SEC Events Use Cases Discussion

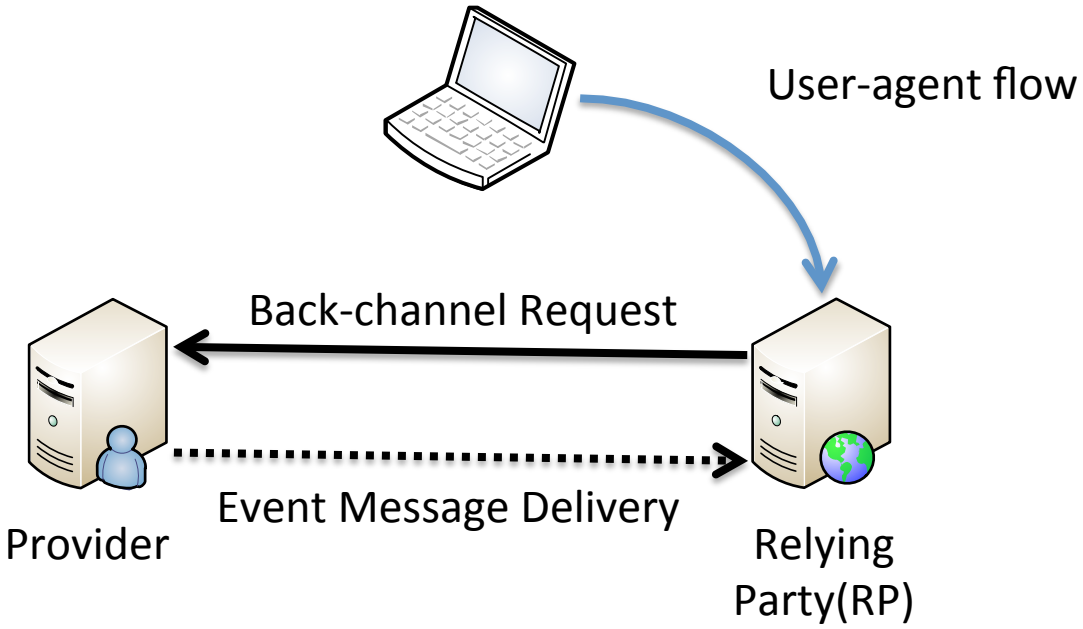
IETF 98, Chicago
Mar 29, 2017
Phil Hunt
(draft)

Agenda

- Network Relationship Cases
- Requirements
- Profile Cases

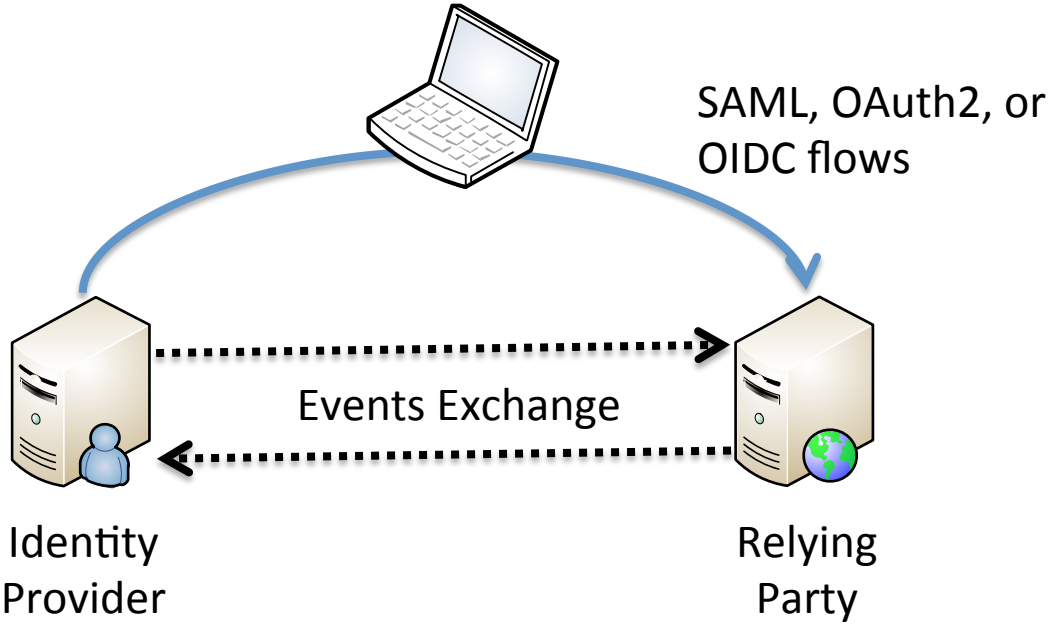
NETWORK RELATION CASES

Notes About Diagrams



- Arrow heads indicate HTTP Request direction (response is assumed)
  - Indicates request or event receiver
- All solid lines are typical HTTP Request & Response
- Blue line – Flow through user-agent
- Black line – Backchannel flow, may be synchronous with UA flow
- Dotted line – Event Stream
  - Usually HTTP (Response only indicates successful SET delivery)
  - Events not linked (not responses), but triggered
  - Events delivered asynchronously, OOB, compared to solid lines

