SCIM Use Case Challenges

New Challenges

- **Reconciliation**

  - For some reason, the RO and its RA's that was push by the Client was change in the Server (by some mechanism that was outside the SCIM agreement), which means that until the RO or one of its RA's changes in the Client, there will be no "fix" to the RO and its RA that are in the Server.
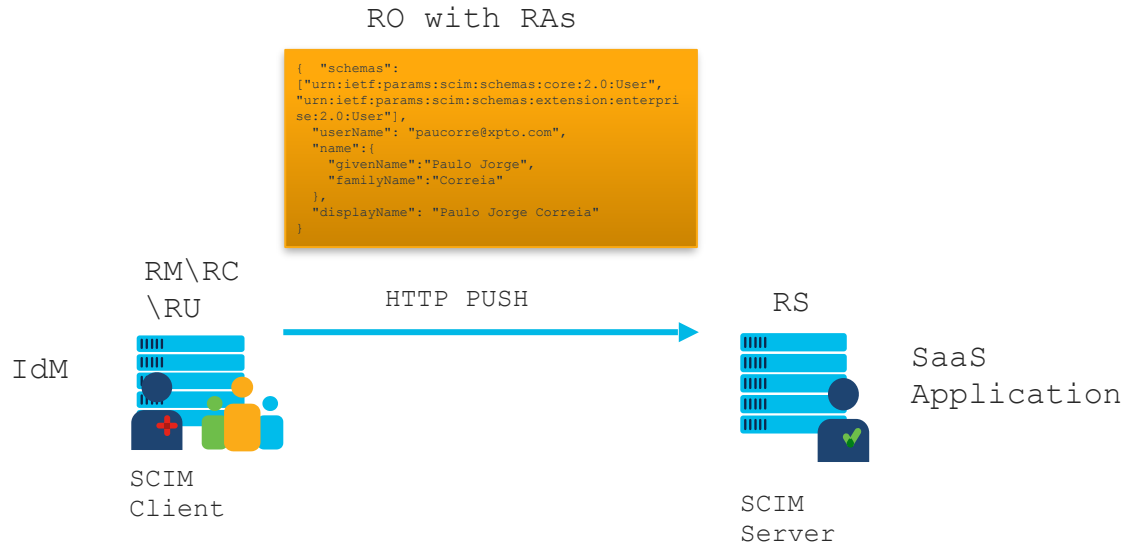
- **HR applications**

  - This type of SCIM element doesn't do any management to the RO and RA information, but it is the creator for RO and RA, most of the times have the RA that are generic to all applications (like firstname, lastname, national ID, office address, home address, etc.), most of the times this elements will not know RA like email, telephone number, etc. This RO and Ra needs to be available in the IdMs, for them to provide it to all the SCIM subscribers application.
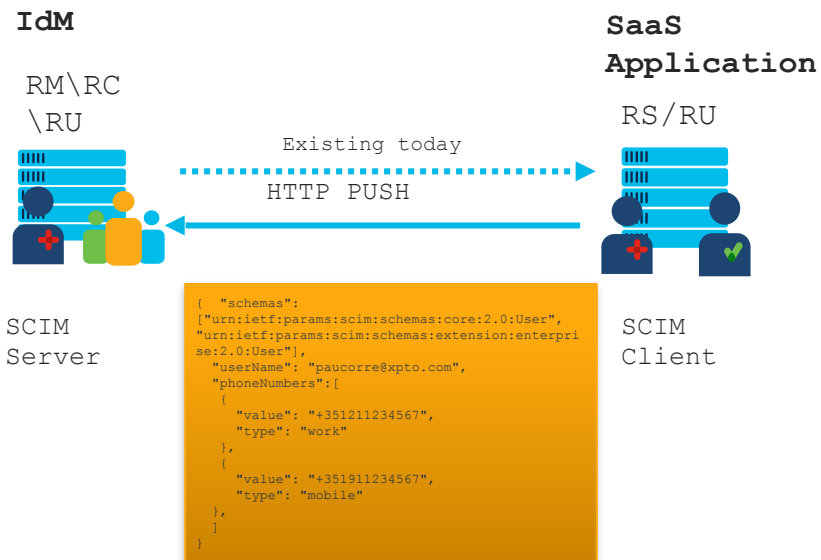
- **Extra RA for RO**

  - Some SCIM application that are typically SCIM Servers, are the creators and updaters of specific RA, for example an email server that will be a SCIM server should create the email RA for all the RO, but should only consume the other RA like firstname, lastname, etc.

