SCIM Notify

IETF 91

October 2014

Phil Hunt, Ian Glazer, Morteza Ansari

IETF NOTEWELL

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

The IETF plenary session

The IESG, or any member thereof on behalf of the IESG

Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices

Any IETF working group or portion thereof

Any Birds of a Feather (BOF) session

The IAB or any member thereof on behalf of the IAB

The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

- Introduction
- Use Cases
- Proposal

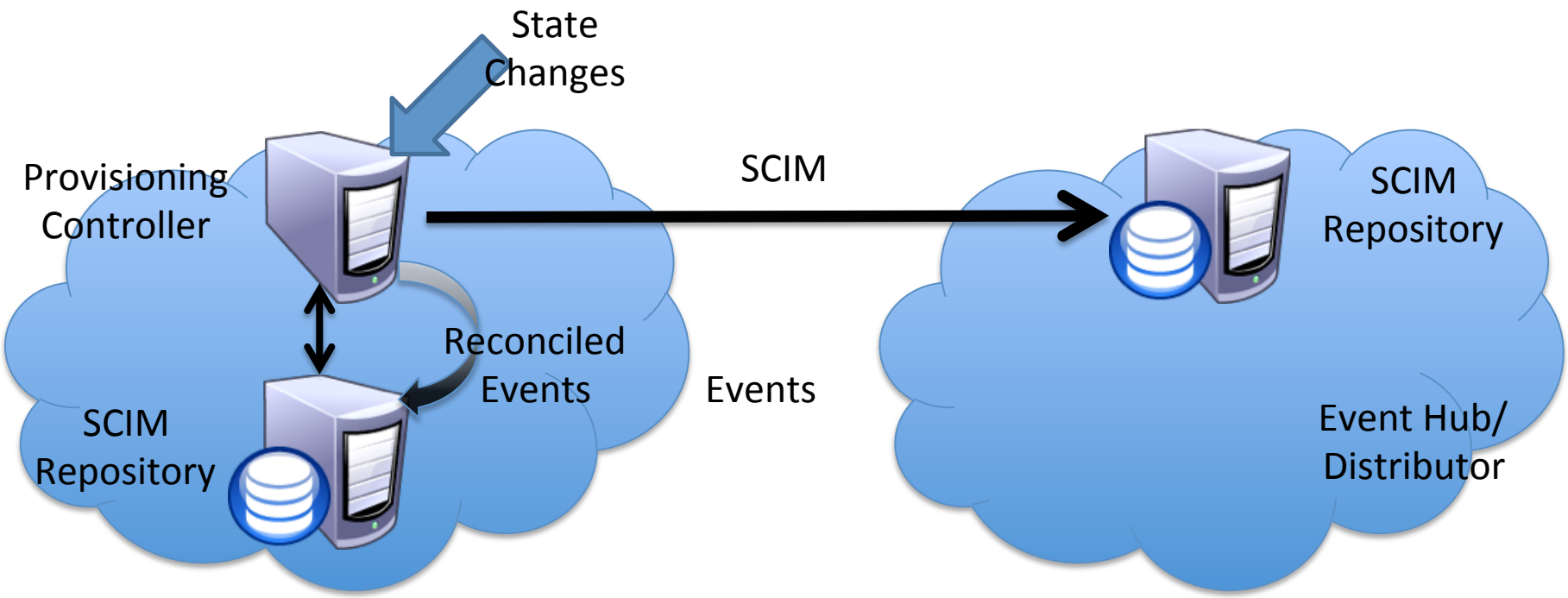
Introduction

- Many REST APIs generate a volume of web accessible resources each with individualized state.
  - Subscribers want to know about changes in state
  - Systems need to co-ordinate events and workflows
- Identity data systems
  - Multiple silos of Identity (federated, local, …)
  - Multiple domains
- SCIM service providers need to
    - Co-ordinate events with enterprise internal IDM systems
    - Co-ordinate events cross-cloud between providers/tenancies

