draft-ietf-anima-brski-cloud

IETF 113 - ANIMA - 2022-03-25

Friel	Cisco
Shekh-Yusef	Auth0
Richardson	Sandelman Software Works

TL;DR

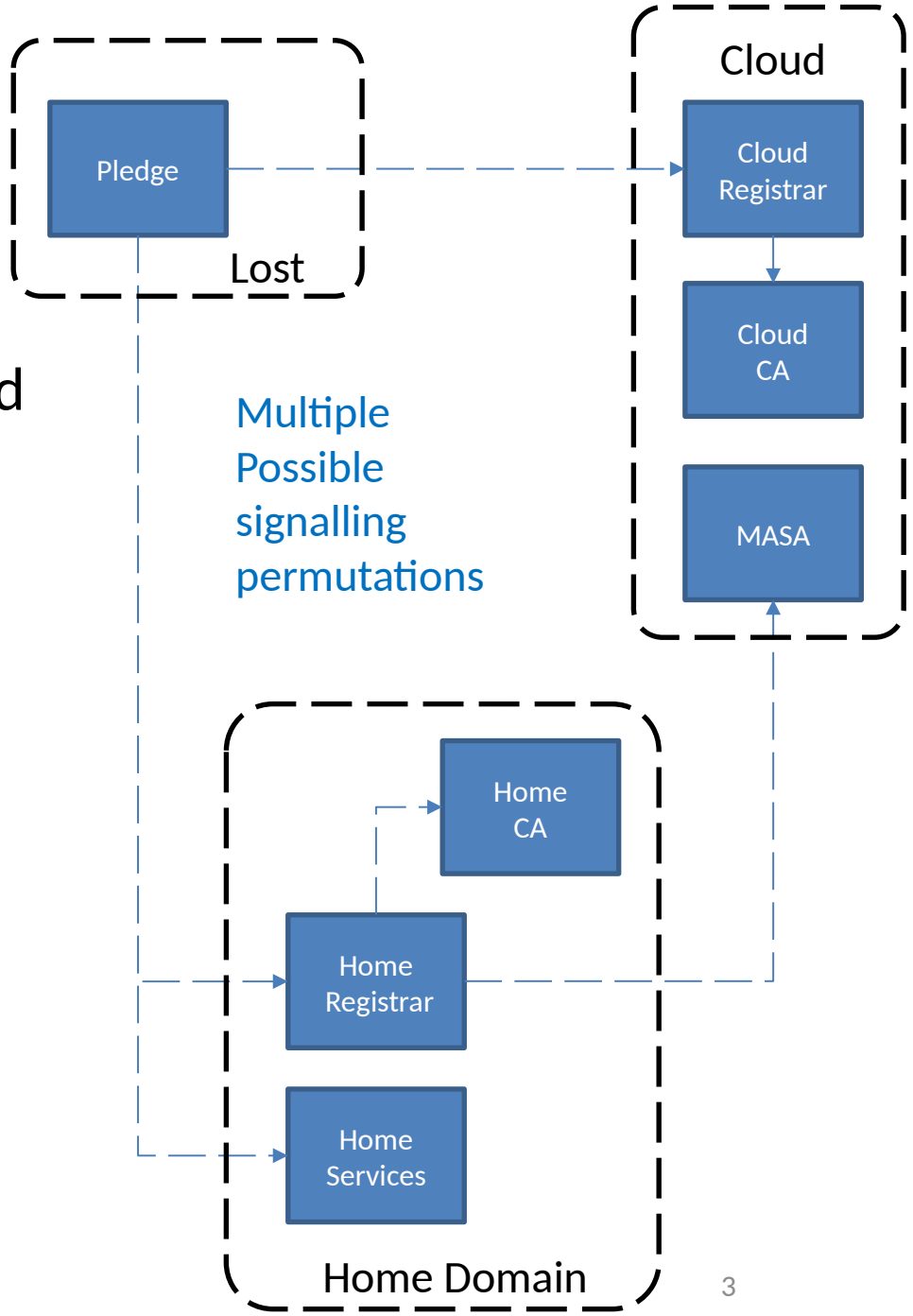
- RFC8995 (BRSKI) does not fully specify default Cloud Registrar operation

- draft-ietf-anima-brski-cloud does
  - two unique scenarios

- Use cases:
  1. A pledge bootstrapping from a location remote from the domain, and having no Join Proxy needs to discover the location of it's home Registrar.
  2. Use case: A pledge bootstrapping in a location in which there is not (yet?) a BRSKI Registrar may need to use a Manufacturer provided service for onboarding to Enterprise CA

