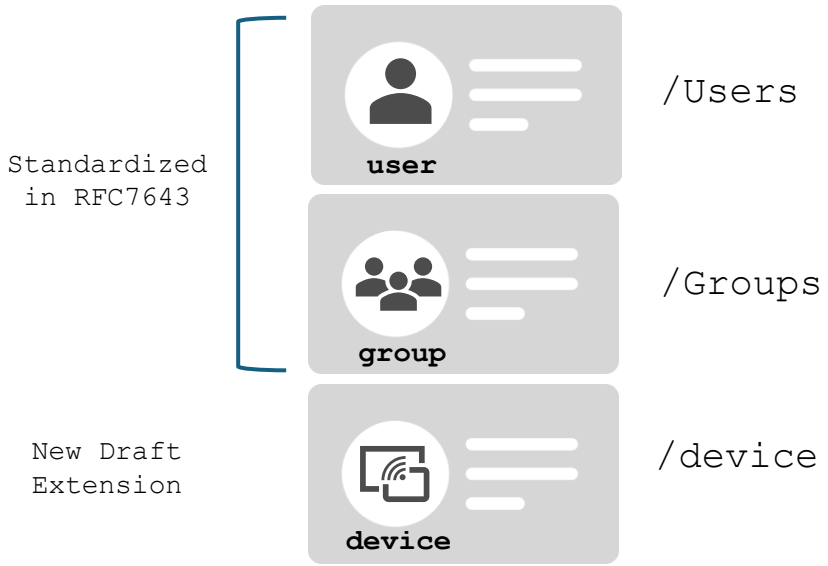
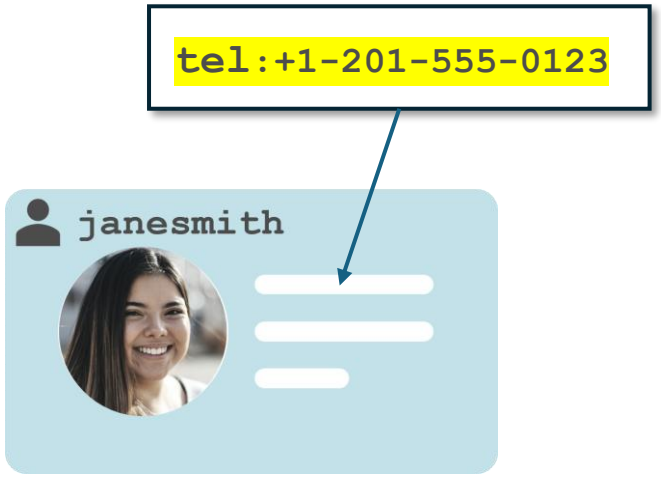
SCIM Use Cases

SCIM Basics





Resource Type

Definition of a resource name, endpoint URL, schema, and other metadata that indicate where a resource is managed and how it is composed

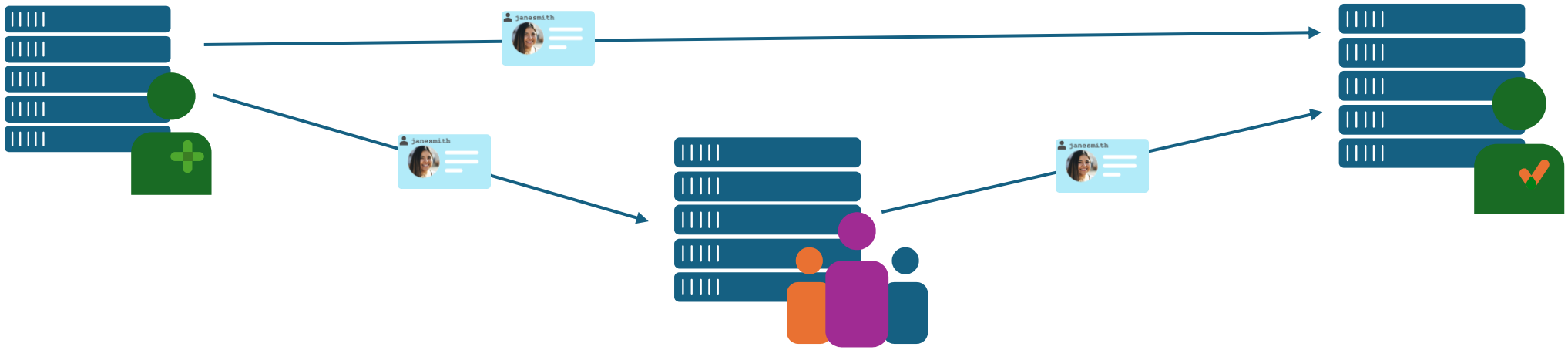
Resource Object(RO)

Set of attributes for a **specific** resource

Resource Attribute (RA)

A name-value pair containing at least one simple or complex value, either of which may be multi-valued.

Orchestrator Roles



Resource Creator (RC)
Resource Updater (RU)

Component of the system that create/updates the resources and their attributes

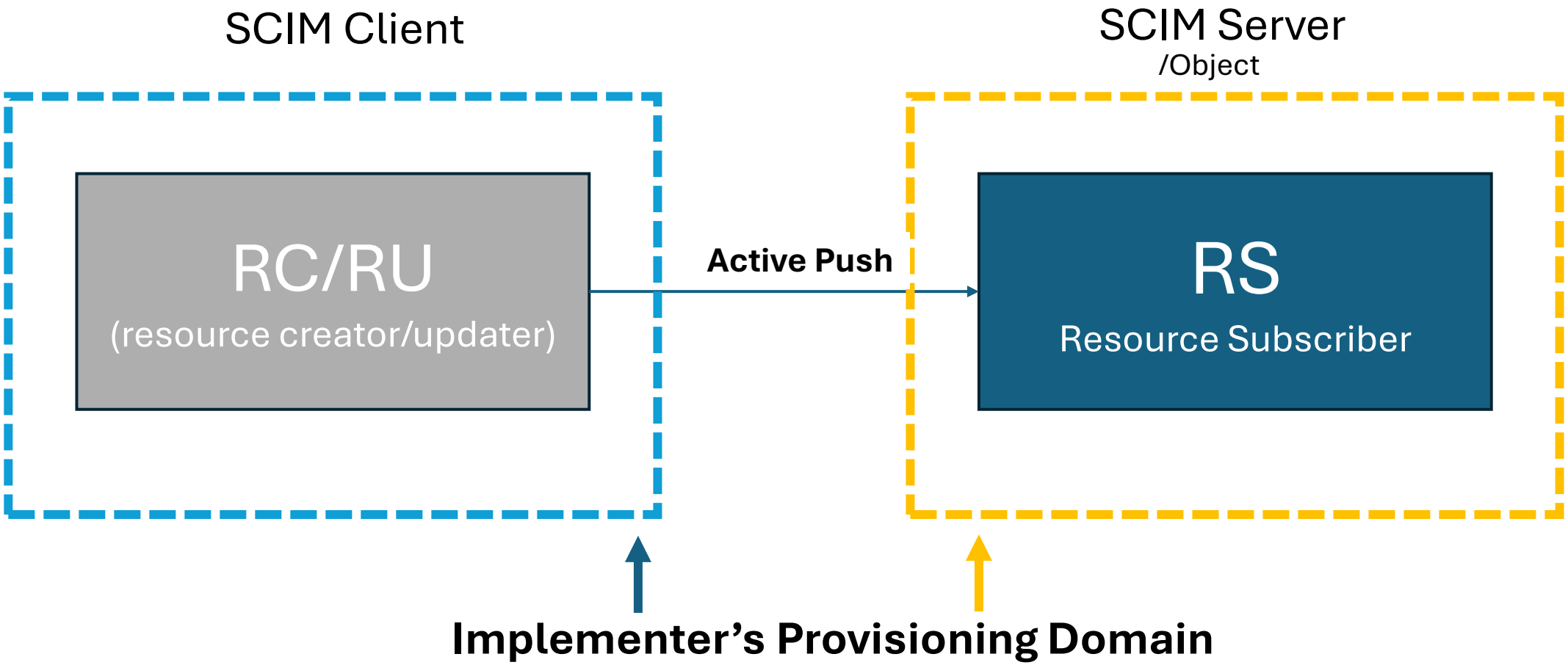
Resource Manager (RM)

