draft-friel-anima-brski-cloud

Friel	Cisco
Shekh-Yusef	Avaya
Richardson	Sandelman Software Works

TL;DR

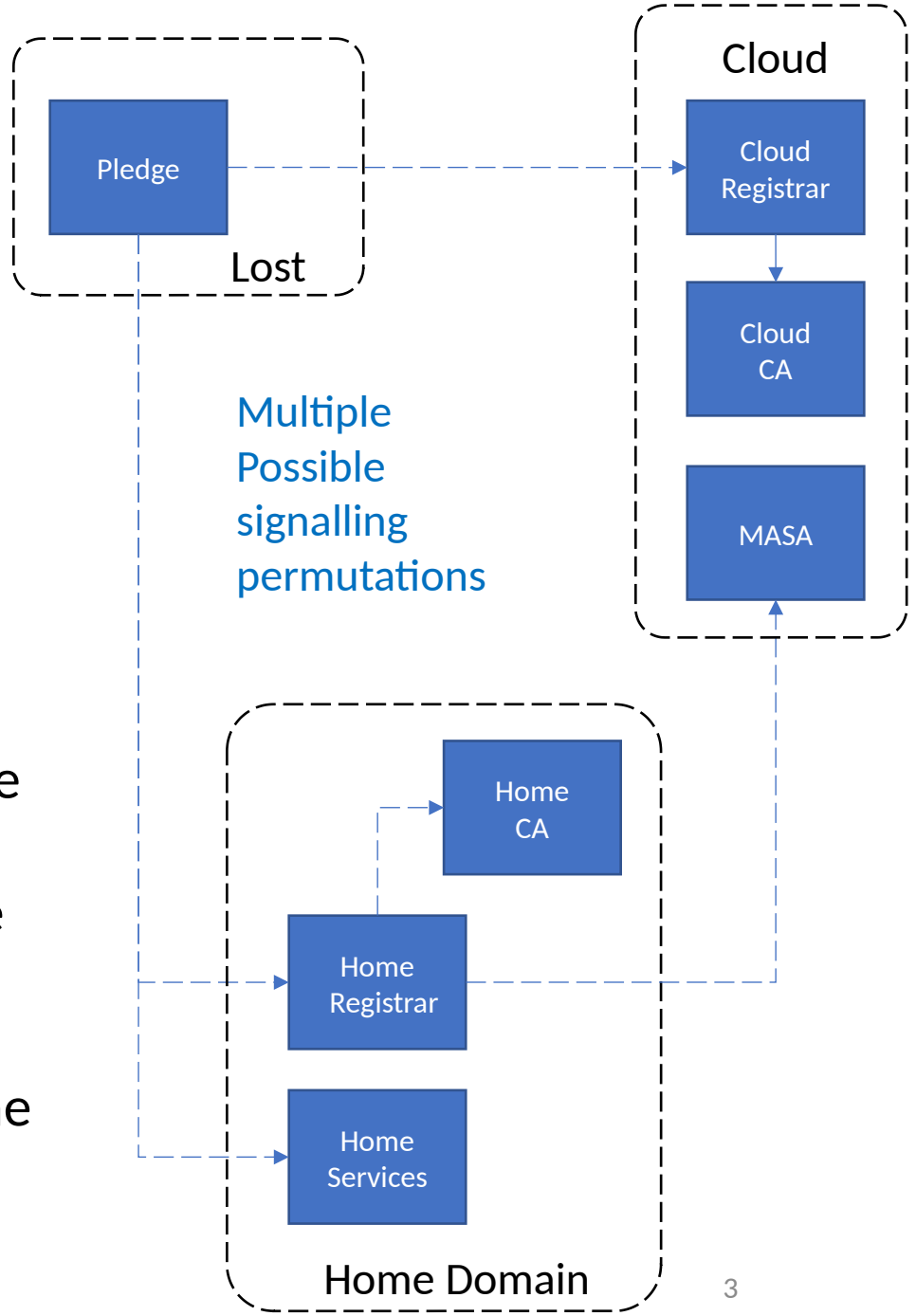
- draft-ietf-anima-bootstrapping-keyinfra does not fully specify Default Cloud Registrar operation

- draft-friel-anima-brski-cloud does

- 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 Registrar may need to use a Manufacturer provided service for onboarding

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?

