnterprise
- o SomeEnterprise requests SomeCSP to transfer Bob's former rights to Bill

Post-conditions:

- o Bob does not have the rights to the file at the cloud provided by SomeCSP
- o Bill has the rights to the file that Bob had had

Requirements:

- o SomeEnterprise can securely communicate to SomeCSP all changes regarding its employee's identity
- o SomeCSP can enforce the requested changes
- o SomeCSP shall be able to log all changes regarding a SomeEnterprise employee's identity
- o The logs should be secure and available for auditing

3.2. Migration of the identities

Description:

A company SomeEnterprise runs an application ManageThem that relies on the identity information about its employees (e.g., identifiers, attributes). The identity information is stored at the cloud provided by SomeCSP. SomeEnterprise has decided to move identity information to the cloud of a different provider - AnotherCSP. In addition, SomeEnterprise has purchased a second application ManageThemMore, which also relies on the identity information. SomeEnterprise is able to move identity information to AnotherCSP without changing the format of identity information. The application ManageThemMore is able to use the identity information.

Pre-conditions:

- o SomeCSP is a cloud service provider for SomeEnterprise
- o SomeCSP has a known attribute name and value for the Enterprise used for managing and transferring data
- o AnotherCSP is a new cloud service provider for SomeEnterprise
- o All involved cloud service providers and applications support the same standard specifying the format for and actions on the user (e.g., employee) identity information

Post-conditions:

- o SomeEnterprise has moved its employees' identity information from SomeCSP to AnotherCSP without making any changes to representation of identity information
- o Application ManageThemMore is able to use the identity information

Requirements:

- o SomeEnterprise, the applications ManageThem and ManageThemMore, the providers SomeCSP and AnotherCSP support a common standard for identity information, which specifies the following:
 - * Format (or schema) for representing user identity information
 - * Interfaces and protocol for managing user identity information
- o Cloud providers shall be able to log all actions related to SomeEnterprise employees' identities
- o The logs should be secure and available for auditing

3.3. Single Sign-On (SSO) Service

Description:

Bob has an account with application hosted by a cloud service provider SomeCSP. SomeCSP has federated its user identities with a cloud service provider AnotherCSP. Bob requests a service from an application running on AnotherCSP. The application running on AnotherCSP, relying on Bob's authentication by SomeCSP and using identity information provided by SomeCSP, serves Bob's request.

Pre-conditions:

- o Bob's identity information is stored on SomeCSP
- o SomeCSP and AnotherCSP have established trust and federated their user identities
- o SomeCSP is able to authenticate Bob
- o SomeCSP is able to securely provide the authentication results to AnotherCSP
- o SomeCSP is able to securely provide Bob's identity information (e.g., attributes) to AnotherCSP
- o AnotherCSP is able to verify information provided by SomeCSP
- o SomeCSP is able to process the identity information received from AnotherCSP

Post-conditions:

Bob has received the requested service from an application running on AnotherCSP without having to authenticate to that application explicitly.

Requirements:

- o Bob must have an account with SomeCSP
- o SomeCSP and AnotherCSP must establish trust and federate their user identities
- o SomeCSP must be able to authenticate Bob
- o SomeCSP must be able to securely provide the authentication results to AnotherCSP
- o SomeCSP must be able to securely provide Bob's identity information (e.g., attributes) to AnotherCSP
- o AnotherCSP must be able to verify the identity information provided by SomeCSP
- o SomeCSP must be able to process the identity information received from AnotherCSP
- o SomeCSP and AnotherCSP must log information generated by Bob's actions according to their policies and the trust agreement between them

3.4. Provisioning of the user accounts for a Community of Interest (CoI)

Description:

Organization YourHR provides Human Resources (HR) services to a Community of Interest (CoI) YourCoI. The HR services are offered as Software-as-a-Service (SaaS) on public and private clouds. YourCoI's offices are located all over the world. Their Information Technology (IT) systems may be composed of the combinations of the applications running on Private and Public clouds along with the traditional IT systems. The local YourCoI offices are responsible for establishing personal information and (i.e., setting the user identities and attributes). YourHR services provide means for provisioning and distributing the employee identity information across all YourCoI offices. YourHR also enables the individual users (e.g., employees) to manage their personal information that they are responsible for (e.g., update of an address or a telephone number).