Component of the system that manage multiple Creators and Subscribers, maintaining the latest information on the resources

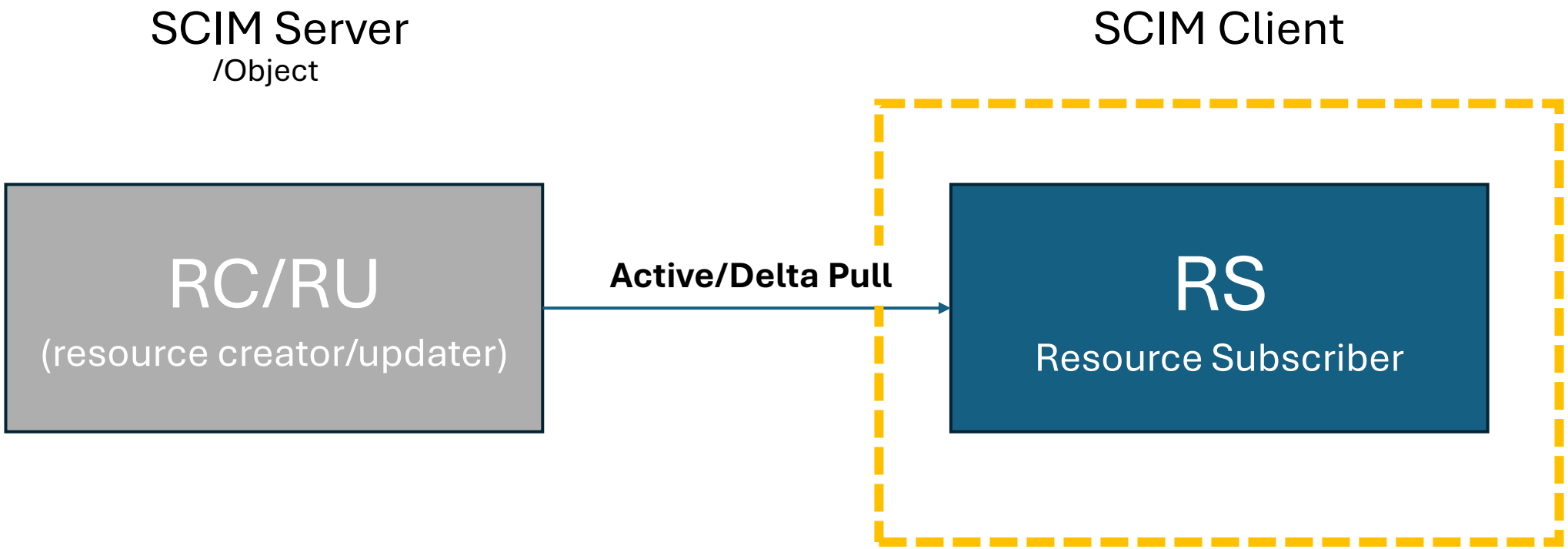
Resource Subscriber (RS)

Component of the system that will consume the information from Resource Manager

Provisioning Domains & SCIM Actions/Triggers



Provisioning Domains & SCIM Actions/Triggers



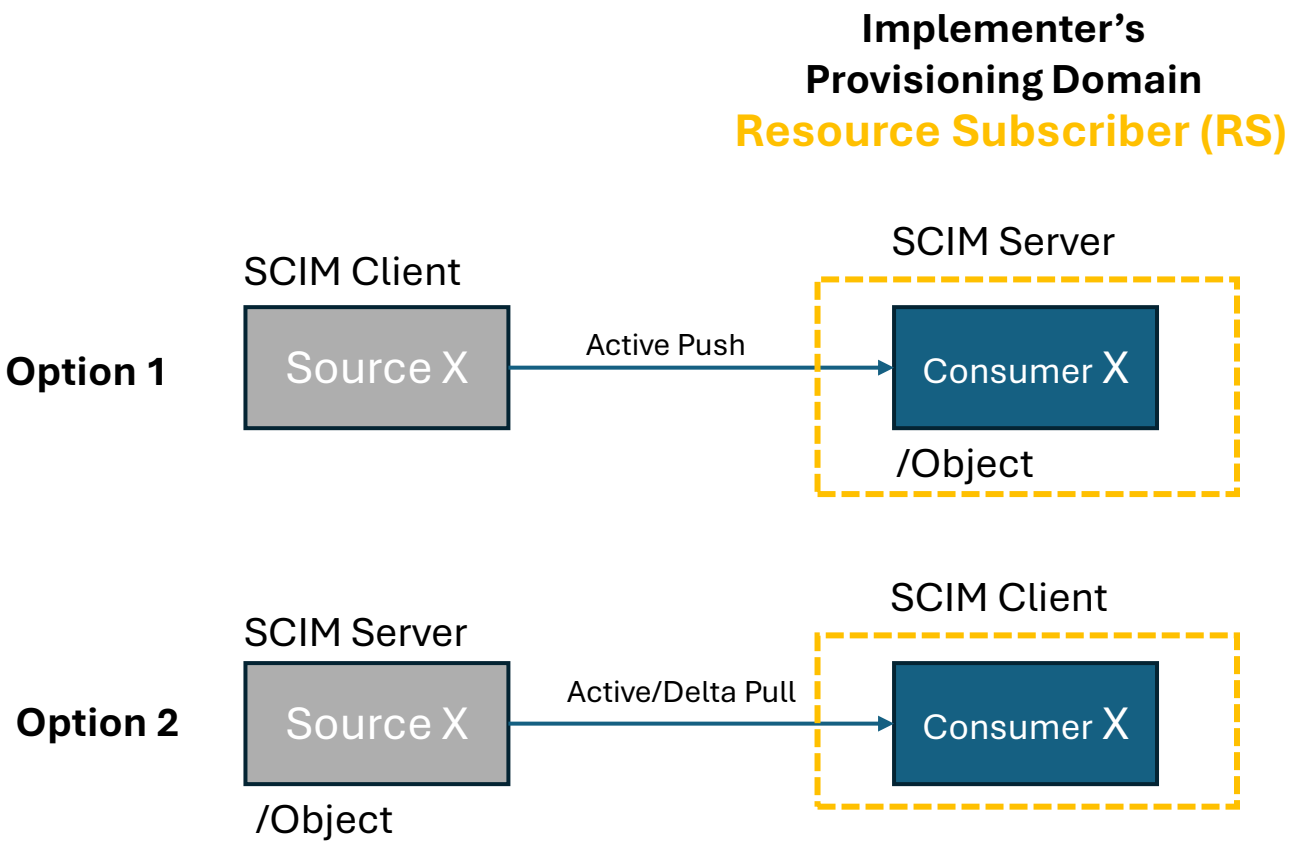
Which Implementer are you?

