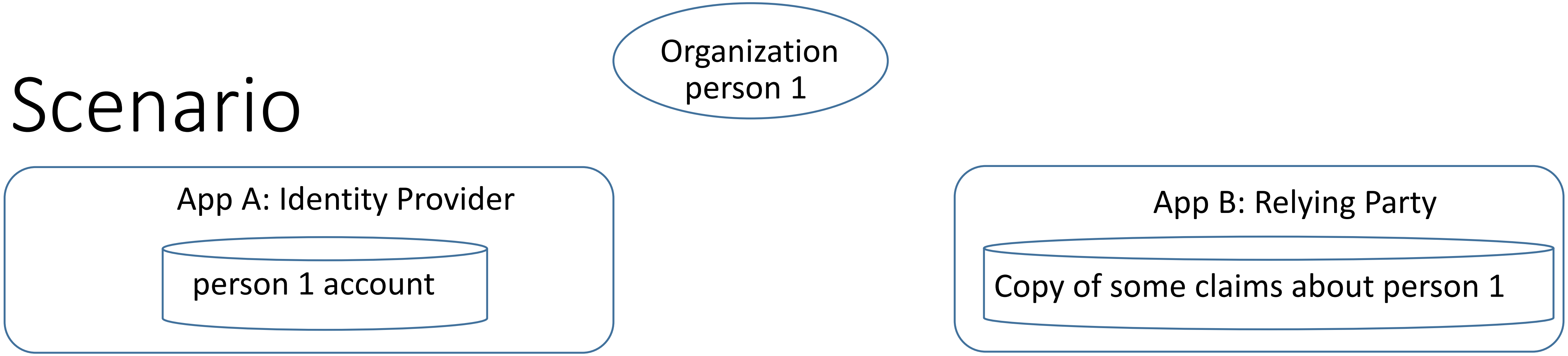
Proposed SCIM profile for improving interop in a typical Internet scenario

Mark Wahl

Microsoft Corporation

May 2021

Scenario

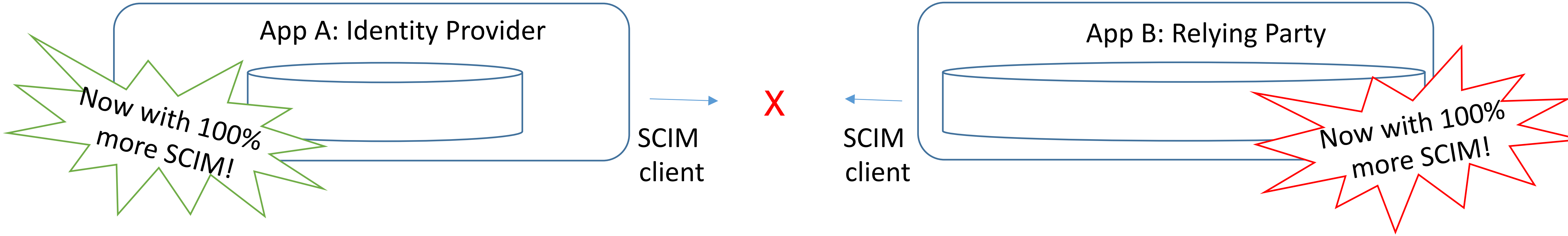


- An organization is using two apps, app A acting as an identity provider that is authoritative and another app B that is acting as a relying party
- Person 1 should be able to sign into relying party B,
  with claims originating from their account in identity provider A

  ➔ Well-known SSO, implementable with SAML, OAuth/OIDC, …
- Changes related to person 1 account occurring in identity provider A
  should be sent on an ongoing basis to relying party B, so that relying party B
  can keep its state about that person up to date. (Cache consistency)

  ➔ Can be addressed using SCIM, if both A and B support SCIM

Problem

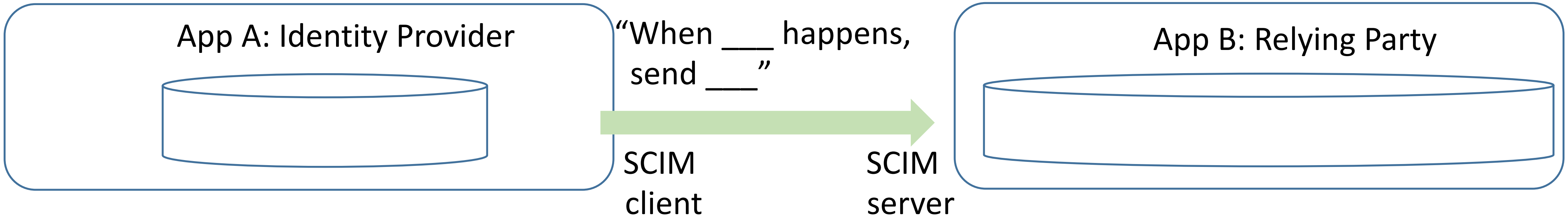


- Any implementer can read the IETF SCIM protocol and schema RFCs and “add SCIM” to their application. That’s good but…
- I’ve observed that when two implementers each independently read the same RFCs, they do not implement complementary set of SCIM capabilities
  - When they try to connect their apps for the first time, even though they are both trying to achieve a compatible goal in that scenario, the outcome is that they do not interoperate without

Investigation

- RFC 7643 and 7644 are intended to cover many scenarios, and so leave choices open to implementers – features intended for one scenario may not be applicable or relevant to another
- Most implementers, when presented with a choice will choose one option, e.g.
  - Build a SCIM server? Or SCIM client?
  - How to handle authentication?
  - Support PUT? Or PATCH? Sorting? eTags? /me? Groups?
  - How many simultaneous requests?
- Implementers new to SCIM may not be aware of common IETF assumptions, e.g.,
  - Robustness principle vs anti-fuzzing for security
  - What does "MAY" mean - RFC 7643 has 62 "MAY", RFC 7644 has 77 "MAY"…

Proposal



- An RFC that is a profile of SCIM for this scenario: a list of the specifics for how implementers of this scenario should implement SCIM in either an identity provider or relying party to maximize interoperability
  - The events that result in a SCIM message being emitted by the identity provider, and what the relying party is expected to respond
  - Use MUST and SHOULD to state minimum requirements for interoperability in the payload generation and processing
  - List the parameters that two implementers must agree upon, such as the endpoint URI of the SCIM server, or authentication credentials

Expired Internet-Draft

- https://tools.ietf.org/html/draft-wahl-scim-profile-00
  - Interoperability-improving statements: payload processing guidance, multi-tenant considerations, overlapping requests, throttling, error handling…
  - Minimum schema, and considerations for the id and externalid attributes
  - Patterns of SCIM operations on an account being added, updated, or removed in the identity provider

- Open questions
  - Reconciliation of state in relying party database with identity provider
  - Service-to-Service authentication
  - Relationship with Fast-Fed and other non-IETF activities