

OAuth 2.0 for native clients with federation

<https://datatracker.ietf.org/doc/draft-zehavi-oauth-native-clients-federation/>

IETF 125: OAuth WG
March 2025 Shenzhen

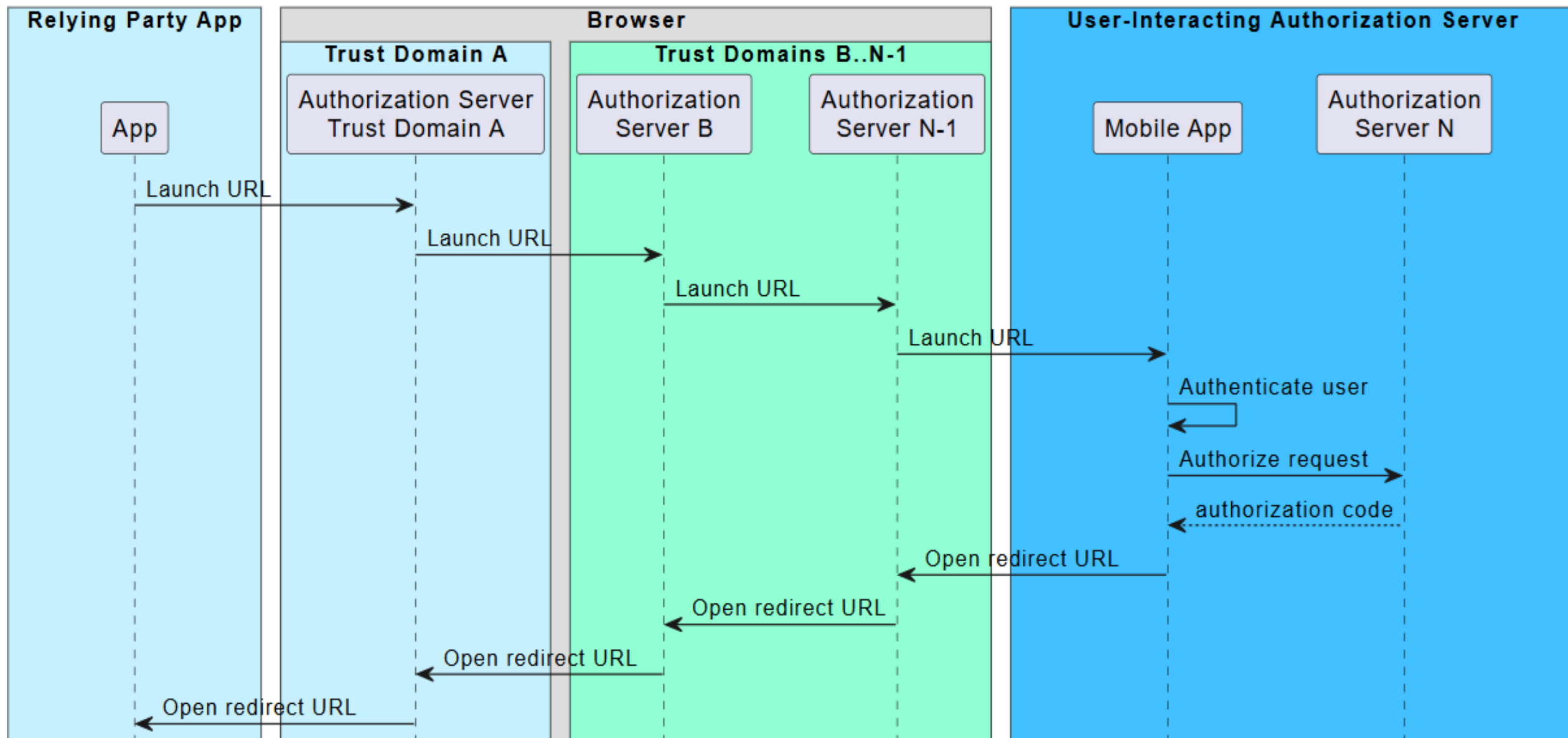
Yaron Zehavi
(Raiffeisen Bank International)