Use Cases

Common Generic Scenarios

UC1: Resource Subscriber

Single-tenant Resource Subscriber (**RS**)

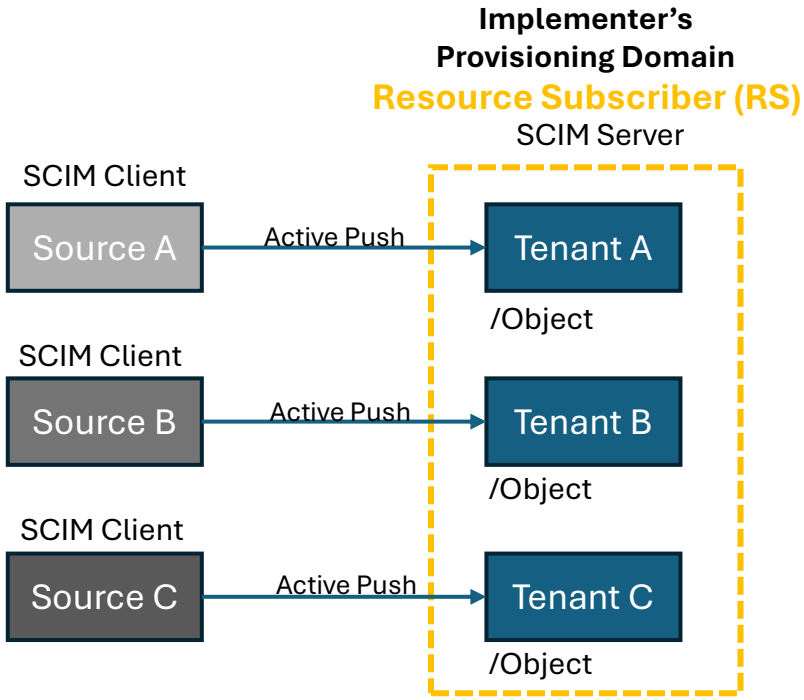


- Resource Subscribers (RS) receive data from a remote corporate data store
- RS can be a SCIM Server or Client
- Implementer Considerations
  - Matching conventions with existing API infrastructure
    - Cursor vs. Index pagination
  - Using existing API security
  - Least Privilege/authorization
- Option 1 it is almost 100% of the implementations today
- Option 2 is a good option for when the Resource Subscriber is not reached from remote corporate data store

UC1: Resource Subscriber

Multi-tenant Resource Subscriber (**RS**)

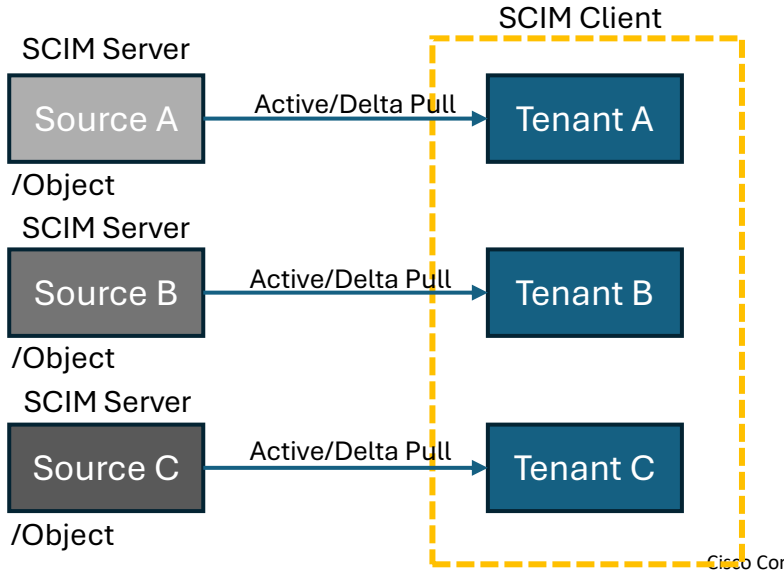
Option 1



- Resource Subscribers (RS) receive data from a remote corporate data store
- RS can be a SCIM Server or Client
- Implementer Considerations
  - Matching conventions with existing API infrastructure
    - Cursor vs. Index pagination
  - Using existing API security
  - Least Privilege/authorization

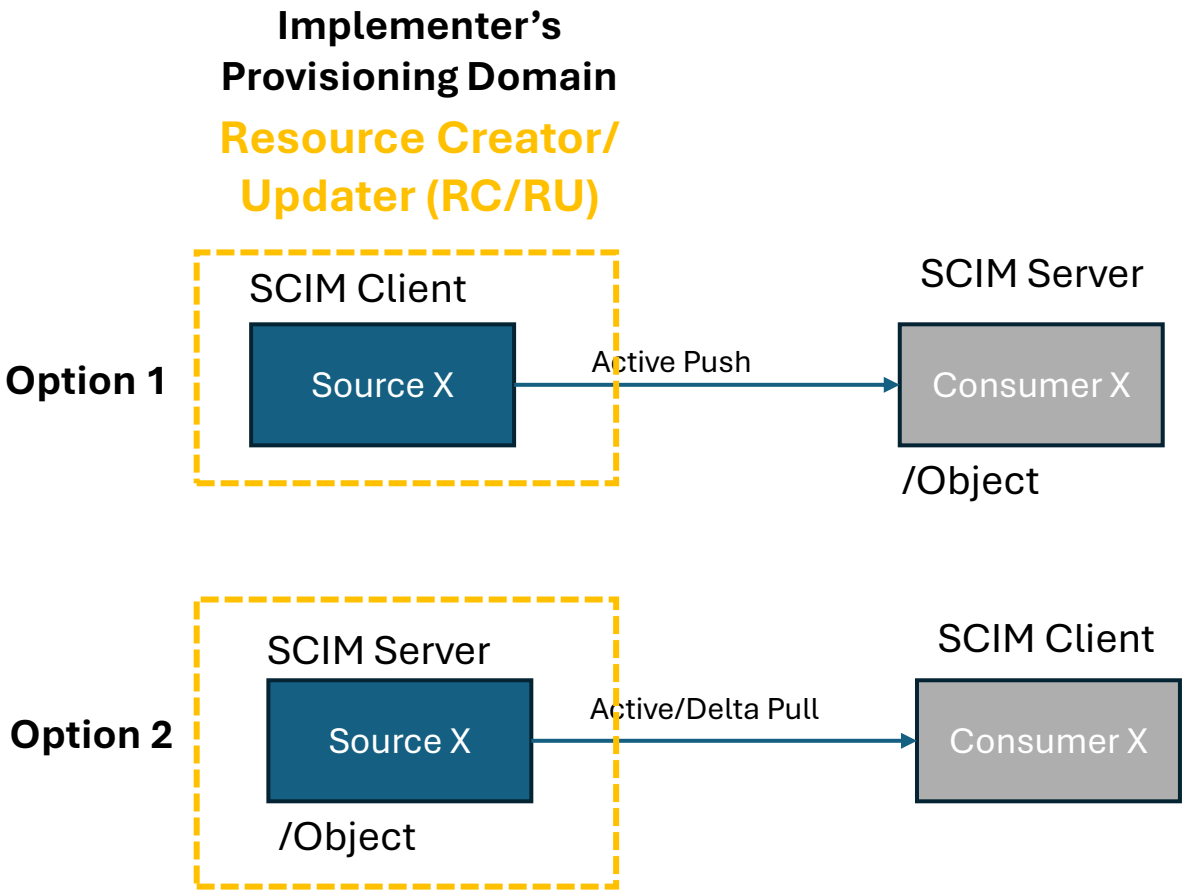
- Option 1 it is almost 100% of the implementations today
- Option 2 is a good option for when the Resource Subscriber is not reached from remote corporate data store