Architecture

- Pledge connects to Cloud Registrar on bootstrap and requests Voucher
  - Mutual TLS enforced using IDevID and implicit TA
  - Assumption is that Pledge has internet access
- Choices, choices, choices
  1. ~~Does~~ Cloud Registrar issue Voucher or 3xx to Home Registrar~~?~~!
  2. ~~If Cloud Registrar issues Voucher, does it also issue suitably namespaced LDevID, or does~~ it redirect to EST requests to home Registrar~~?~~
  3. ~~If Cloud Registrar issues LDevID, how does it tell the Pledge about its home domain?~~

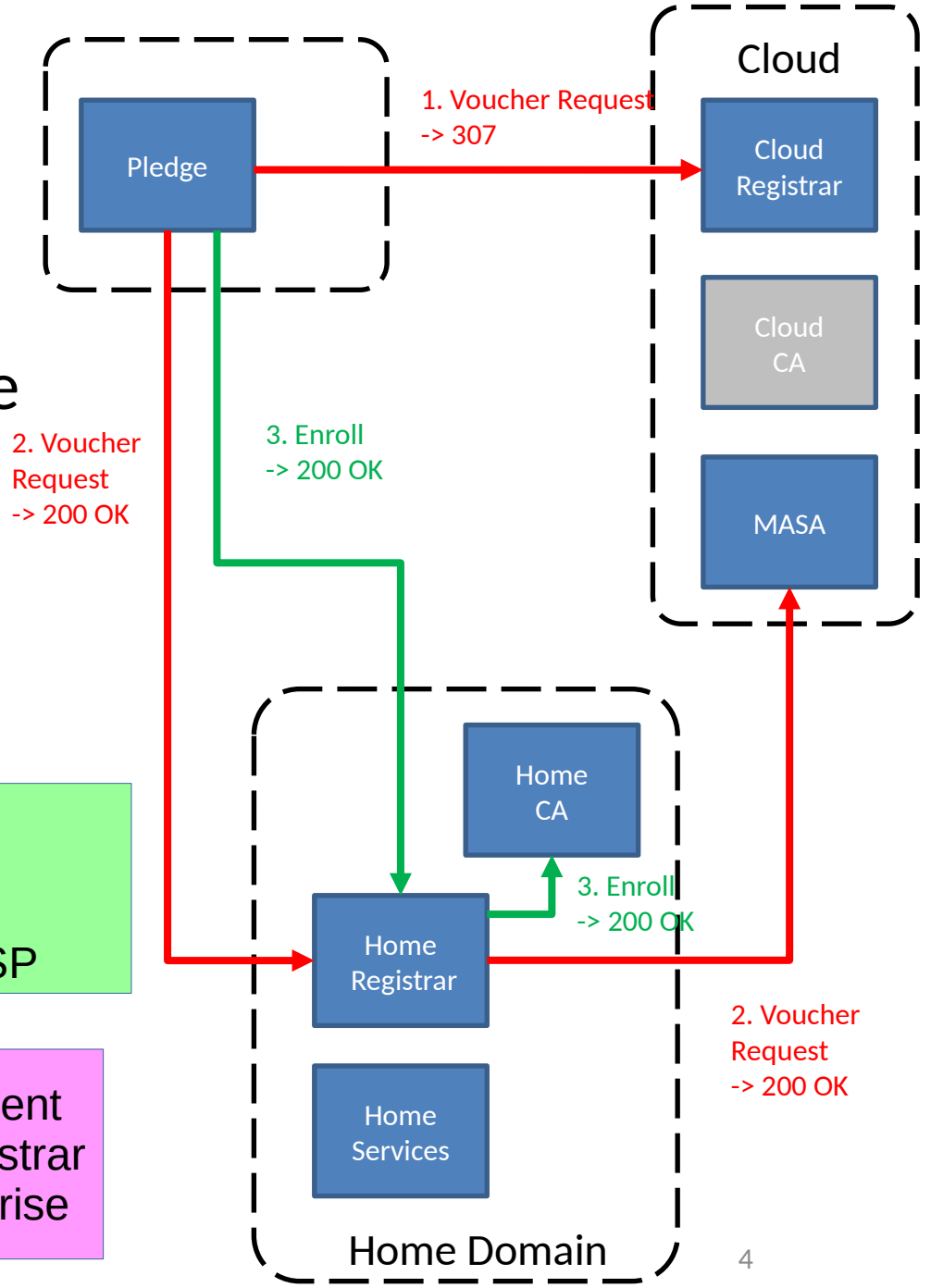


Scenario 1: Cloud Registrar Redirects

- Cloud Registrar replies with a ~~3xx~~ 307 to the Voucher Request
- Pledge completes full BRSKI flow against Home Network