Explicit Federation

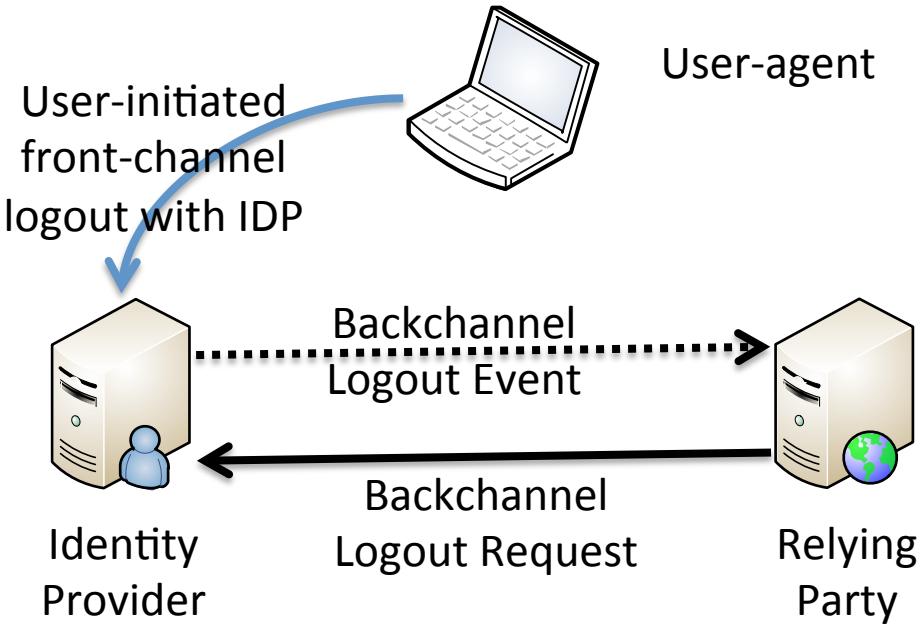


1. User logs into an RP using an IDP (OIDC, SAML, OAuth)
2. User may explicitly consent to events exchange
3. IDP sends session events and account state events in backchannel
4. RP sends suspicious activity, assoc, logout events in backchannel

Observations:

- Explicit consent possible
- Many RPs for every IDP
- Some IDPs monolithic (Google), and some tenancy based (Oracle)

Logout Events

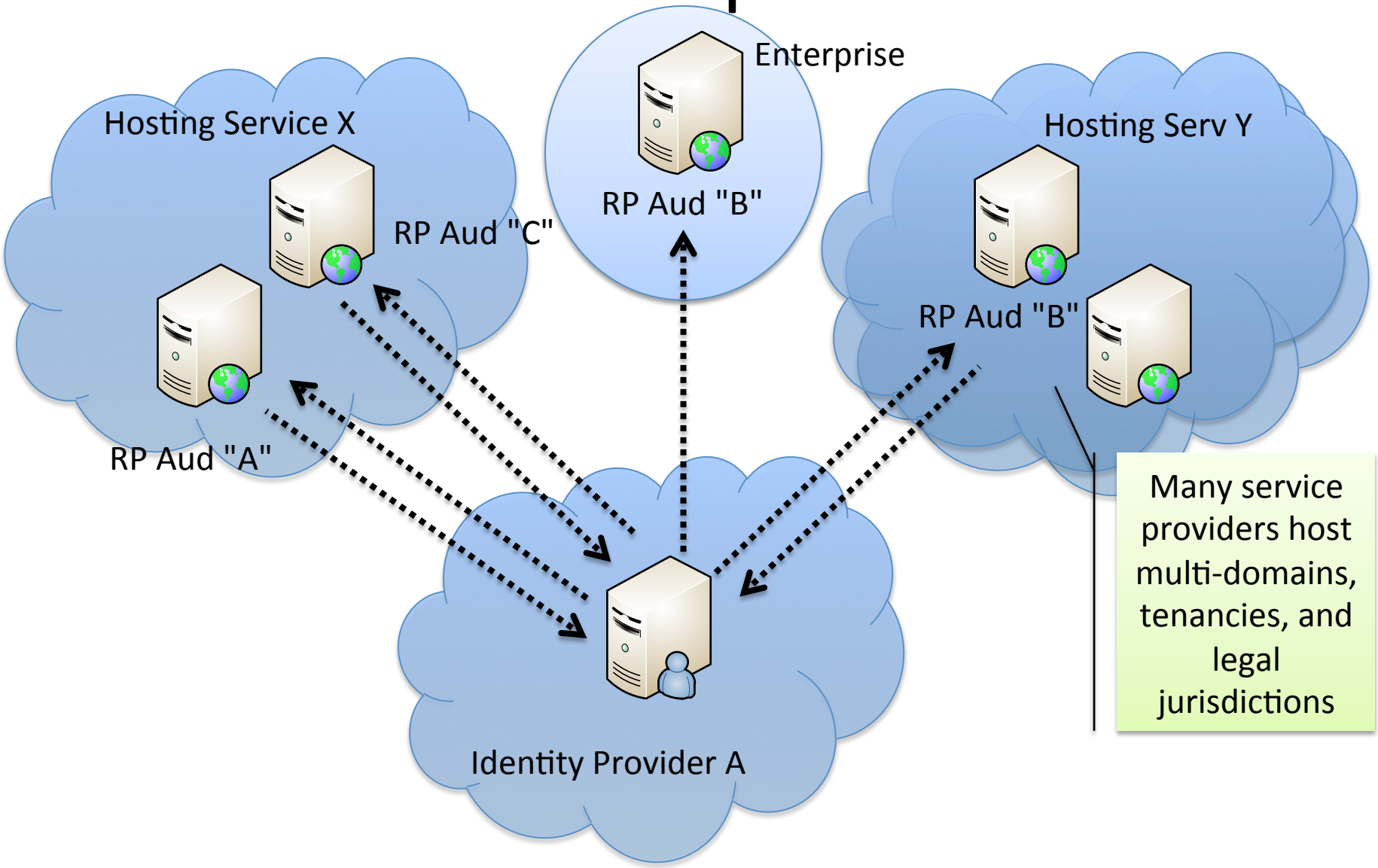


1. User initiates at OP, or RP initiates by calling backchannel logout
2. OP marks session as revoked and issues Event to relevant RPs