Option 2



UC2: Resource Creator

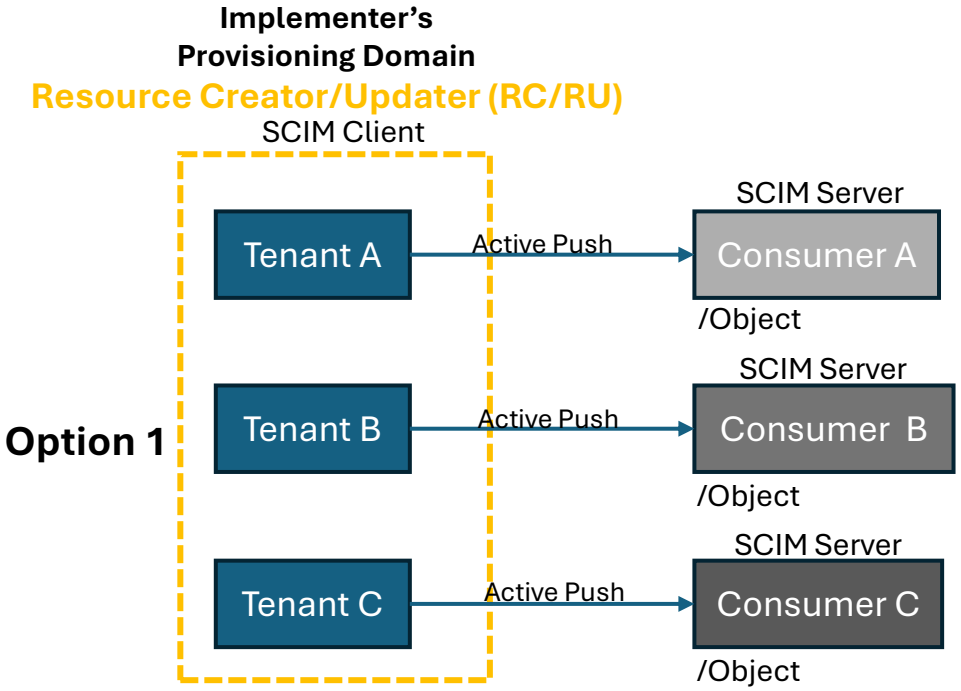
Single-tenant Resource Creator/Updater (**RC/RU**)



- Single-Tenant Resource Creator/Updater (RC/RU) sends data to consumer
- RC/RU can be a Single-Tenant SCIM Server or Client
- Implementer Considerations
  - Matching conventions with existing API infrastructure
    - Cursor vs. Index pagination
  - Using existing API security
  - Least Privilege/authorization
- Option 1 it a common implementation today
- Option 2 is a good option for when the Resource Subscriber is not reached from remote corporate data store

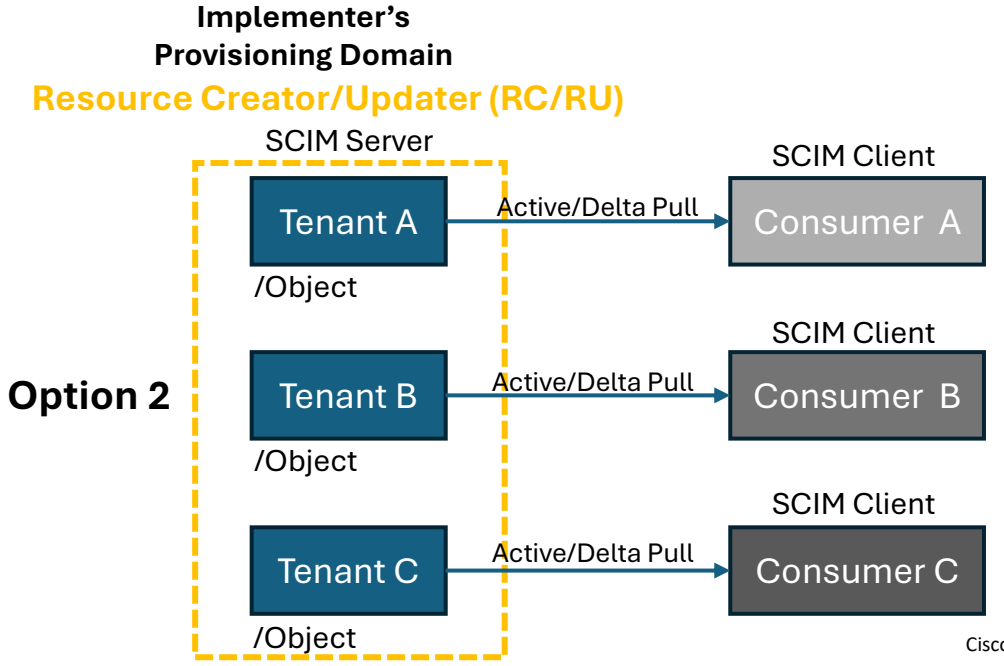
UC2: Resource Creator

Multi-tenant Resource Creator/Updater (**RC/RU**)