Aaron Parecki (Okta)

Recap

- App2app draft presented at IETF 123 & 124, to tackle app2app flows with federation **across trust domains**, resulting in degraded non-native UX

App2App across non-app-claimed urls requires browser

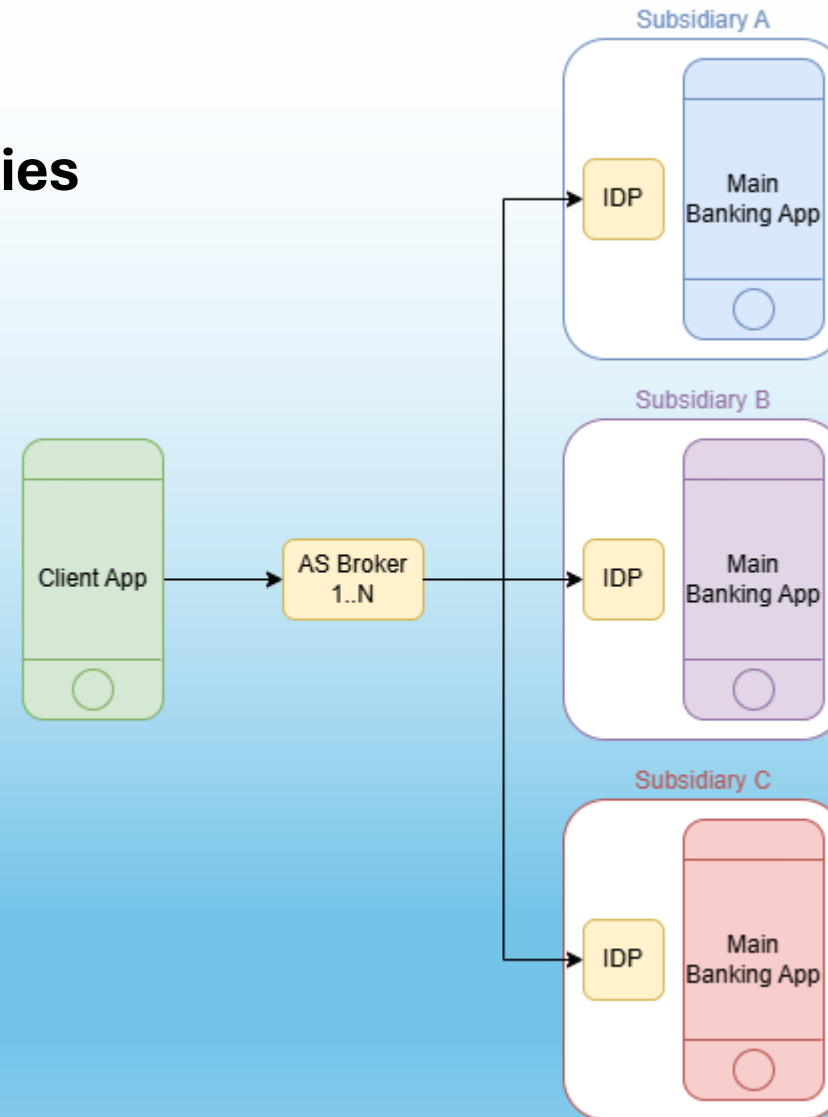