Solves problem that pledge has been deployed in a network with no join proxy, no ACP, no GRASP

e.g., a VoIP phone sent home, must find Registrar in cloud, or at enterprise

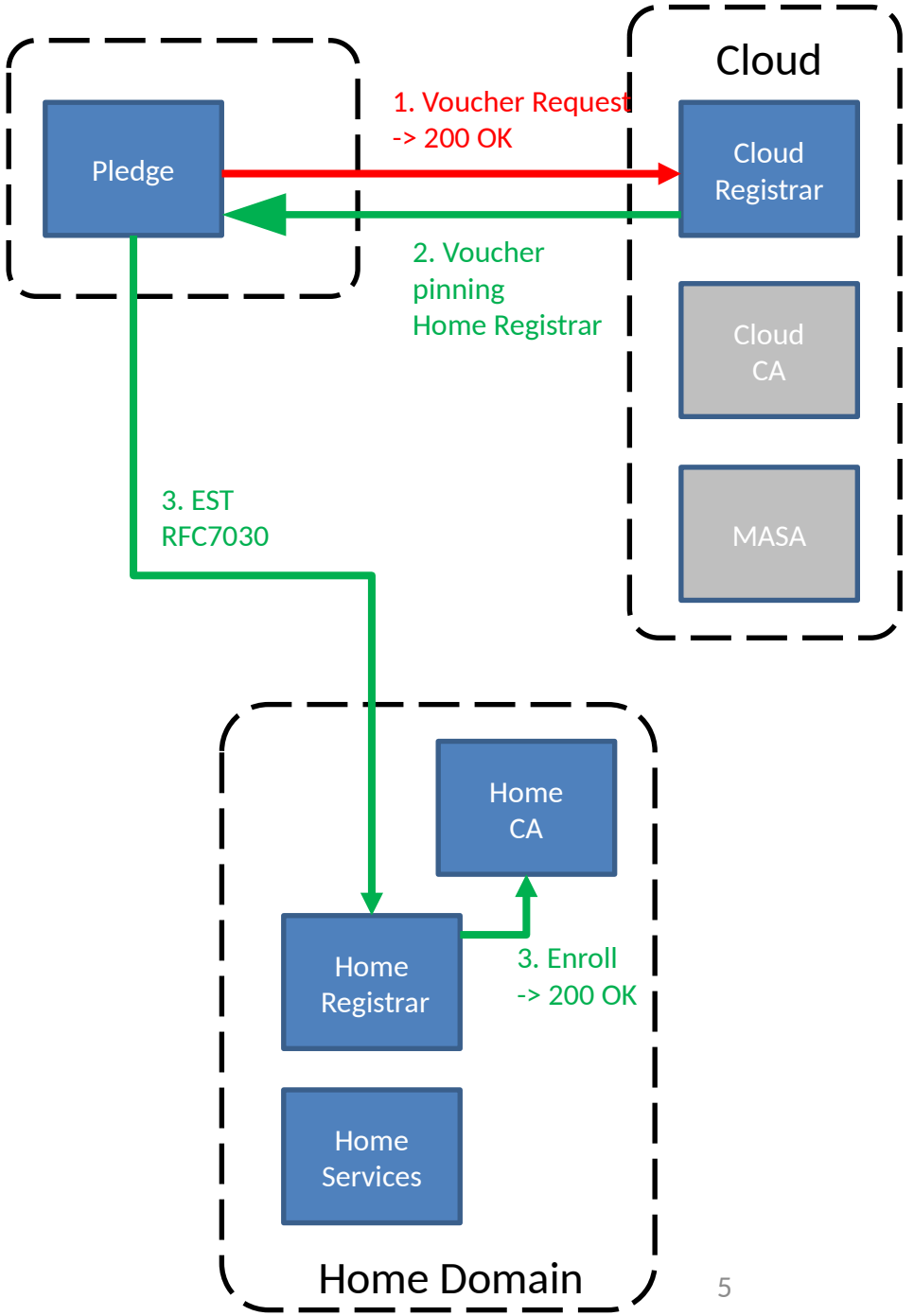


Scenario 2:
Cloud Registrar Issues Voucher
Enterprise CA issues LDevID

- Cloud Register issues Voucher
  - voucher contains extension pointing to Enterprise EST server
- Enterprise EST server performs enrollment based upon IDevID trust

Solves problem that enterprise does EST (RFC7030), but does not yet do BRSKI.

Strong similarity to Intel SDO, etc.



Document status

1) Document adopted in 2021
2) Security Considerations merged in early fall 2021
3) Document ready for reviews and WGLC