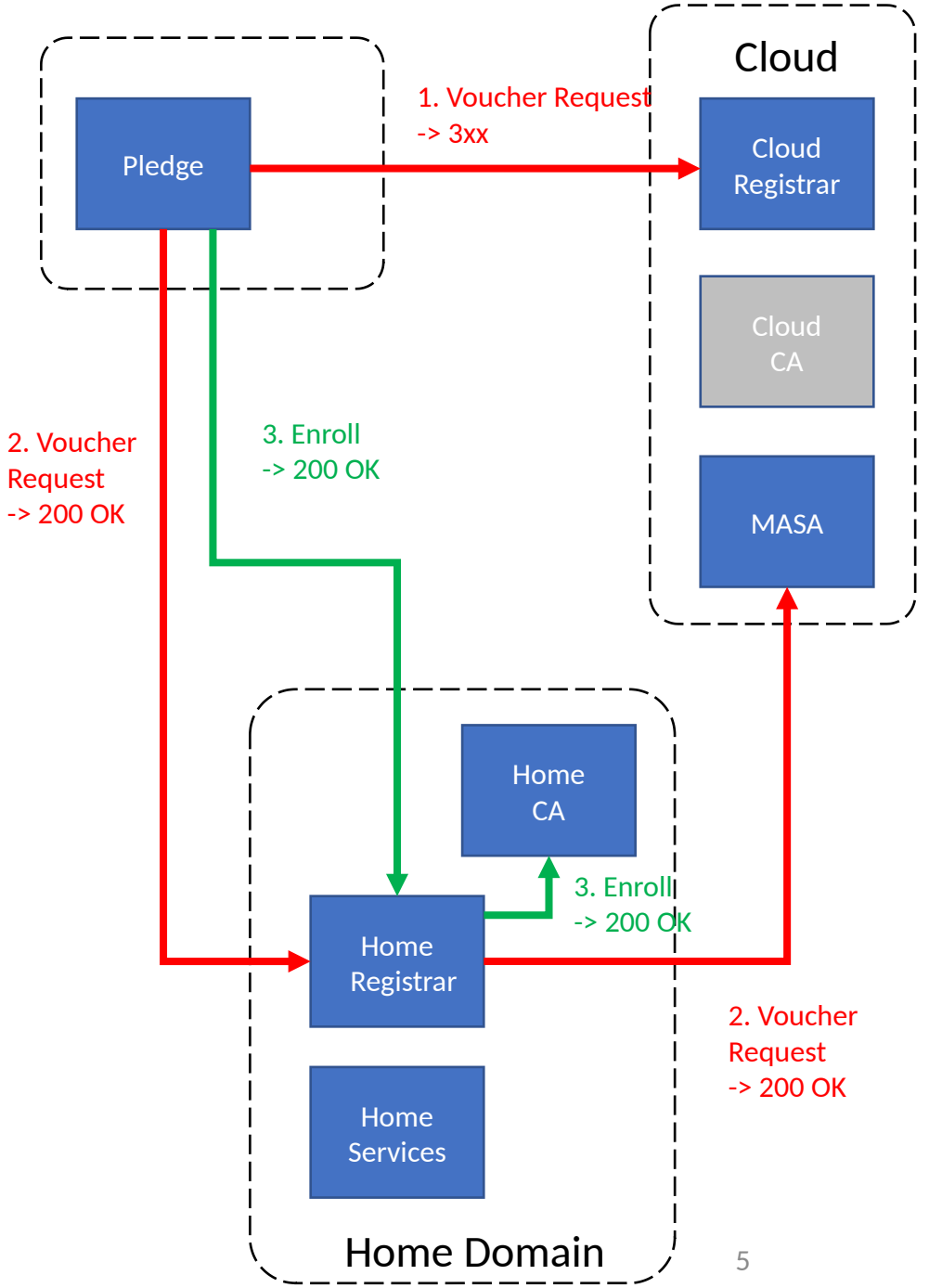


Home Domain Mutual Authentication

- Pledge must be imprinted with trust anchor for home Registrar
  - Pledge may need to be imprinted with realm/domain name of home domain if trust anchor is a Public CA
  - Details on realm/domain identity mapping and verification TBD
- Home Registrar must either
  - Have visibility to and verify Voucher issued by MASA that is bound to Pledge
  - Verify locally significant LDevID that Pledge presents