Recap

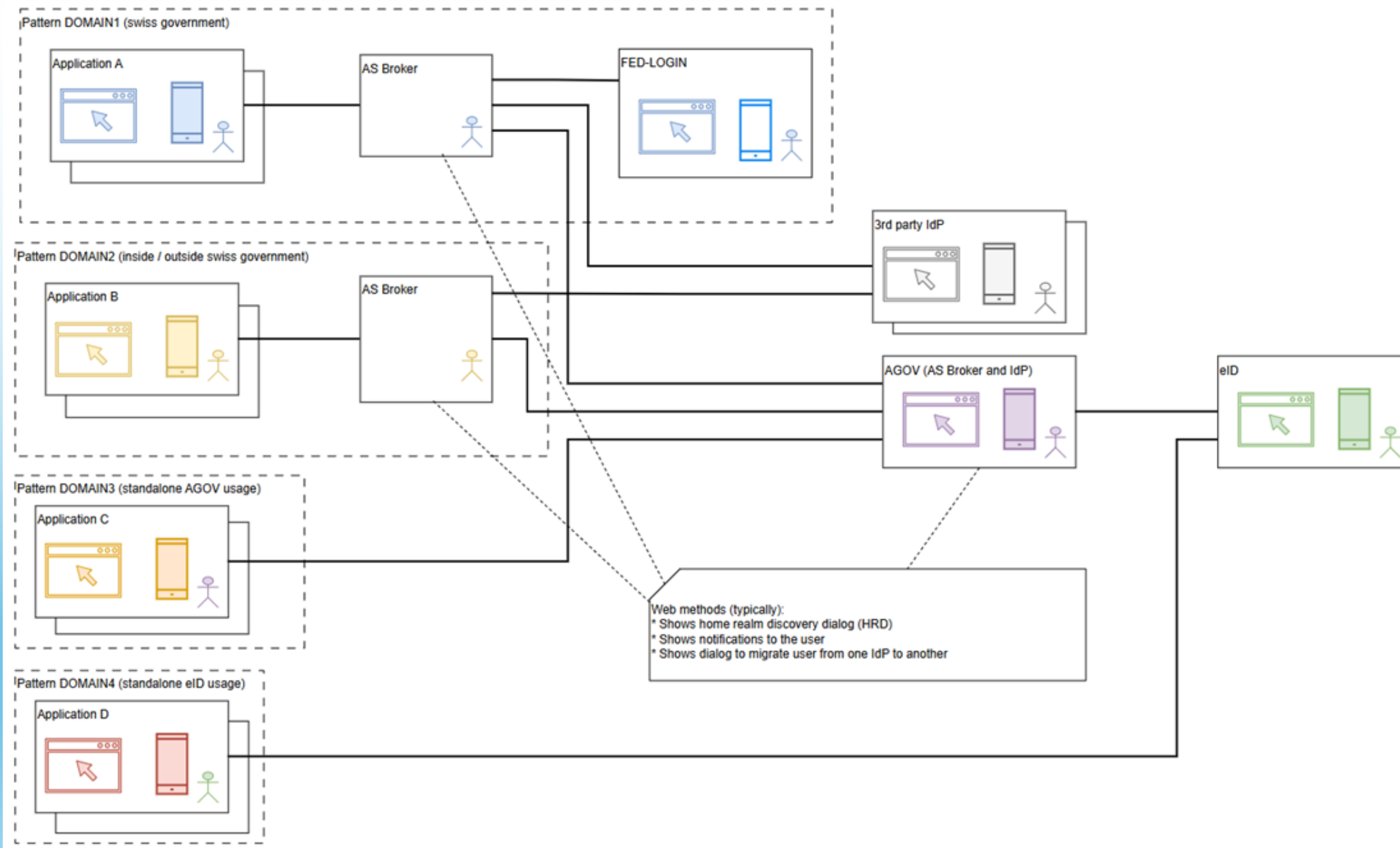
- App2app draft presented at IETF 123 & 124, to tackle app2app flows with federation across trust domains, resulting in non-native UX
- Raiffeisen Bank Int'l, Swiss government find this use-case challenging