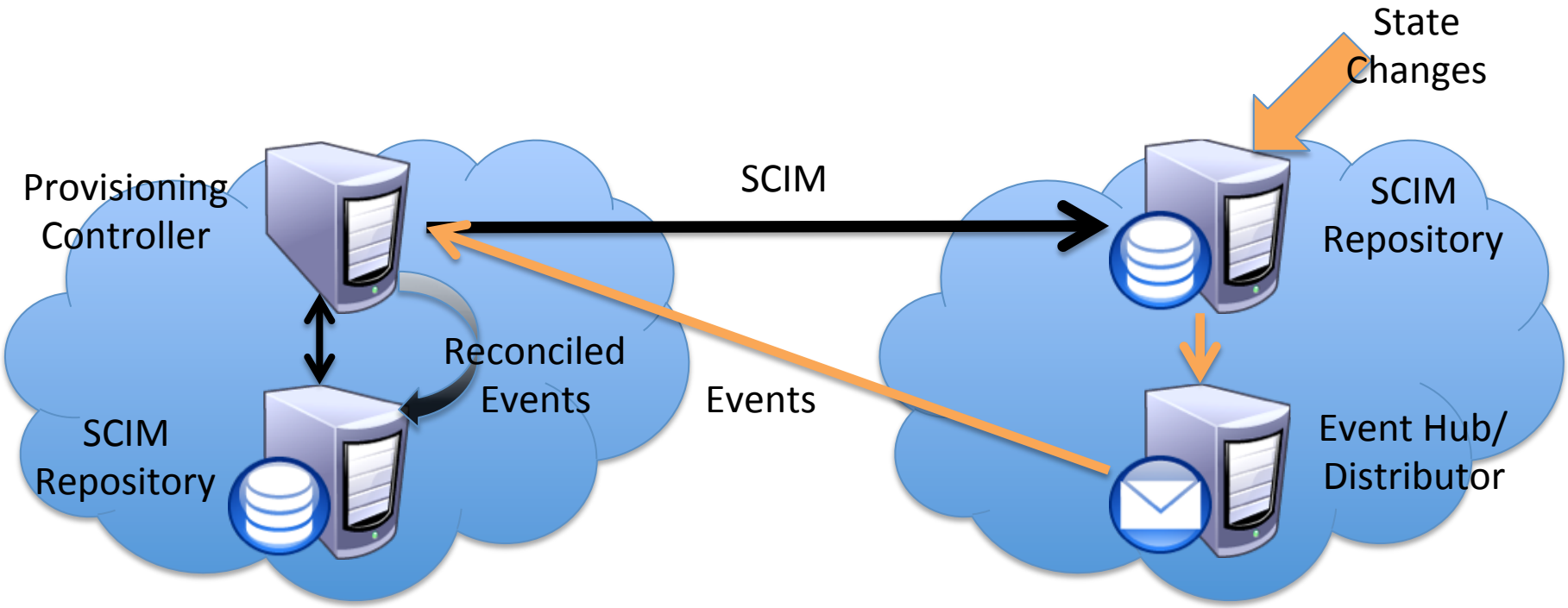
RESTful vs. Eventful

- With restful SCIM, "control" resides with the client requestor.
  - The client is transferring state to/from the service provider which responds to the client requests as information "owner"
- In Change Notify, "control" resides with a subscriber, in response to a published event.
  - "State change" instead of "state transfer"
  - Subscriber decides relevance
  - Subscriber uses SCIM to "reconcile" or request more information (transformation)
  - Delivery of event matters
    - The publisher is not aware of "completion" on the subscriber side