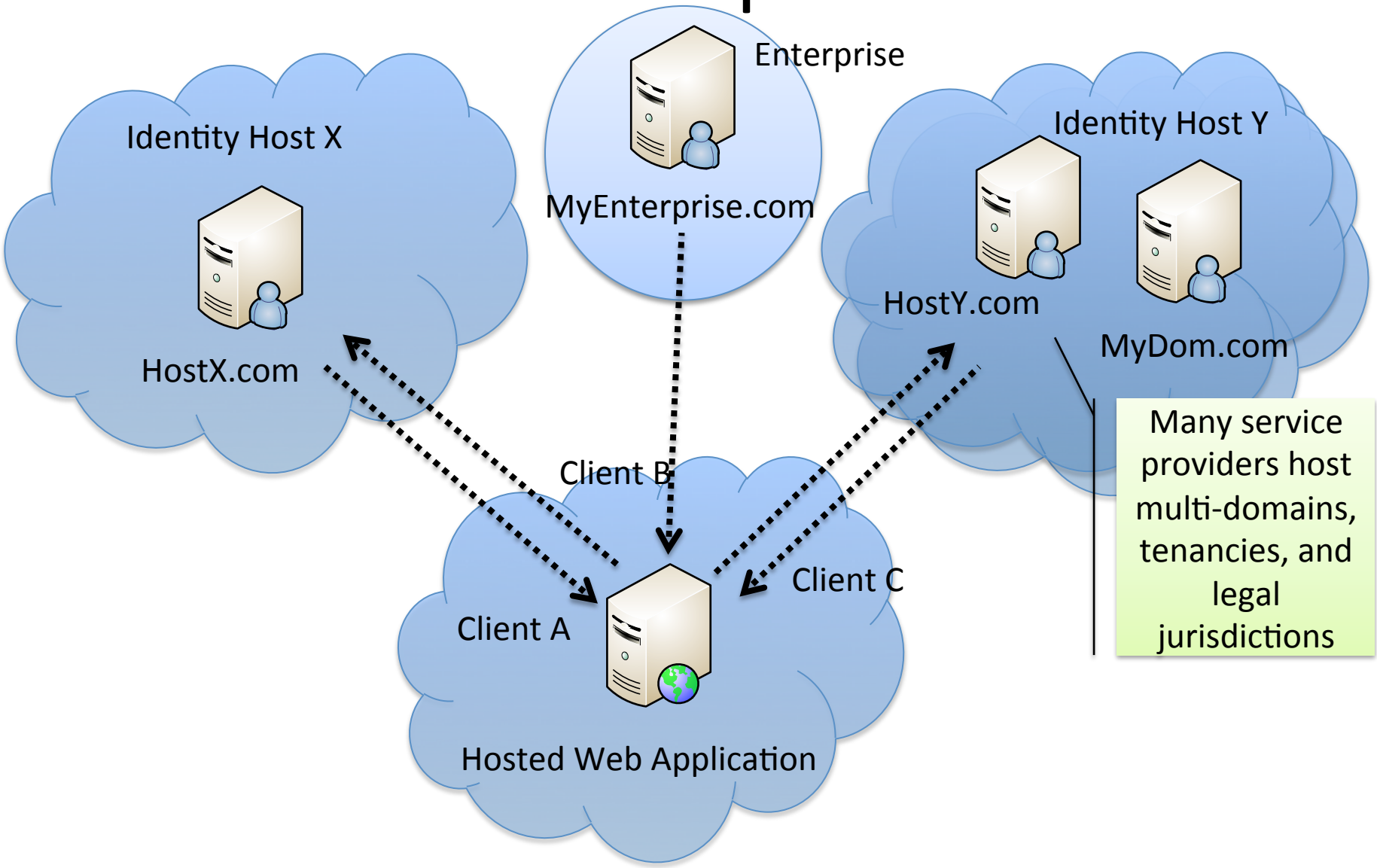
Observations:

- There may be a many RPs notified for a particular session logout
- Current draft does not support sign-out at RP and reverse event (TBD)