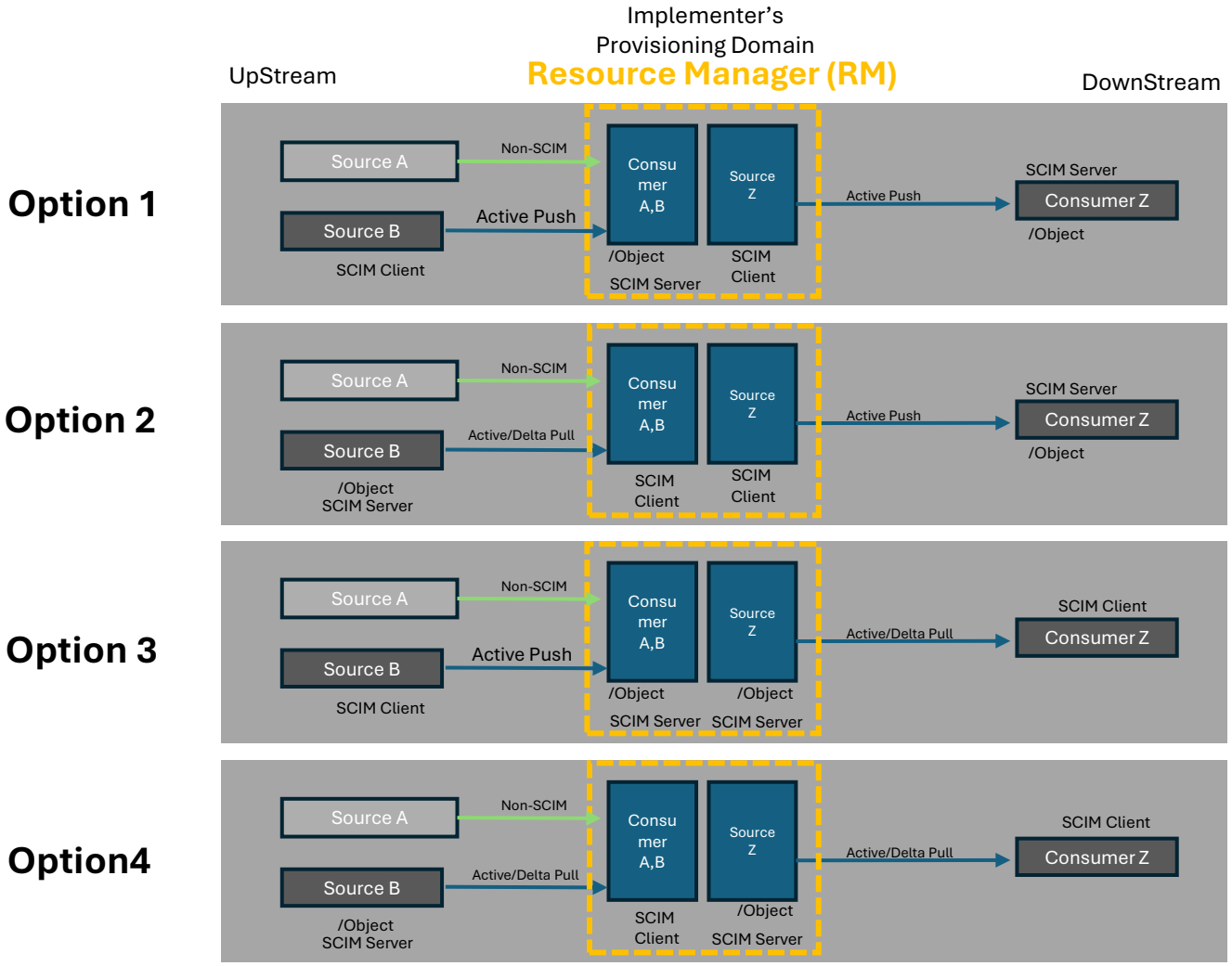
- Multi-Tenant Resource Creator/Updater (RC/RU) sends data to consumers
- RC/RU can be a Multi-Tenant SCIM Server or Client
- Implementer Considerations
  - Matching conventions with existing API infrastructure
    - Cursor vs. Index pagination
  - Using existing API security
  - Least Privilege/authorization

- Option 1 it is almost 100% of the implementations today
- Option 2 is a good option for when the Resource Subscriber is not reached from remote corporate data store



UC3: Resource Manager

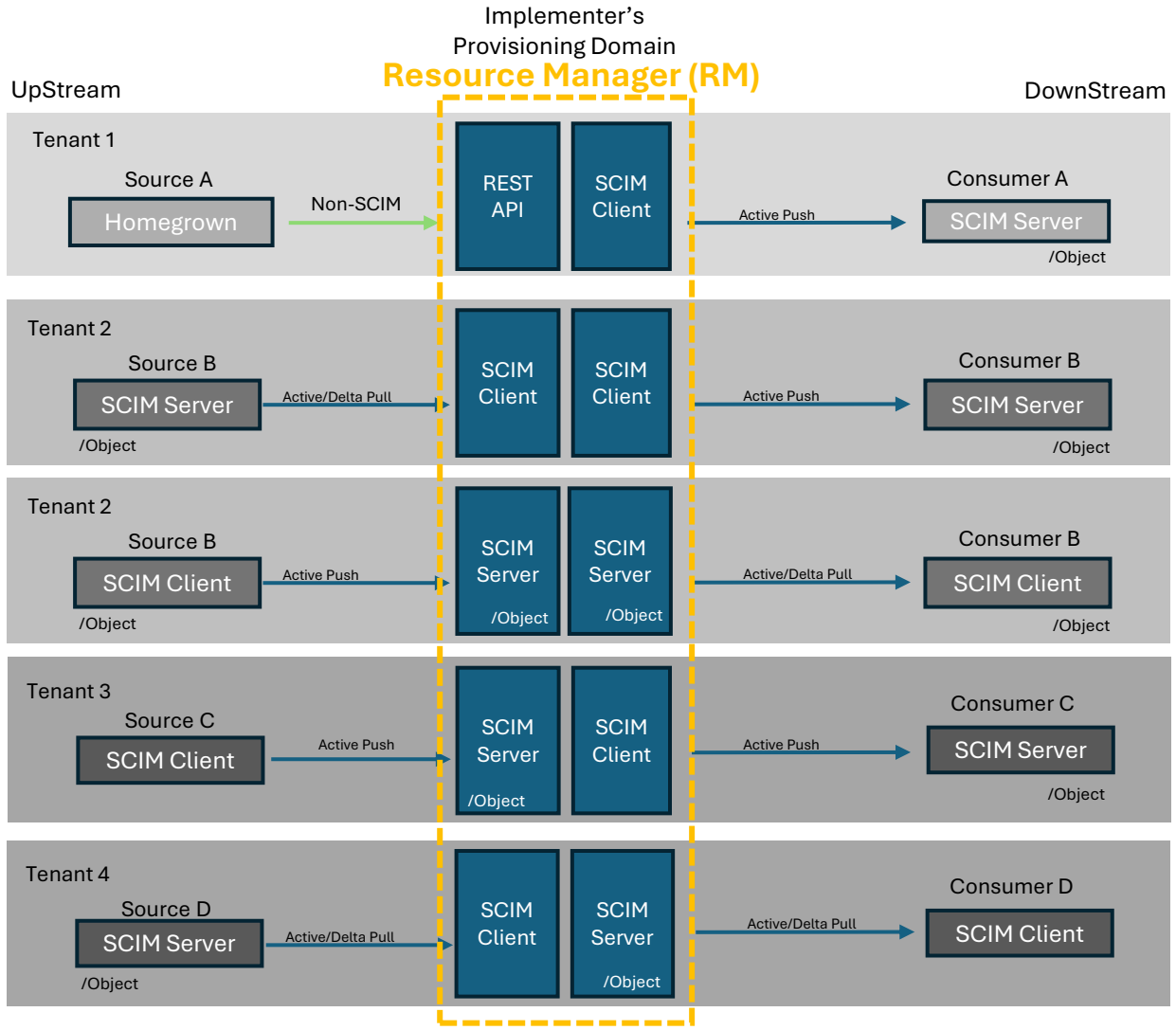
Single-Tenant Resource Manager (**RM**)



- Normally one or more upstream object database that populates the Resource Manager that after provides that resource information to downstream services that requires a specific that requires a specific sets of the populated objects.
- Implementer Considerations
  - Matching conventions with existing API infrastructure
    - Cursor vs. Index pagination
  - Using existing API security
  - Least Privilege/authorization
- Option 1 and 2 are most common to see in the Implementers Provision Domain
- Option 3 and 4 will make sense when upstream or downstream services can't be directly reach.