Typical SCIM



SCIM and Event Notification



"State" Problem

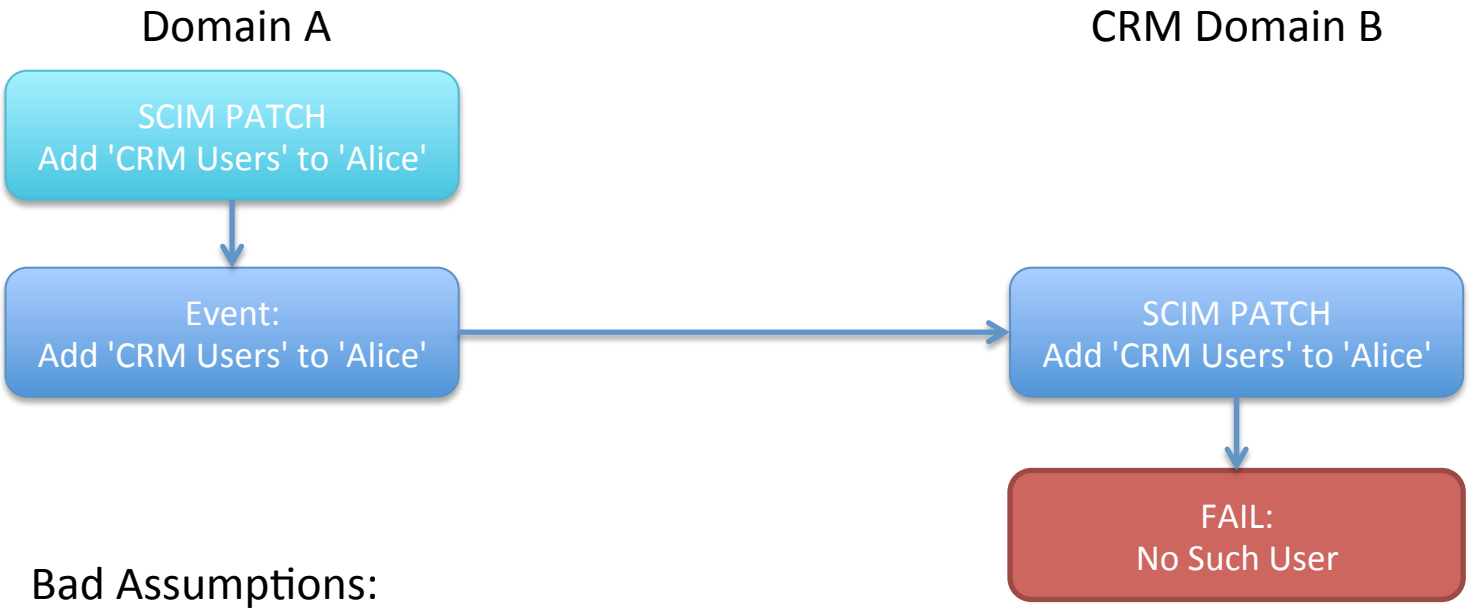
- Domains are independent
  - Resources may be different (e.g. populations)
  - Resources may have differing life-cycles/ workflows
  - Schema may be different (e.g. extensions)
  - Error signals can leak confidential information
  - State is never 100% synchronized
- Events need interpretation / transformation in context