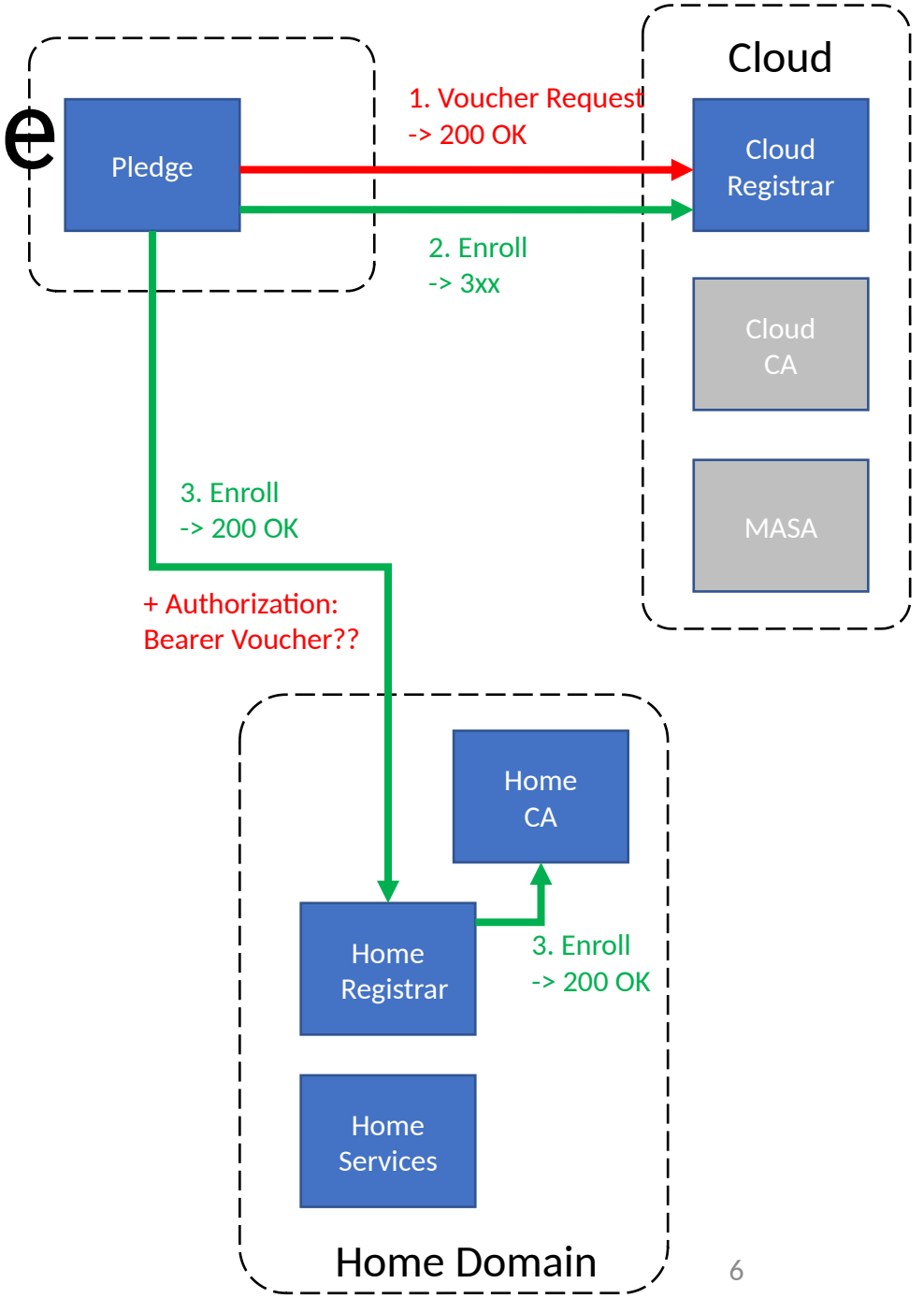
Cloud Registrar Redirects

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



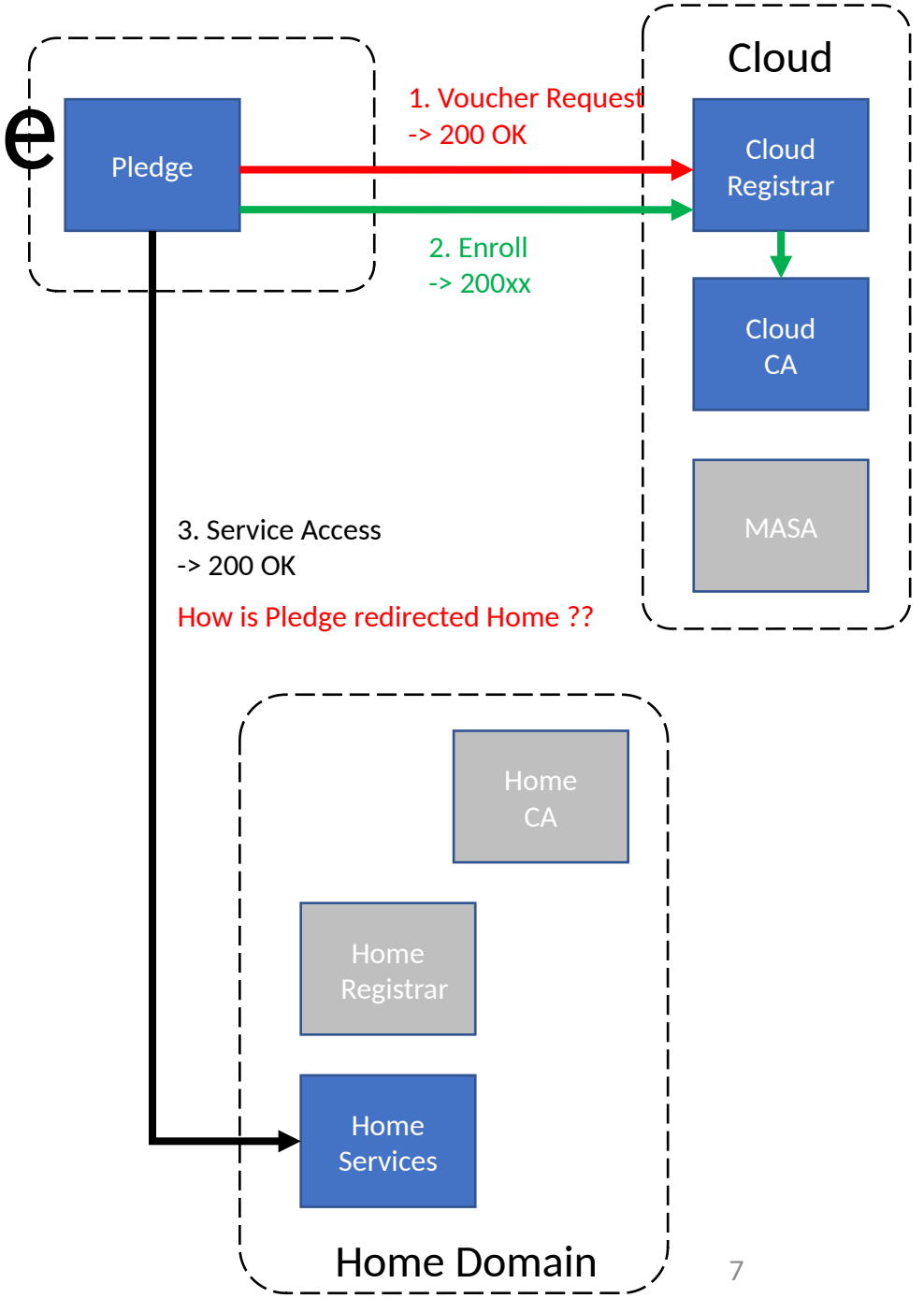
Cloud Registrar Issues Voucher Home CA issues LDevID

- Cloud Register issues Voucher
- Cloud registrar replies with a 3xx to EST enrol / CSR Attributes requests
  - A suboption is that Voucher includes EST domain
- The Voucher issued by the Cloud must include the home network trust anchors
- **There is a problem here:** The Home Network does not see the Voucher so how does it know to trust the Pledge i.e. the IDevID serial number?
  - Could the Voucher be included as a Bearer?
  - Does the Home Registrar need to fetch the Voucher from the Cloud?
  - Does the Pledge need to be explicitly configured on both Home Doman and Cloud?