App2App federation use case: Raiffeisen

10 Subsidiaries

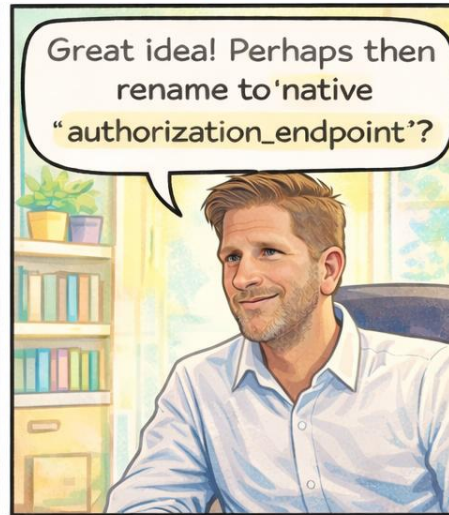


App2App federation use case: **Swiss Government**



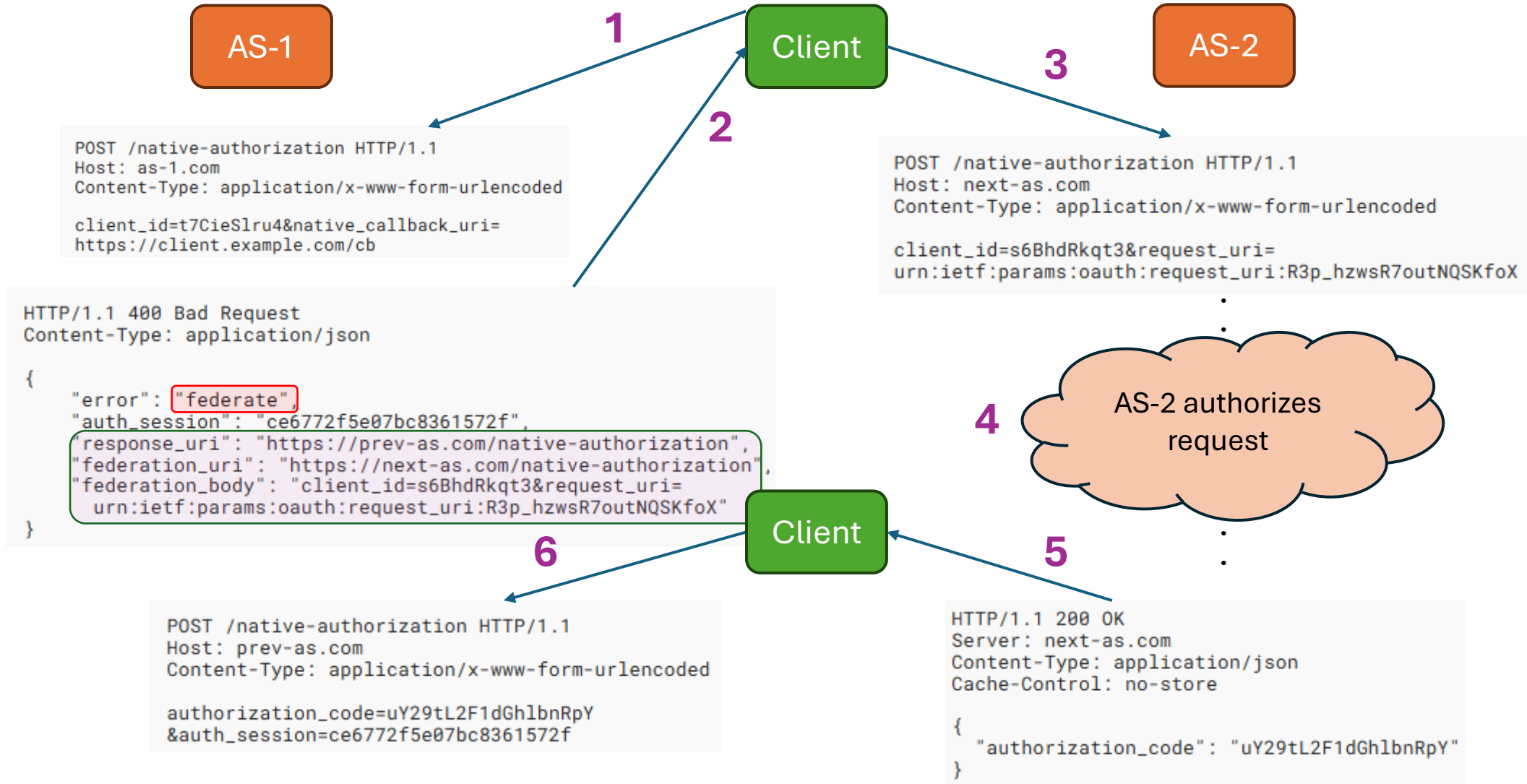
Recap

- App2app draft presented at IETF 123 & 124, to tackle app2app flows with federation across trust domains, resulting in non-native UX
- Raiffeisen Bank Int'l and the Swiss government have challenges with this use-case
- Draft introduced a new endpoint serving OAuth as an API
- IETF 124: enter Aaron...