SCENARIOS & USE CASES

Example Scenarios

1. Alice is given the CRM role causing her to be provisioned in another domain.
2. Alice's role in CRM is revoked.

Scenario 1 Flow – Replica Style



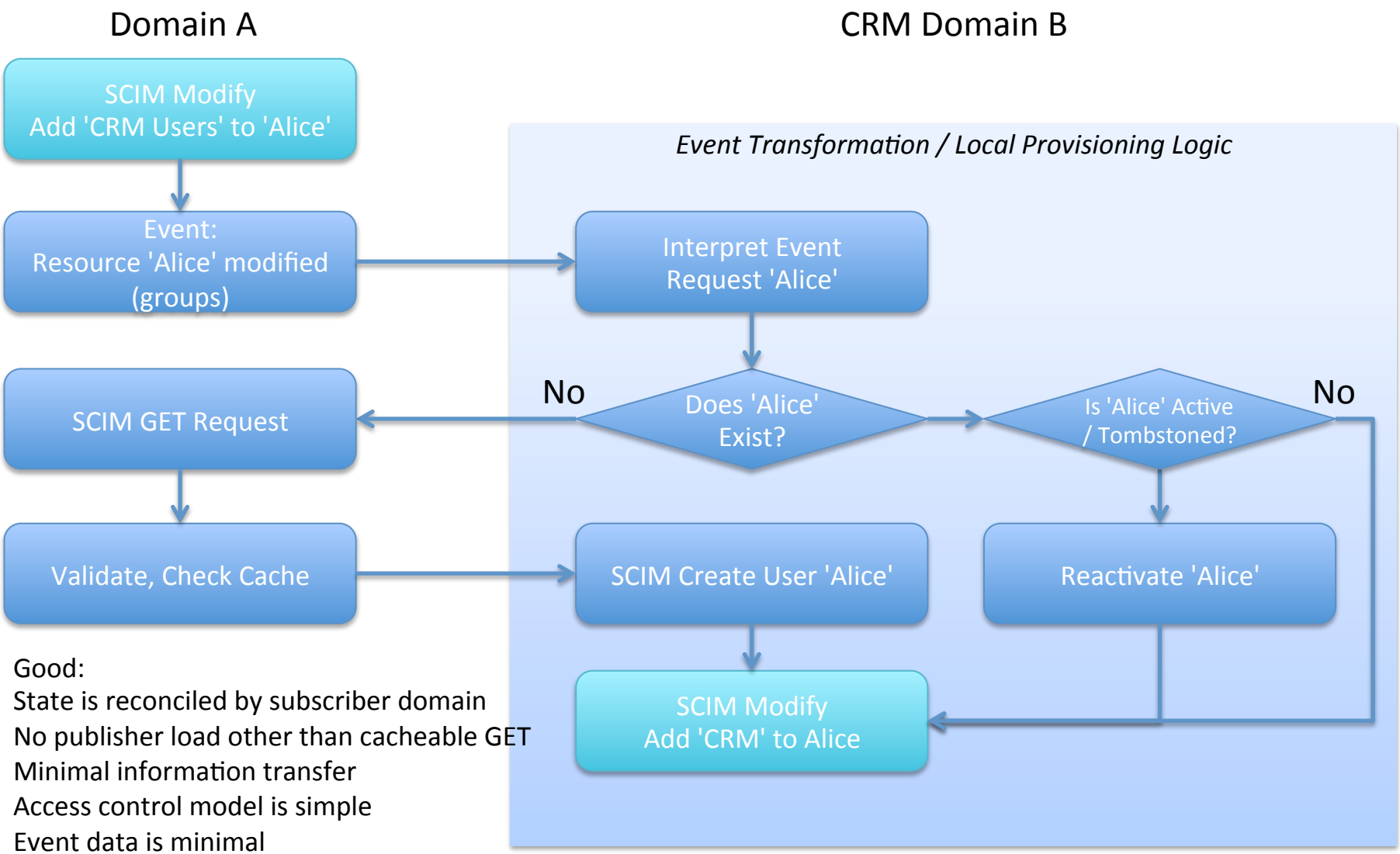
Bad Assumptions:

- Domain A Users == Domain B Users
- Domain B can copy domain A events 1:1
- A and B are same enterprise 'tenant', all data can be the same

Cause:

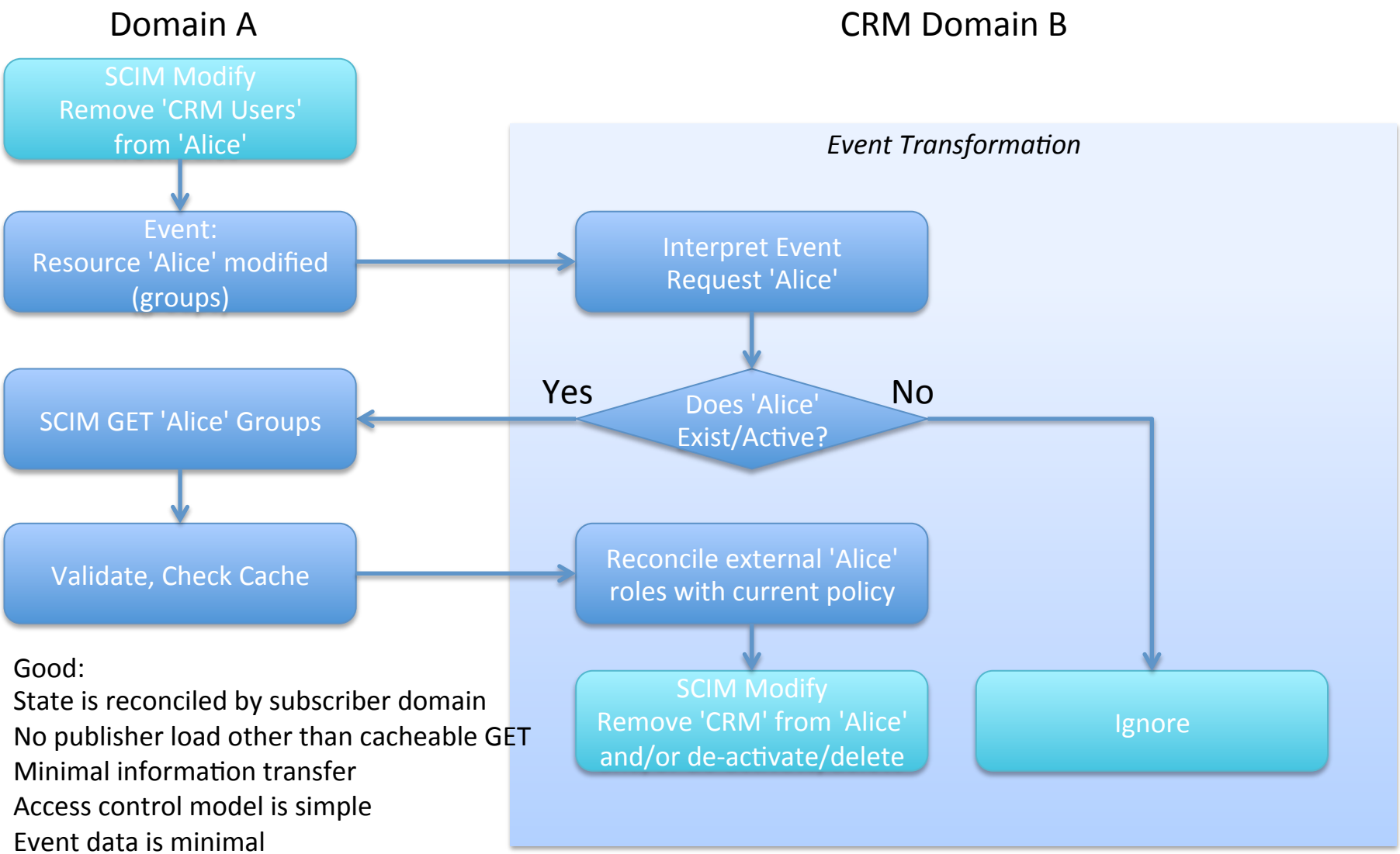
- Domain B only keeps data it needs
- Schema will vary by domain
- Life-cycles of resources vary by domain
- Transactions MUST transform