Federation Perspective - IDP

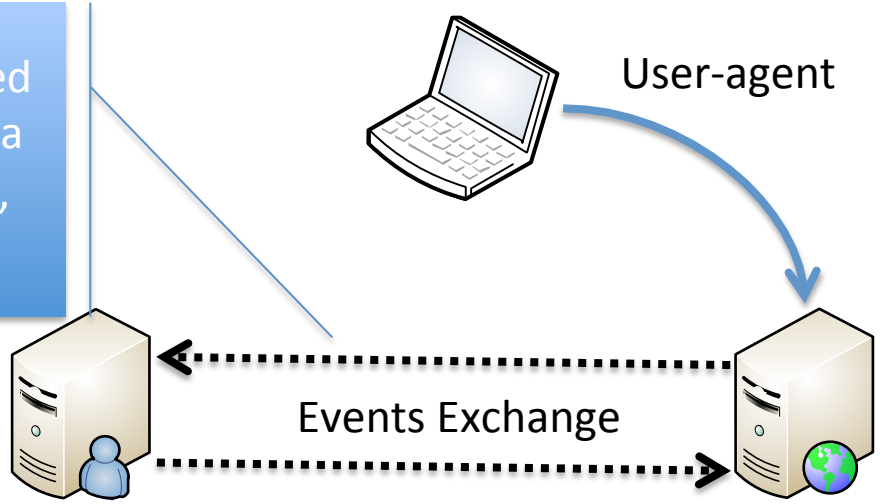


Federation Perspective - RP



Implicit Federation

EPs and RPs are linked by data and NOT by a protocol (e.g. email, telephone num)



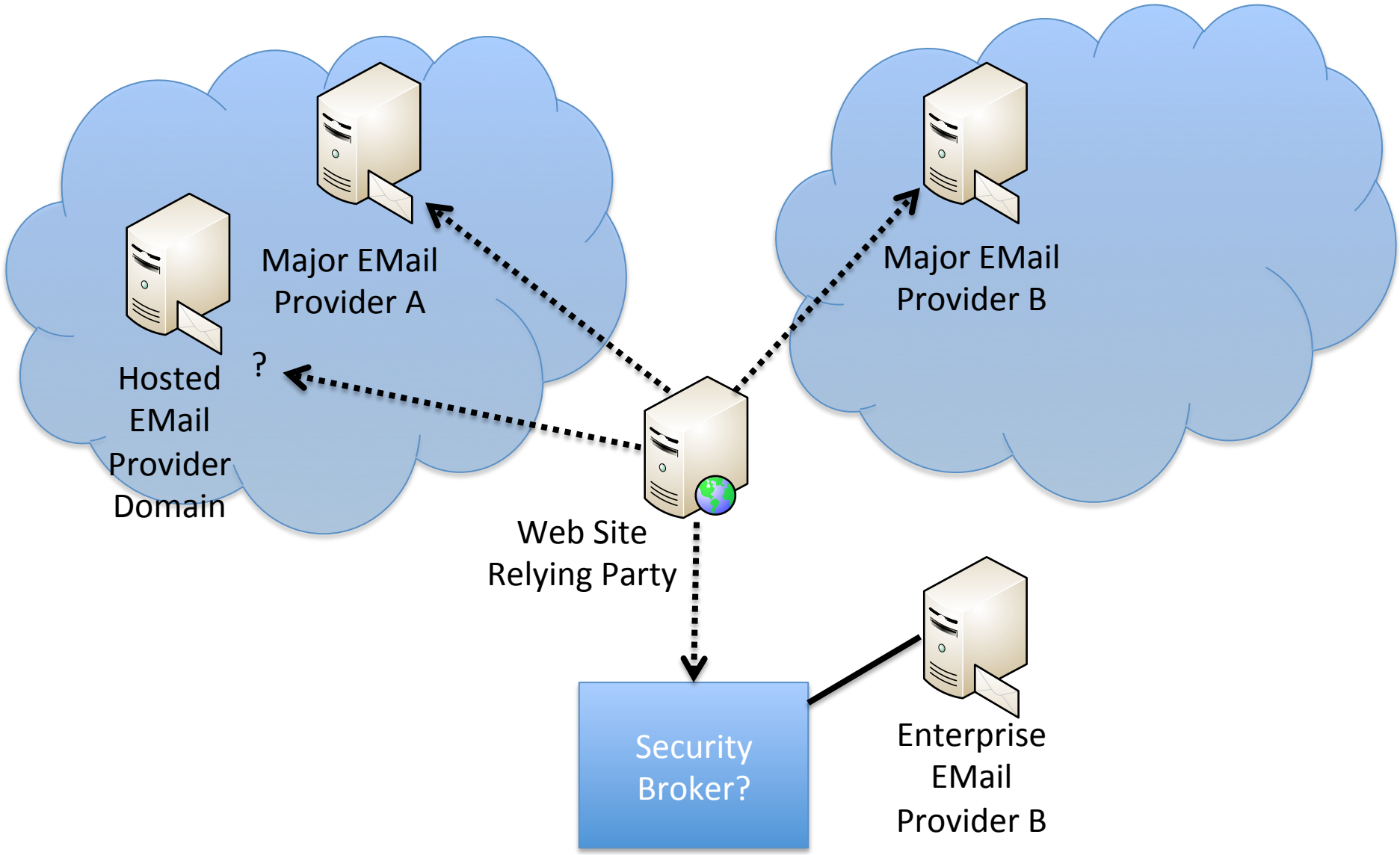
1. User creates account on RP using an email, telephone number, etc
    - Email provider(EP) not involved initially
2. Subsequently, RP sends EP an Assoc Event/Cmd (tbd)

Later:

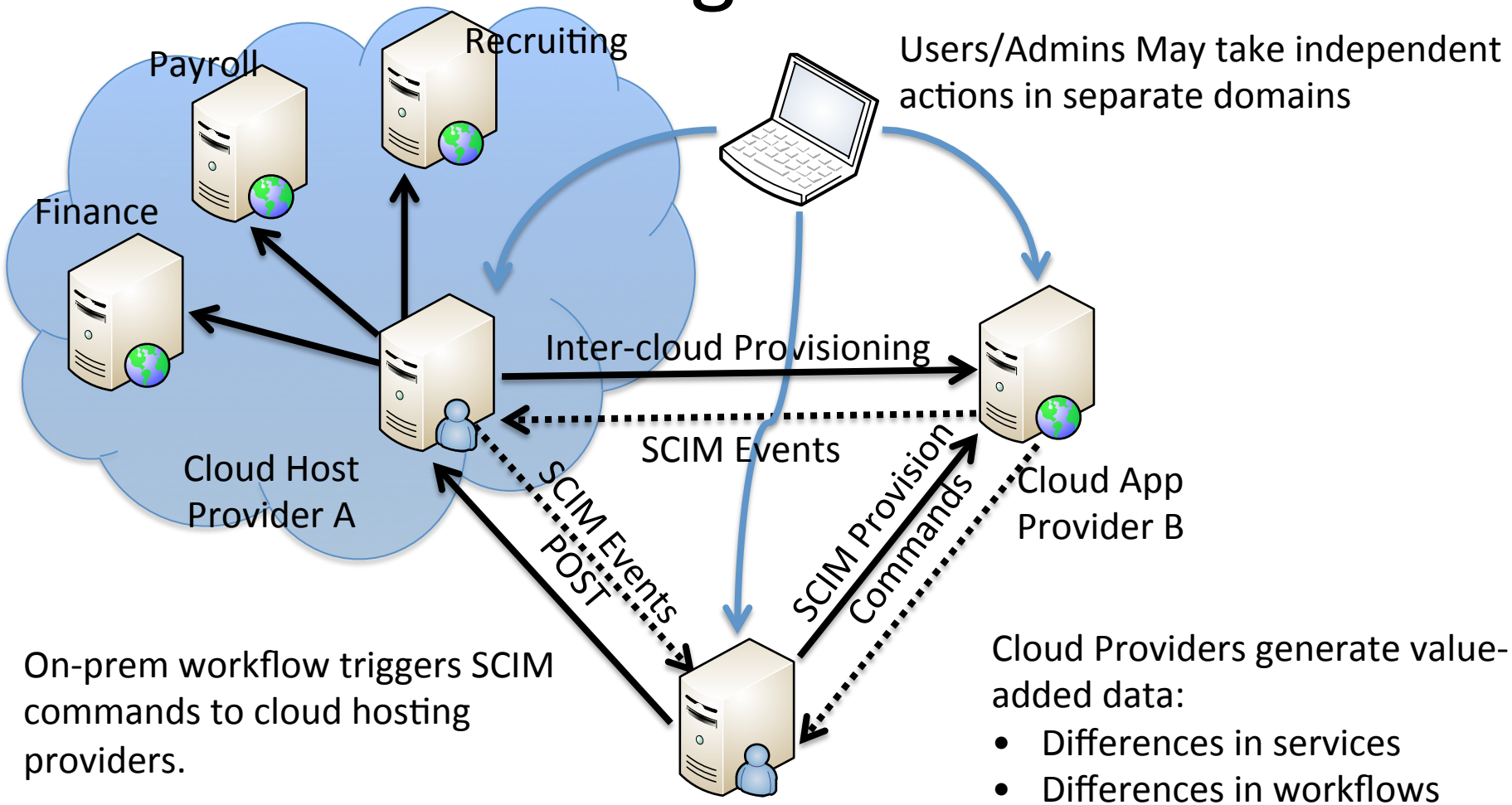
A. RP sends suspicious activity, recovery events to EP
    - May be in backchannel or as header in recovery Email
    - EP may require stronger user challenge before granting access to email