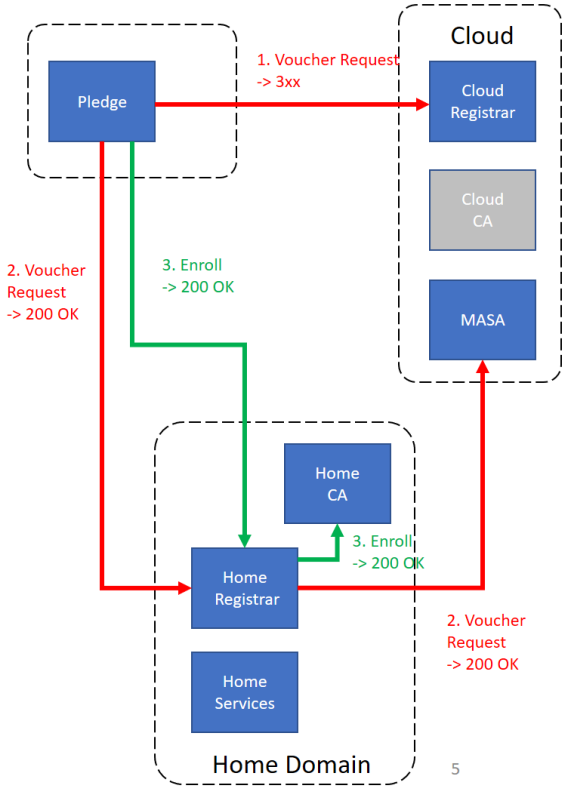


Cloud Registrar Issues Vouche
Cloud CA issues LDevID

- **Two problems here:**
- How does the Cloud Registrar inform the Pledge about its home network for service access?
  - Include a domain in the Voucher?
- How is the LDevID suitably namespaces so that the home network can enforce policy?
  - E.g. is the SAN off a home network subdomain:
    serial-number.pledges.home-network.com?
  - RFC 5280 Name Constraints not suitable as the Cloud CA will be issuing LDevIDs for multiple home service domains

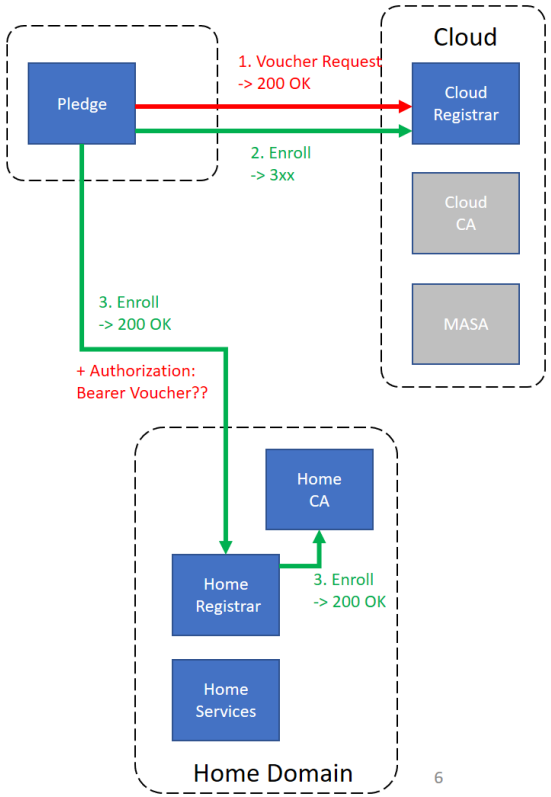


Option 1
Cloud Registrar redirects



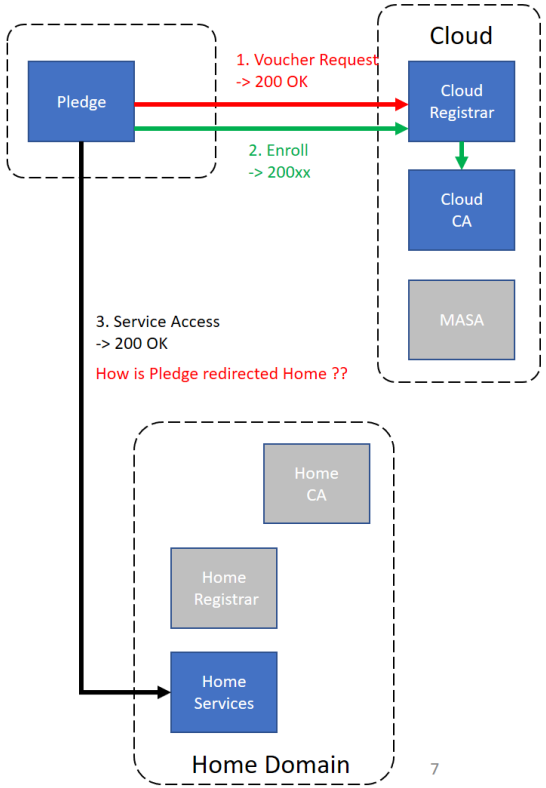
- If the pinned-domain-cert is a Public CA, does the Voucher also include a home registrar domain / realm?

Option 2
Cloud Registrar Issues Voucher
Home CA issues LDevID



- Could Voucher include Home Registrar / EST Domain?
- How is Voucher given to Home Registrar?

Option 3
Cloud Registrar Issues Voucher
Cloud CA issues LDevID



- How does Pledge discover Home Service Domain?
- How is Cloud CA issued LDevID namespaced?

- **How many options should be supported?**
- **Discussion / Next Steps?**