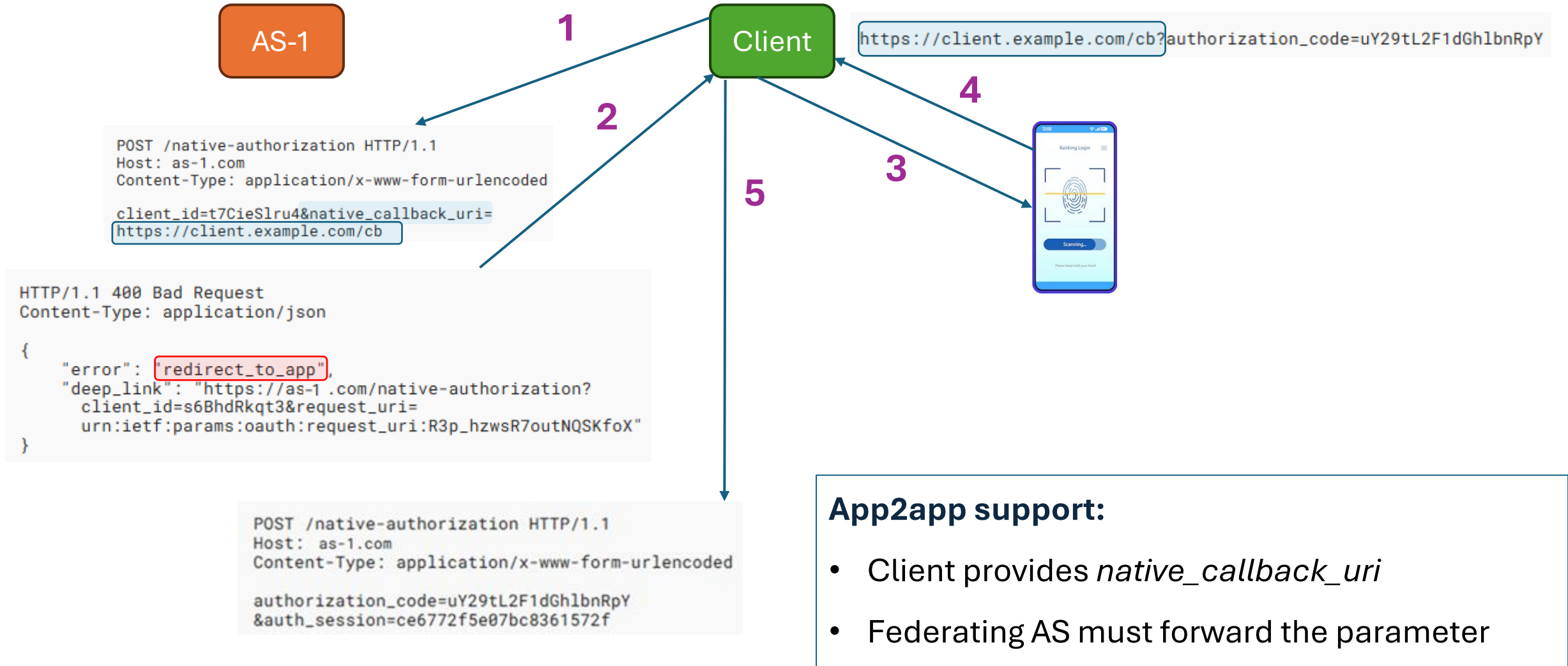


Protocol Overview: New FiPA Responses

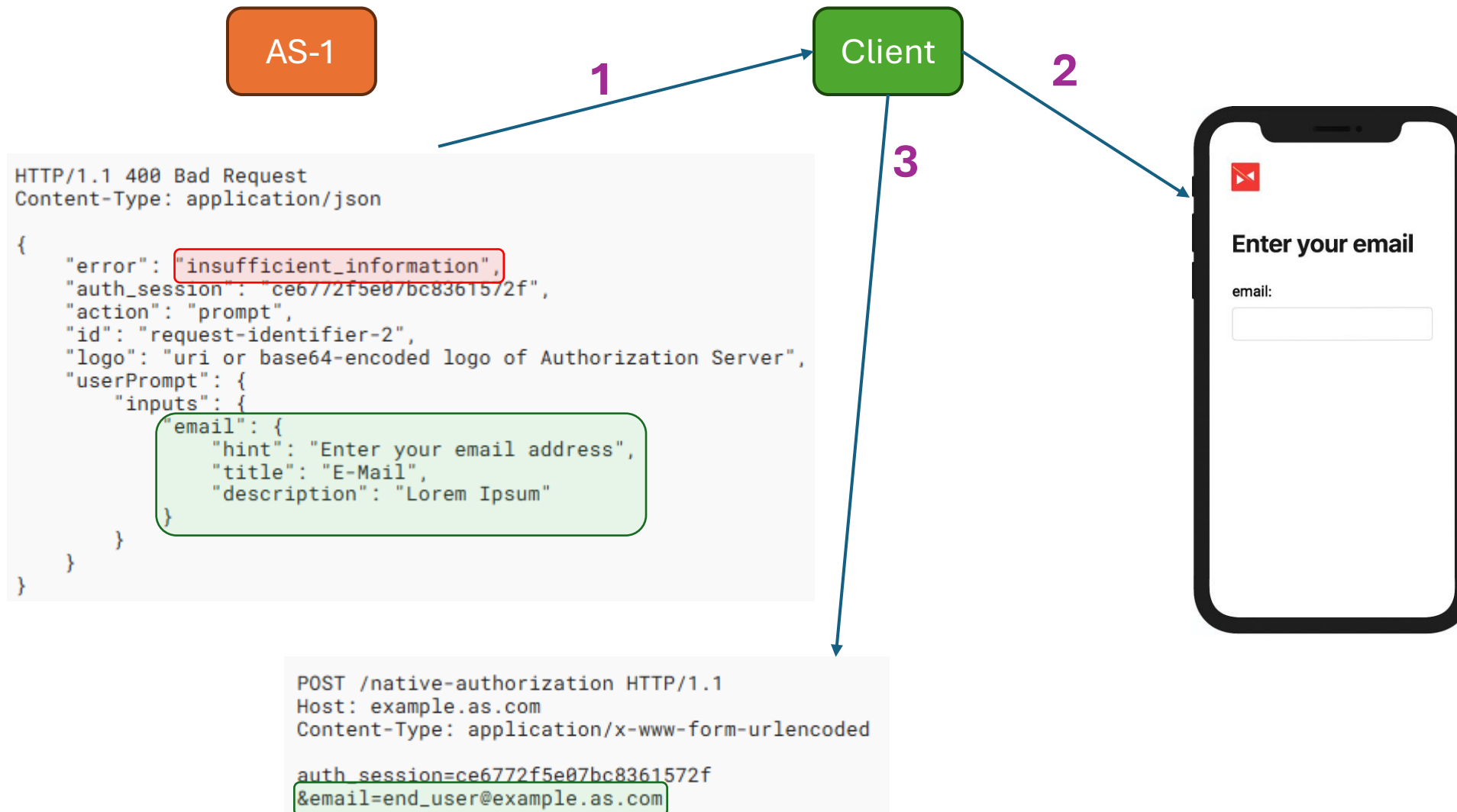
New FiPA response: federate



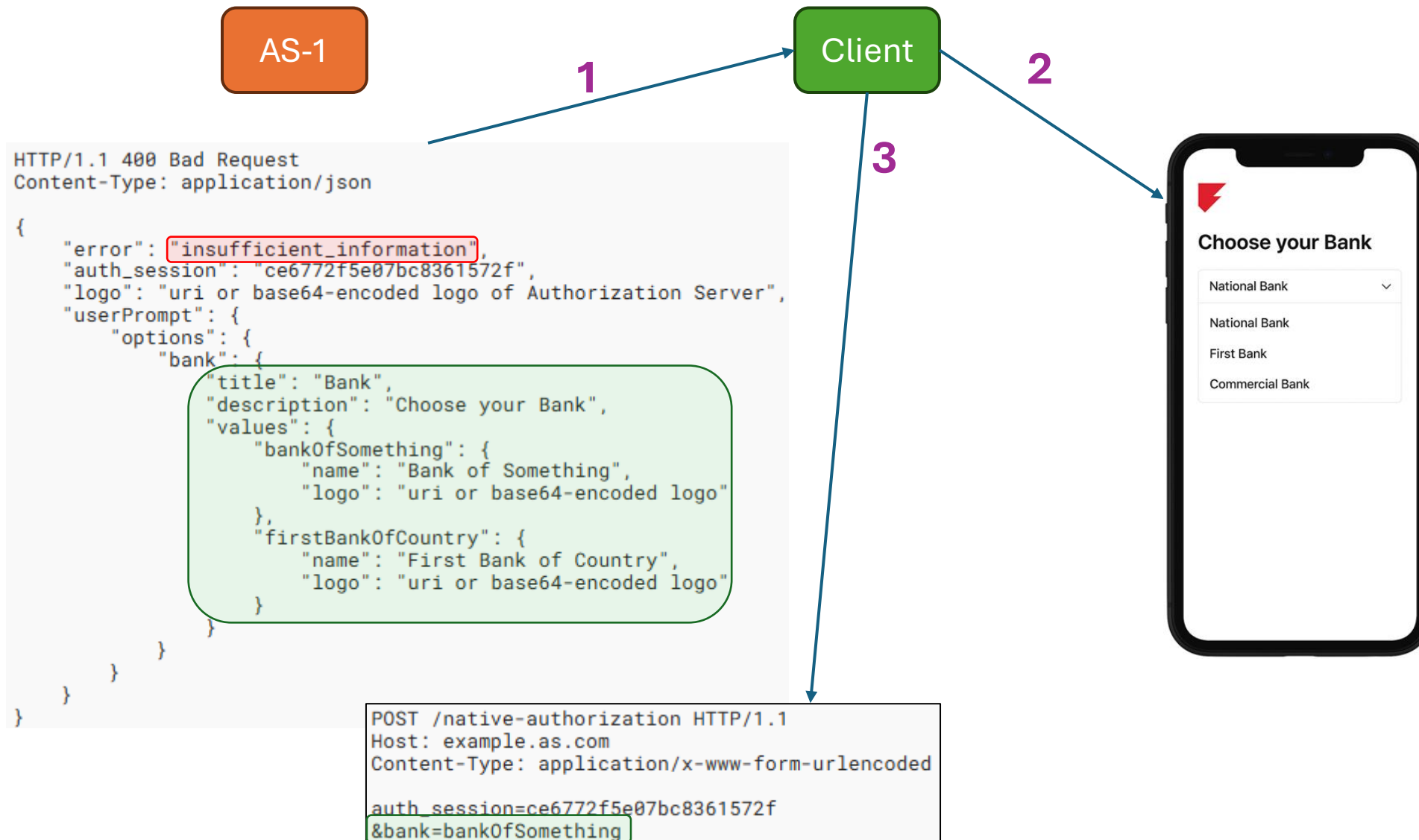
New FiPA response: **redirect_to_app**



New FiPA response: **insufficient_information**



New FiPA response: **insufficient_information**



Non-first-party native clients

- Native client can't authenticate to downstream AS → federating AS must use PAR
- Downstream AS should identify federating AS as such and:
 - Mandate PAR
 - Consider privacy of challenges served