B. EP gives account state change (takeover, suspension) events to RP

Implicit Network Relationships



Provisioning Events - POST



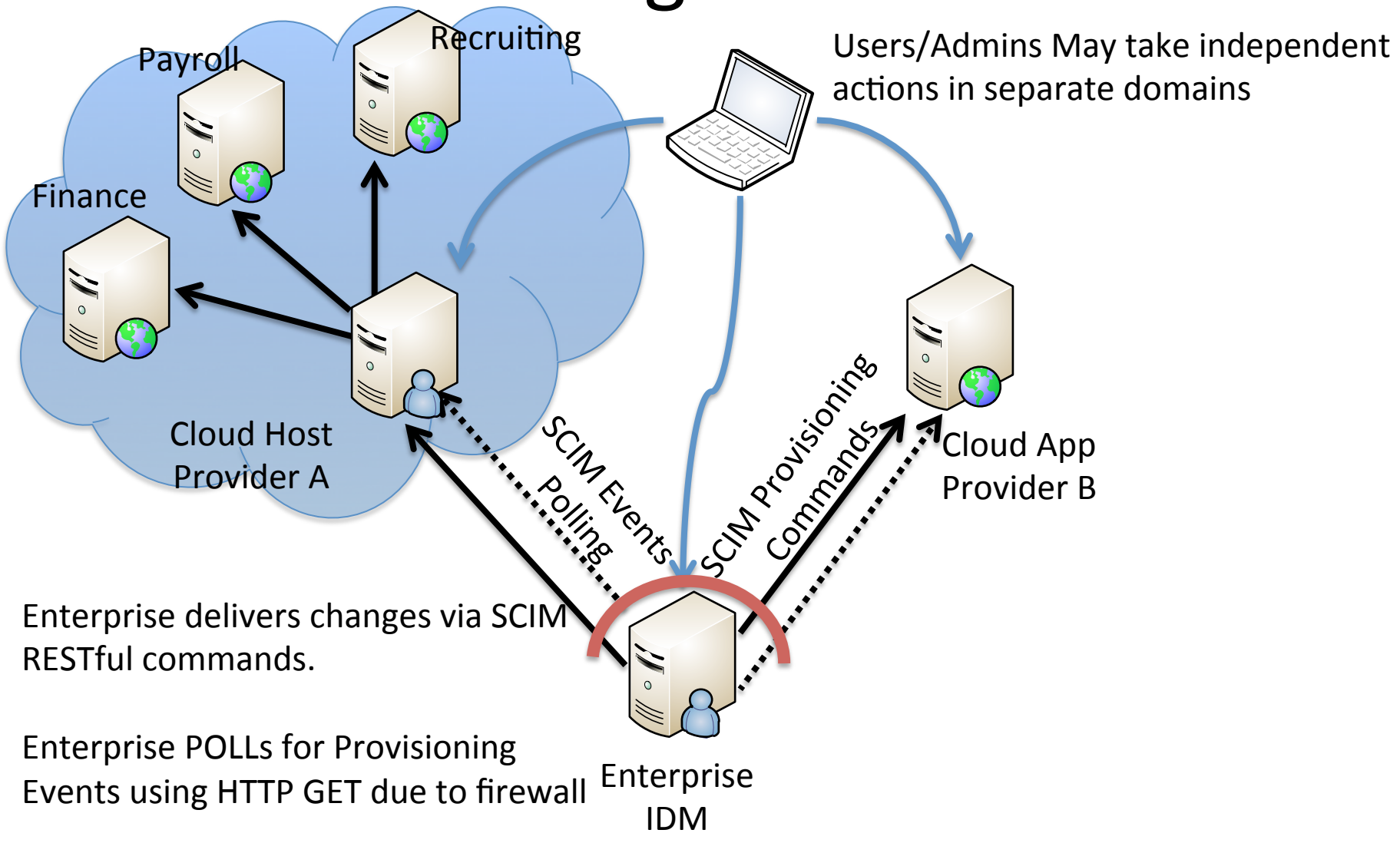
On-prem workflow triggers SCIM commands to cloud hosting providers.

Changes that occur in cloud are signalled back to enterprise via SCIM Events for reconcilliation

Cloud Providers generate value-added data:

- Differences in services
- Differences in workflows
- Differences in control
- Difference in state (min PII)