UC3: Resource Manager

Multi-tenant Resource Manager (**RM**)



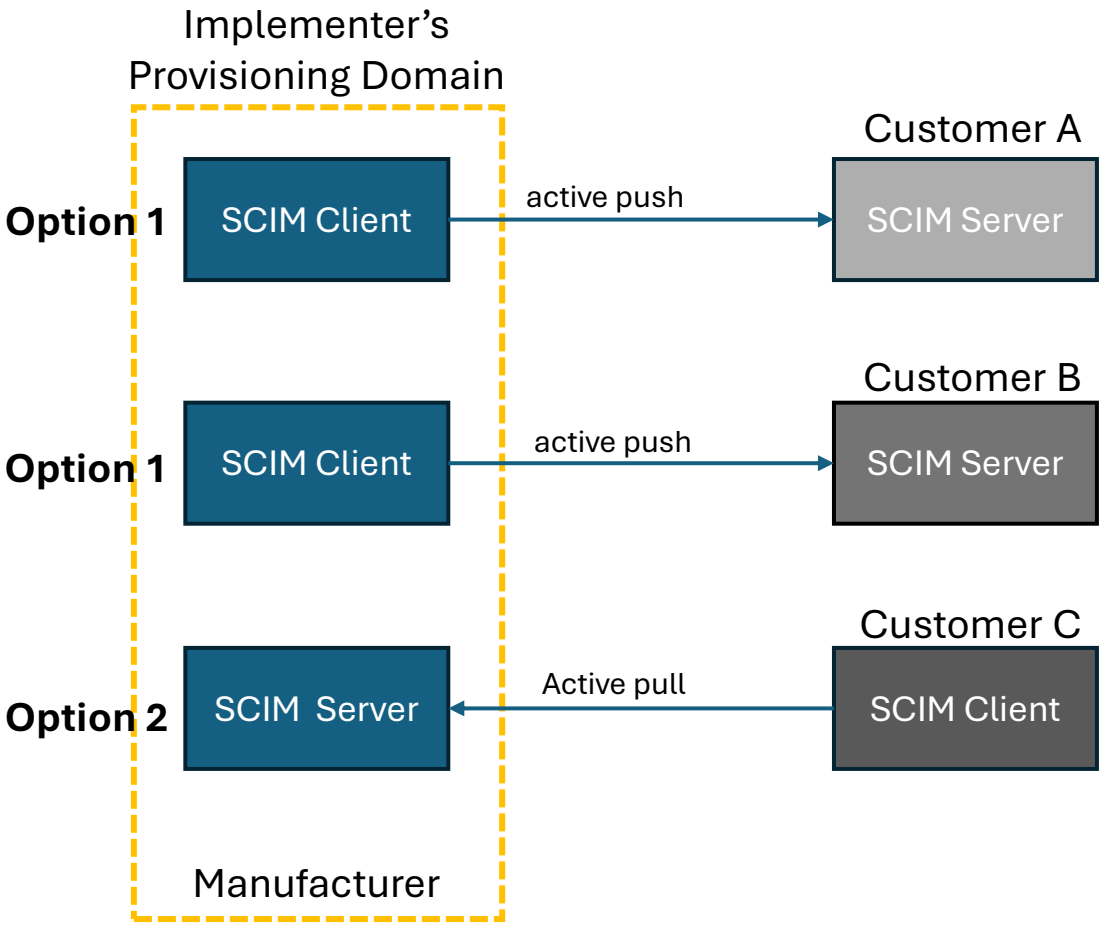
- Normally one or more upstream object database that populates the Multi-Tenant Resource Manager, that after provides that resource information to downstream services that requires a specific sets of the populated objects.
- Implementer Considerations
  - Matching conventions with existing API infrastructure
    - Cursor vs. Index pagination
  - Using existing API security
  - Least Privilege/authorization
- Typically, we see SCIM Clients functions in the Resource Manager.
- To address issues of upstream or downstream services not be reachable we might also fin in the Resources Manager the SCIM server role.

Use Cases

Specific implementations

UC4: Partner Device Registry

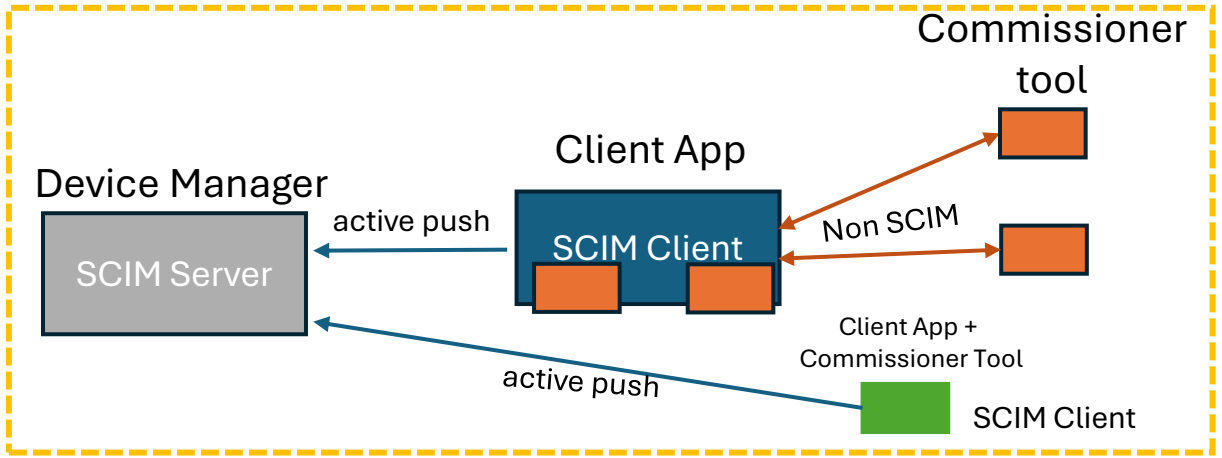
Manufacturer details pushed to customers at time of device sale



- Specification:
- ROs representing devices purchased by a customer are pushed only to that customer
- Maybe or may not be Multi-tenant

UC5: Device identity Creation from Commissioner Tool

Customer uses Client App to provide specific centric customer attributes of the IOT device

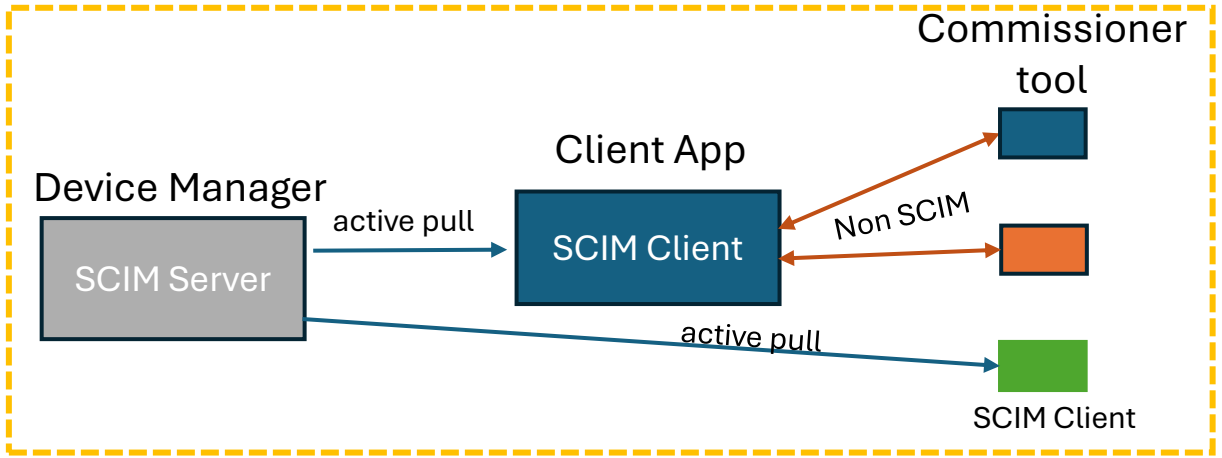


Specification:

- IOT devices using Matter or other protocol provide the Client App (Mobile App, Web Application) information about itself
- Client App fill up information about the IOT device
- Typically, the communication between IOT Device and Client App is using protocols like Bluetooth, Zigbee, Thread, etc.
- SCIM clients should only be able to access to devices that they manage

UC6: Client App get directory services

Client App gets information about all the devices and its attributes in customer environment

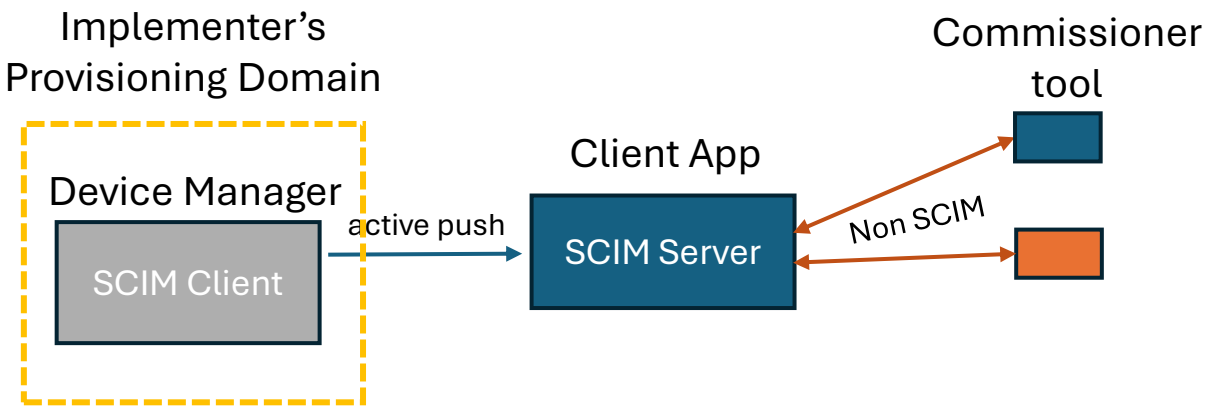


Specification:

- Client App gets from device manager information about all devices and its attributes from their environments
- Client App does the operation of downloading the full list of devices typically every day in non working hours, optionally with on-demand sync
- SCIM clients should only be able to access to devices that they manage

UC7: other device use cases

Provide credentials to manage device

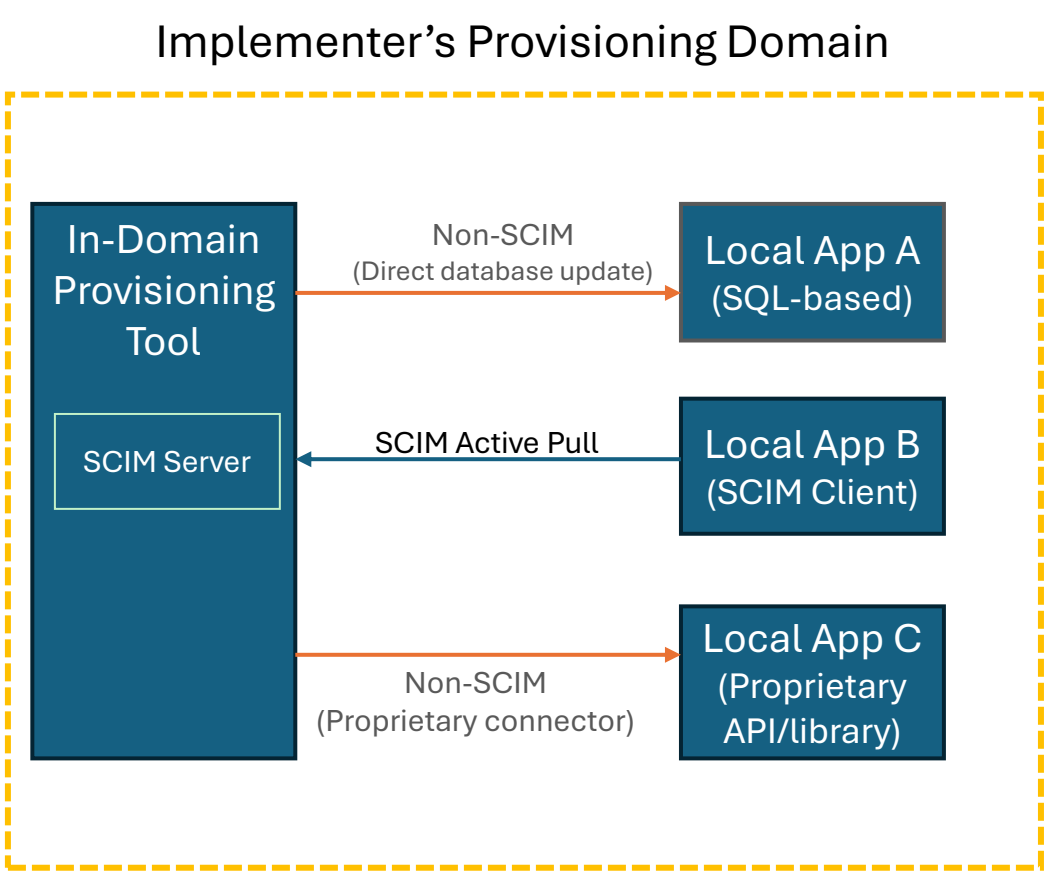


Specification:

- Device manager provides certificate and application details to the Devices gateway to allow it to establish trust.

UC8: Enterprise Simple Apps

Single-tenant Resource Creators & Subscribers

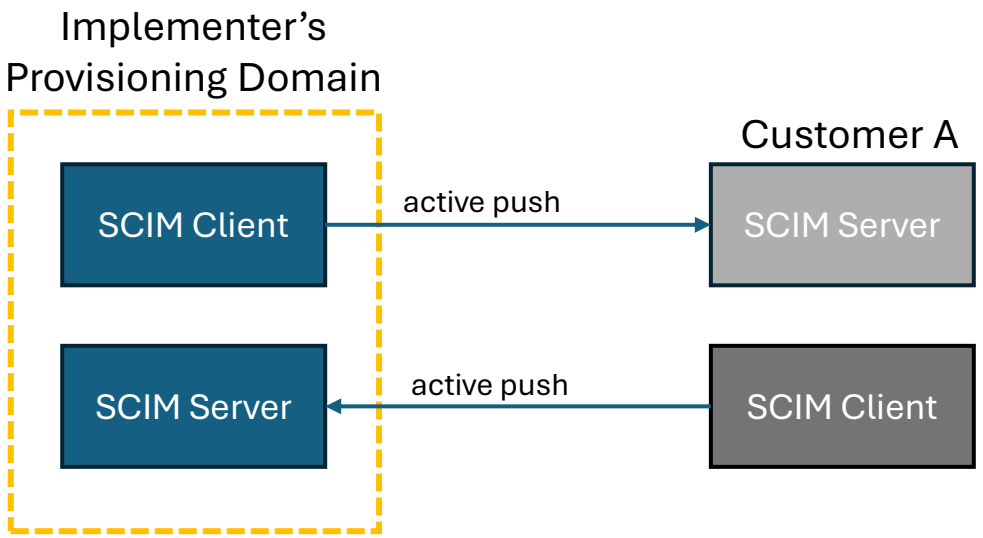


- Some apps can't run fancy SCIM implementations
  - Homegrown apps with local databases
  - Small line of business applications
- If no native provisioning capabilities
  - HTTP Headers
  - Libraries / framework modules
  - Proxies
- No ability to be SCIM Server
  - Often must be client