Existing today

RO with RAs

```
{  "schemas":
["urn:ietf:params:scim:schemas:core:2.0:User",
"urn:ietf:params:scim:schemas:extension:enterpri
se:2.0:User"],
  "userName": "paucorre@xpto.com",
  "name":{
    "givenName":"Paulo Jorge",
    "familyName":"Correia"
  },
  "displayName": "Paulo Jorge Correia"
}
```

RM\RC
\RU

HTTP PUSH

RS

IdM

SCIM
Client

SaaS
Application

SCIM
Server

Extra RA for RO
Option 1

IdM

RM\RC
\RU

SCIM
Server

Existing today
HTTP PUSH

SaaS Application

RS/RU

SCIM
Client

{ "schemas":
["urn:ietf:params:scim:schemas:core:2.0:User",
"urn:ietf:params:scim:schemas:extension:enterpri
se:2.0:User"],
  "userName": "paucorre@xpto.com",
  "phoneNumbers":[
   {
    "value": "+351211234567",
    "type": "work"
   },
   {
    "value": "+351911234567",
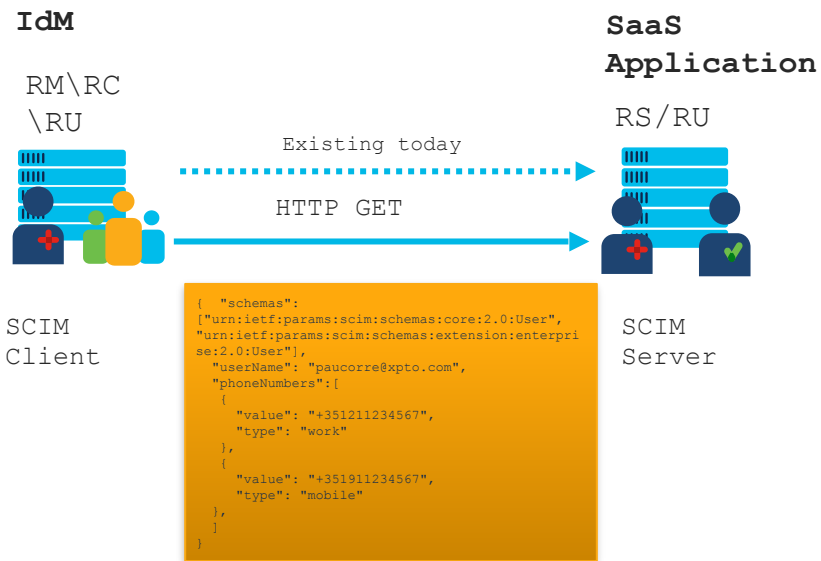   "type": "mobile"
   },
   ]
  }

Implications:

Both SCIM elements would need to implement SCIM Server and Client code

Both would need to have HTTP services, with endpoints like /users /groups, etc.

Both would need to have an authorization mechanisms for the HTTP endpoints.

Extra RA for RO
Option 2

IdM

RM\RC\RU

Existing today

HTTP GET

SaaS Application

RS/RU

SCIM Client

```
{  "schemas":
["urn:ietf:params:scim:schemas:core:2.0:User",
"urn:ietf:params:scim:schemas:extension:enterpri
se:2.0:User"],
   "userName": "paucorre@xpto.com",
   "phoneNumbers":[
     {
       "value": "+351211234567",
       "type": "work"
     },
     {
       "value": "+351911234567",
       "type": "mobile"
     },
   ]
}
```

SCIM Server

Implications:

There would need to be a changes database in the Server, just for the interesting RA, to provide only the deltas from the last trigger.

We would need to have independent RA agreements per direction configured in the client.

RFC 7642