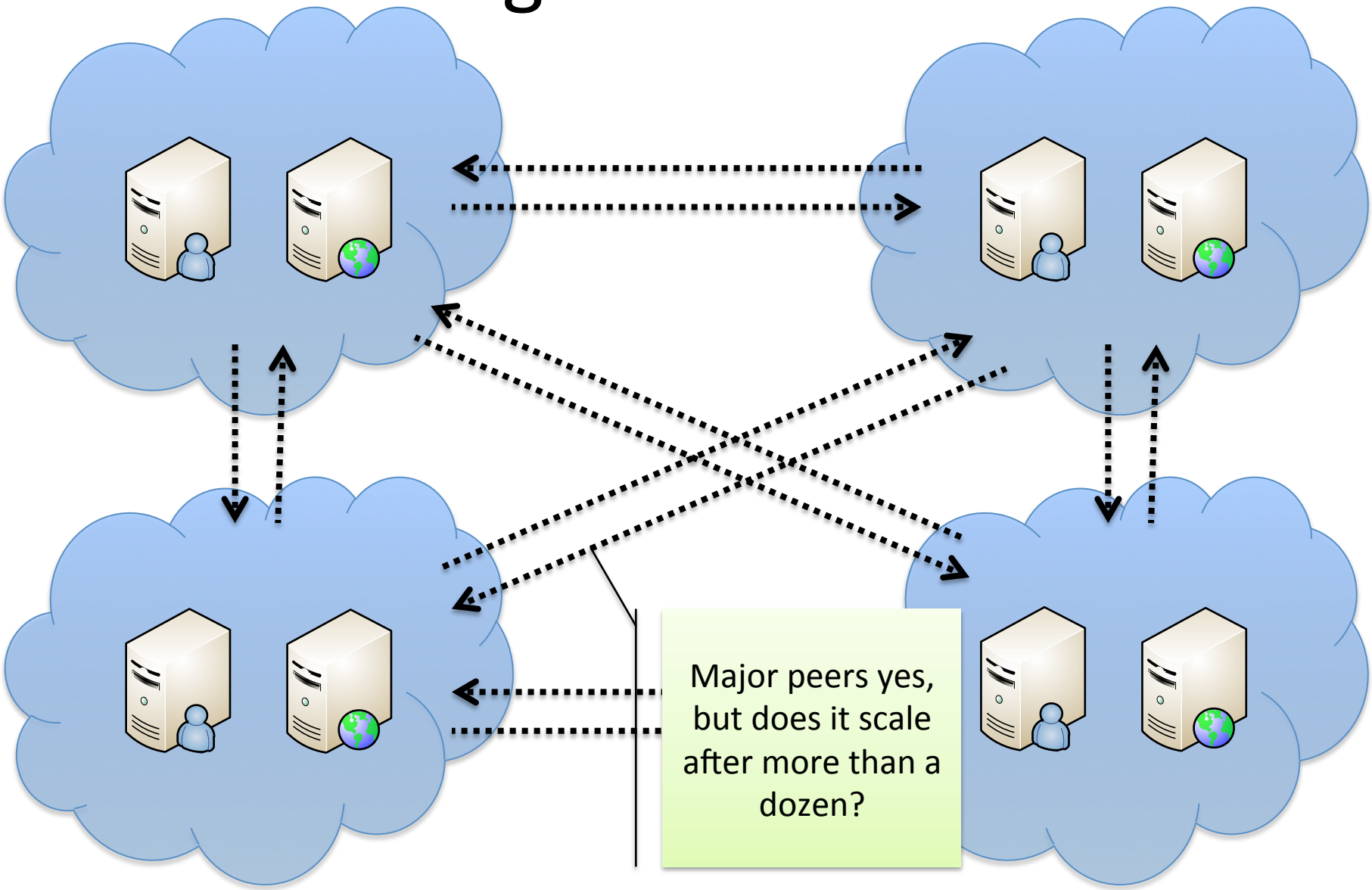
Provisioning Events - POLL



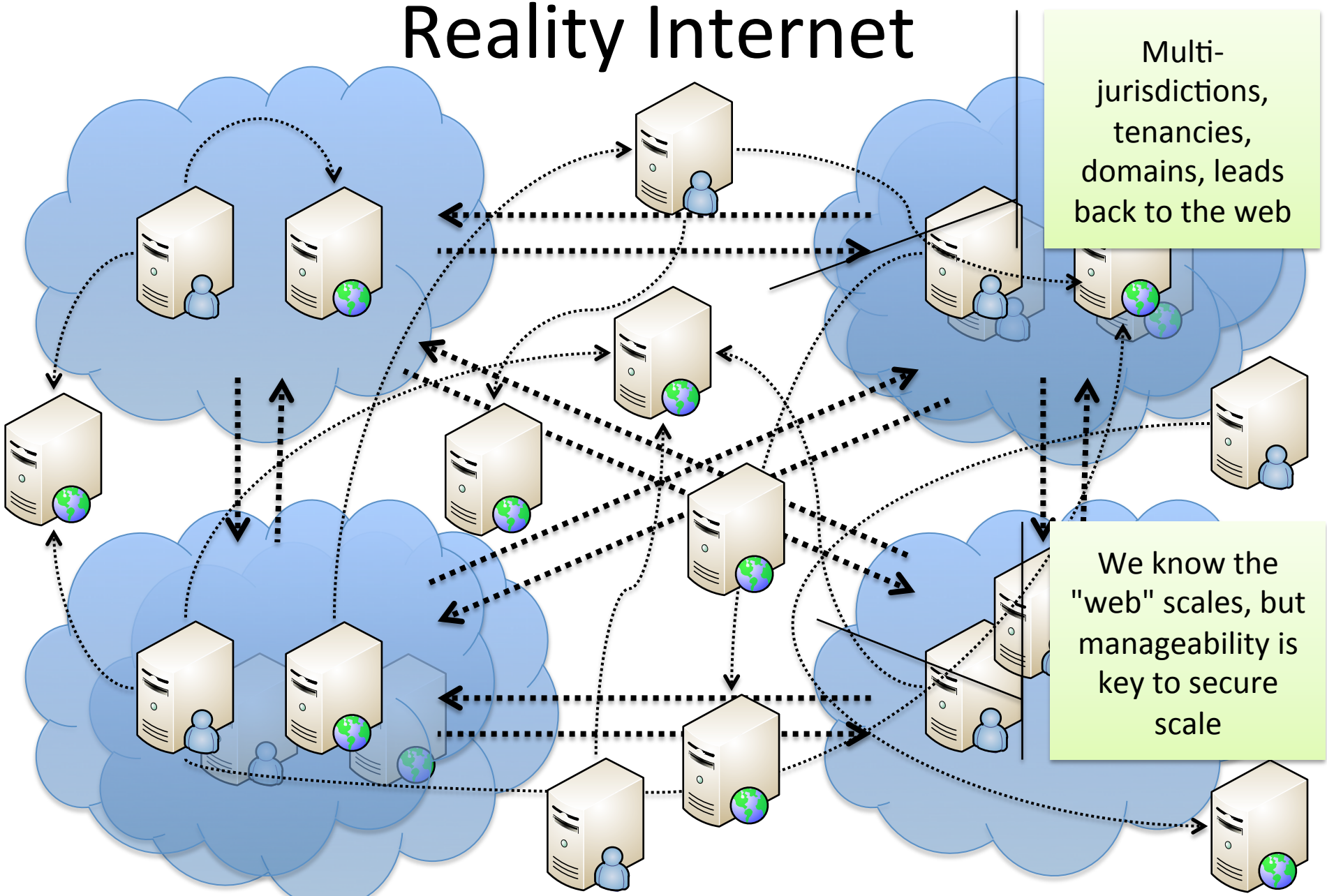
Enterprise delivers changes via SCIM RESTful commands.

Enterprise POLLs for Provisioning Events using HTTP GET due to firewall

Sharing Between Peers



Reality Internet



Multi-jurisdictions, tenancies, domains, leads back to the web

We know the "web" scales, but manageability is key to secure scale

REQUIREMENTS

Requirements

- Method of transfer − Data Plane
  - A common way to deliver messages over a Stream
  - Optional Assured Delivery
    - Receiver's choice
- Deploy: Method to configure streams
  - Endpoints, security, crypto etc
- Check: Method to detect/prevent missed SETs
  - How does receiver know if it missed events?
  - Has the transmitter been unable to deliver?
  - Can receiver pause SET delivery to facilitate operational issues to avoid loss?