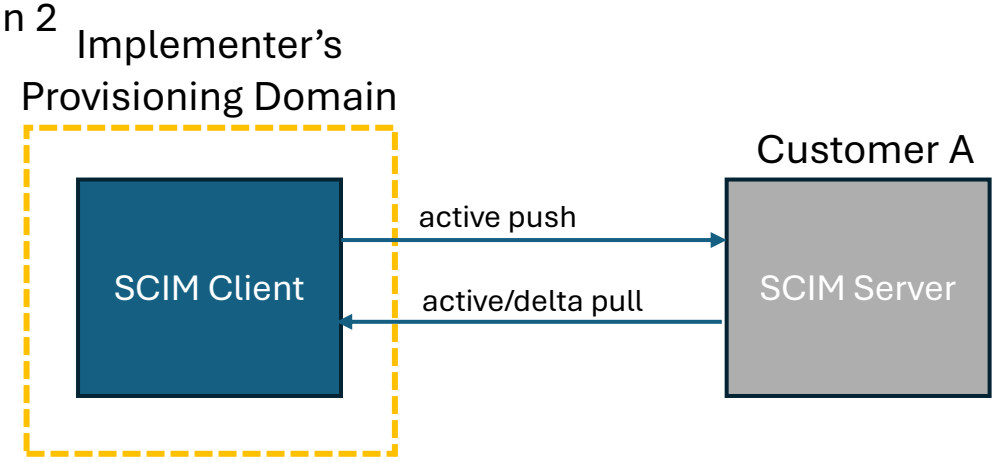
UC9: RA authority in SaaS App

Creation and Updating of attributes resides in SaaS App and Resource Creators/Updaters

Option 1



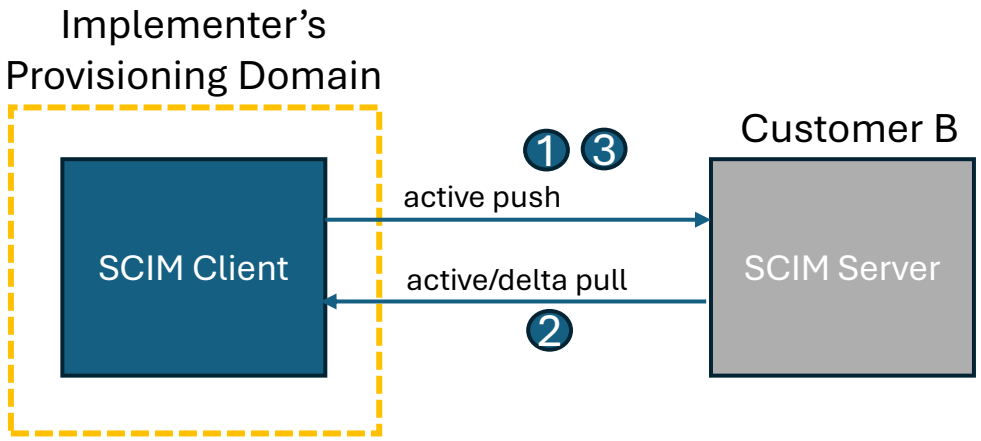
Option 2



- Some Attributes are own by the SaaS Application while the Resource Object and the other attributes are own by the IdM

UC10: Reconciliation

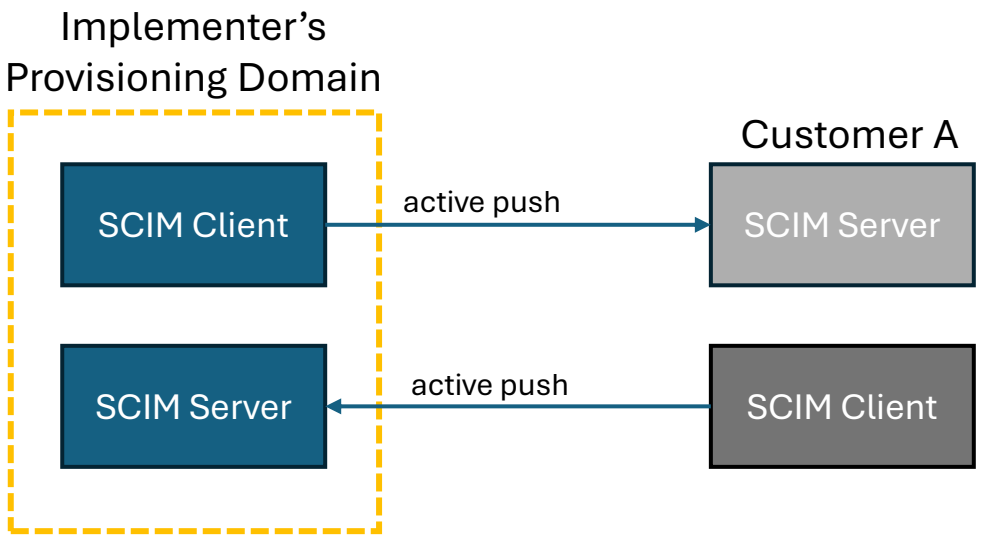
Bringing consistency between the IdM and the Enterprise Applications



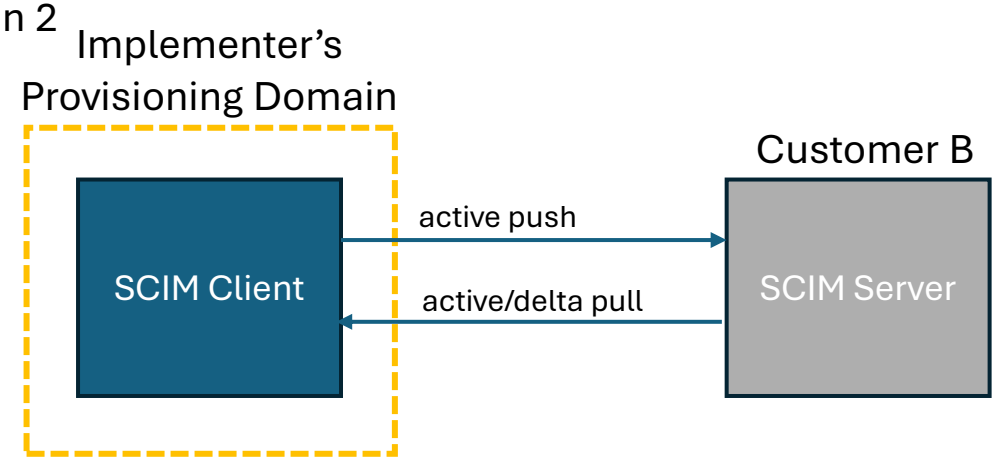
- Because of inconsistencies or mistakes in the SaaS App Resource Objects and it attributes might change and there is no visibility of the IdM that it happens.
- System will do reconciliation to make sure that Resource Objects and its Attributes are consistent across different systems
- If there is a new attributes from SCIM Server in the Delta Pull, the SCIM client will do a push to fix it and make again synchronize

UC11: HR Application

Option 1



Option 2



- Some Attributes are own by the SaaS Application while the Resource Object and the other attributes are own by the Provision domain (Typically the IdP)

Other Slides