Scenario 1 Flow – Notify Style



Good:
State is reconciled by subscriber domain
No publisher load other than cacheable GET
Minimal information transfer
Access control model is simple
Event data is minimal

Scenario 2 Flow – CRM Revoked



Good:
State is reconciled by subscriber domain
No publisher load other than cacheable GET
Minimal information transfer
Access control model is simple
Event data is minimal

Scenario Observations

- Control / Authority
  - Ownership or authority of "Users" may change over time
    - Shifting center of authority
    - Corporate and service restructuring
  - User population will vary by domain
  - Different domains have different life-cycles and policies

Observations 2

- "Schema"
  - Each each administrative domain may have different justified use of attributes
  - Cloud based apps use data on need-to-know
  - There are many new attributes and applications in cloud that are not part of enterprise directory
    - MDM, MAM, are all new vs. Legacy Windows

Cross-Domain Use Cases

- Cloud-to-Enterprise
  - Pass changes to attributes in cloud back to enterprise domain
  - Real-time and polling
  - Challenge: co-operative reverse provisioning, cross-tech platform (SCIM to LDAP?)
  - Identity "sync" oriented
- Cloud-to-Cloud (tenancy-to-tenancy)
  - Hub-to-hub / Each side has independent changes
  - Event based provisioning life-cycles
  - Bi-directional attribute flows
  - Real-time and polling updates
  - Challenge: security, scale, feeds may contain millions of users.

Internal Domain Cases

- Web-Application Notification
  - E.g. Cache Invalidation
  - The ability to notify a subscriber that data has changed in order to invalidate the subscriber's cache and/or update it
  - Challenge: ability to customize information in event
- Mobile Notification
  - Client needs to be notified of profile or entitlement change
  - Challenge: scale - millions of subscribers using single-resource feeds, non-HTTP delivery (e.g. APNS, GMS, WNS)

Proposal to SCIM WG

- Develop a protocol for supporting publish/ subscribe feeds
- Describe
  - SCIM Feeds (e.g. what Users in a particular feed?)
  - SCIM Events
    - Types (POST/PUT/PATCH/DELETE + Add/Remove from Feed + Other)
    - Format (e.g. JWT)
    - Security/Confidentiality Model
  - Profile or Create an Event Distribution Protocol
    - e.g. Derivative of PubSubHubub, WebPUSH, etc