SCIM Use Case Scenario
Presumptions

- SCIM Triggers
- SCIM Security Model
- PII
Scenarios

• **Cloud-to-Enterprise PUSH and Cloud-to-Cloud PUSH**
  • The Event Receiver already has SCIM access to the Event Transmitter service provider (includes HTTP credentials and endpoint).
  • Event Receivers and Transmitters can agree out-of-band on SET/JWT security requirements including use of signing and/or encryption to be documented in a Stream Configuration.
Scenarios

- **Cloud-to-Enterprise POLLING**
  - The Event Receiver already has SCIM access to the Event Transmitter service provider (includes HTTP credentials and endpoint).
  - Event Receivers and Transmitters can agree out-of-band on SET/JWT security requirements including use of signing and/or encryption to be documented in a Stream Configuration.
Scenarios

• **Cloud-to-Mobile Application PUSH**
  • The Event Receiver already has SCIM access to the Event Transmitter service provider (includes HTTP credentials and endpoint).
  • Event Receivers and Transmitters can agree out-of-band on SET/JWT security requirements including use of signing and/or encryption to be documented in a Stream Configuration.