Pre-conditions:

- o YourCoI has a complex infrastructure composed of the large number of local offices that rely on the diverse IT systems
- o YourCoI has contracted YourHR to provide the HR services
- o Each local office has a right to establish a personal account for an employee

Post-conditions:

- o All personal accounts are globally available to any authorized user or application across the YourCoI system through the services provided by YourHR
- o The employees have ability to manage the part of personal information that is in their responsibility

Requirements:

- o YourHR must ensure that the personal information generated by the local offices is timely available in a globally-accessible database
- o Identity management of the personal data must be secure
- o All operation with identity data must be securely logged
- o The logs should be available for auditing

3.5. Transfer of attributes to a relying party web site

Description:

An end user has an account in a directory service A with one or more attributes. That user then visits relying party web site B, and the user authorizes the transfer of data via authorization protocols (e.g. OAuth, SAML), so selected attributes of the user are transferred from the user's account in directory service A to the web site B at the time of the user's first visit to that site.

Pre-conditions:

- o User has an account in a directory service A
- o User has one or more attributes

- o User visits web site of a relying party B

Post-conditions:

Selected attributes of the user are transferred from the user's account in directory service A to the web site B at the time of the user's first visit to that site.

Requirements:

Relying parties have to be aware of changes to their cached copy, as these would potentially cause a state change in other relying parties.

3.6. Change notification

Description:

An end user has an account in a directory service A with one or more attributes. That user then visits relying party web site B. Relying party web site B queries directory service A for attributes associated with that user, and related resources.

The attributes of the user change later in directory service A. For example, the attributes might change if the user changes their name, has their account disabled, or terminates their relationship with directory service A. Furthermore, other resources and their attributes might also change. The directory service A then wishes to notify relying party web site B of these changes, as relying party B might (or might not) have a cache of those attributes, and if the relying party B were aware of these changes to their cached copy, would potentially cause a state change in relying party B.

The volume of changes, however, might be substantial, and only some of the changes may be of interest to relying party B, so directory service A does not wish to "push" all the changes to B. Instead, directory service A wishes to notify B that there are changes potentially of interest, such that B can at an appropriate time subsequently contact directory service A and retrieve just the subset of changes of interest to B.

Note that the user must authorize the directory A service to transfer data to the web site, and the user must authorize the directory A service to notify the web site.

Pre-conditions:

- o User has an account in a directory service A

- o User has one or more attributes
- o User visits relying party web site B
- o The resource being updated is at the web site

Post-conditions:

Service A is able to notify B that there are changes potentially of interest.

Requirements:

B must be able at an appropriate time to subsequently contact directory service A and retrieve just the subset of changes of interest to B.

4. Security considerations

Authorization and authentication must be guaranteed for the SCIM operations.

5. IANA considerations

This Internet Draft includes no request to IANA.

6. Acknowledgements

Authors would like to thank Ray Countermand, Richard Fiekowsky and Bert Greevenbosch for their reviews and comments.

Also thanks to Darrian Rolls and Patrick Harding, the SCIM user scenarios section is taken from them.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

7.2. Informative References

[I-D.ietf-scim-api]
Drake, T., Mortimore, C., Ansari, M., Grizzle, K., and E. Wahlstroem, "System for Cross-Domain Identity Management:Protocol", draft-ietf-scim-api-01 (work in progress), April 2013.

[I-D.ietf-scim-core-schema]

Mortimore, C., Harding, P., Madsen, P., and T. Drake,
"System for Cross-Domain Identity Management: Core
Schema", draft-ietf-scim-core-schema-01 (work in
progress), April 2013.

Authors' Addresses

Phil Hunt
Oracle

Email: phil.hunt@oracle.com

Bhumip Khasnabish
ZTE USA, Inc.

Phone: +001-781-752-8003
Email: vumip1@gmail.com, bhumip.khasnabish@zteusa.com

Anthony Nadalin
Microsoft

Email: tonymad@microsoft.com

Zachary Zeltsan
Individual

Email: Zachary.Zeltsan@gmail.com

Kepeng LI
Huawei
Bantian
Shenzhen, Guangdong 518129
China

Email: likepeng@huawei.com