Requirements Cont'd

- Update: Method to update Stream configuration
  - Key rotation (issuer or receiver)
  - Authorization updates
  - Pause or stop stream

- Manage Content:
  - What event types?
  - What entities/subjects are in the stream?
    - How does a client negotiate the events it wants?
      - Control Stream updates? or Data events?

EVENT TYPES

RISC Event Types

- TBD: Variable subject identification?
- Account Status Changes
  - Account Secured due to suspected compromise
  - Suspended – by owner / by provider
  - Reactivated – by owner / by provider
  - Deleted – by owner / by provider
  - Reissued
- Account State Change
  - Password change
  - Session(s) / Token(s) revoked
  - Recovery email/phone changed
  - Public identifier changed
  - 2nd factor added

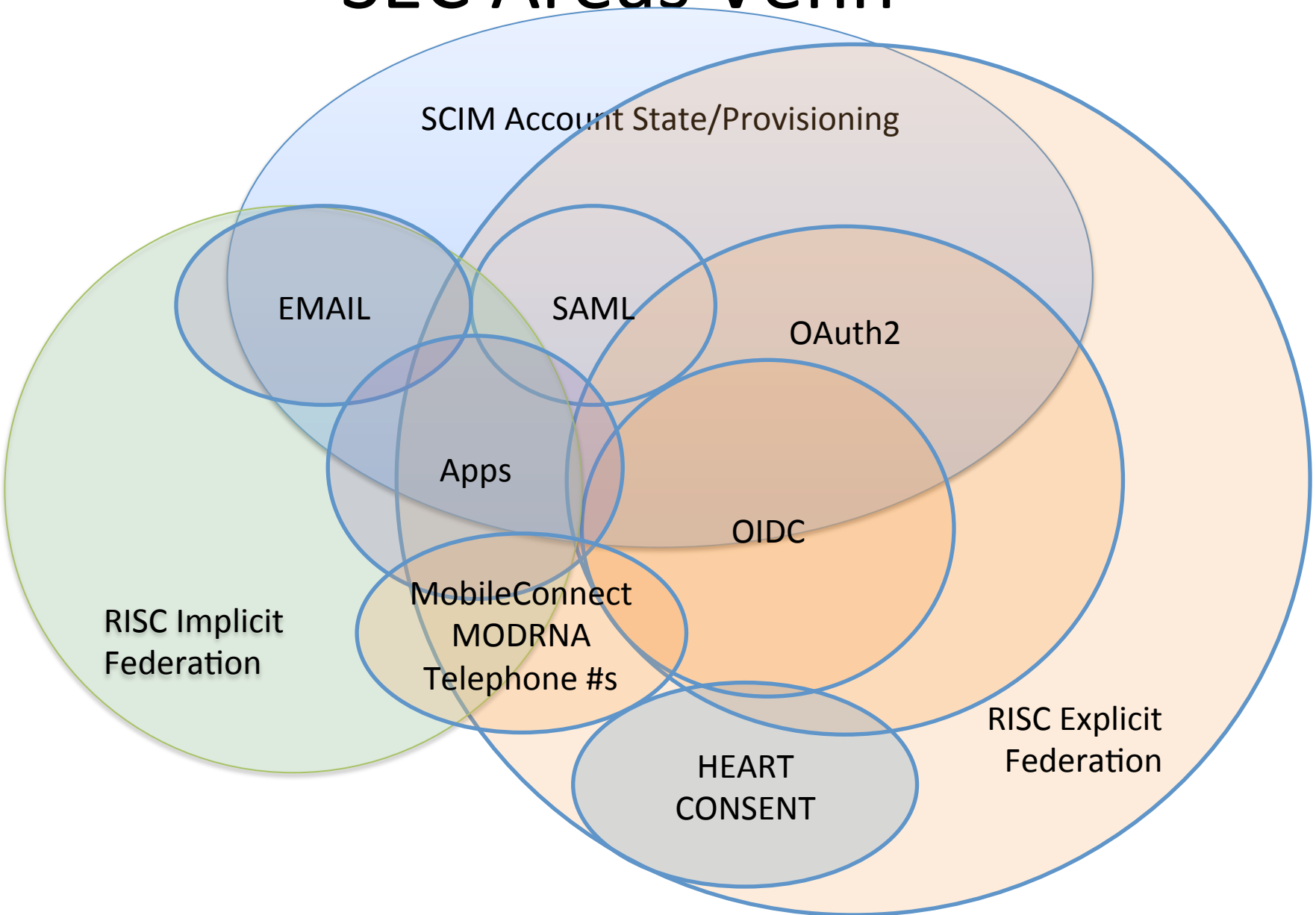
SCIM Events

- Subjects defined by URI
- Low-level Resource Level
  - Created, Modified, Deleted
- Account Status Changes
  - Account Secured due to suspected compromise
  - Suspended / Reactivated
  - Reissued
- Account Change
  - Password change
  - Session(s) / Token(s) revoked
  - Recovery email/phone changed
  - Public identifier changed
  - 2nd factor added

Event Types

- OIDC
  - Backchannel Logout
  - Subjects defined by "iss" and "sub"
- HEART
  - Consent (TBD)
- OAuth2
  - Token Revocation Event (complement to RFC7009)
  - Subjects defined by "jti" and optional "sub"

SEC Areas Venn



SEC Event Examples