draft-friel-anima-brski-cloud

IETF 108 - ANIMA - 2020-07-30

Friel	Cisco
Shekh-Yusef	~~Avaya~~ -> Auth0
Richardson	Sandelman Software Works

TL;DR

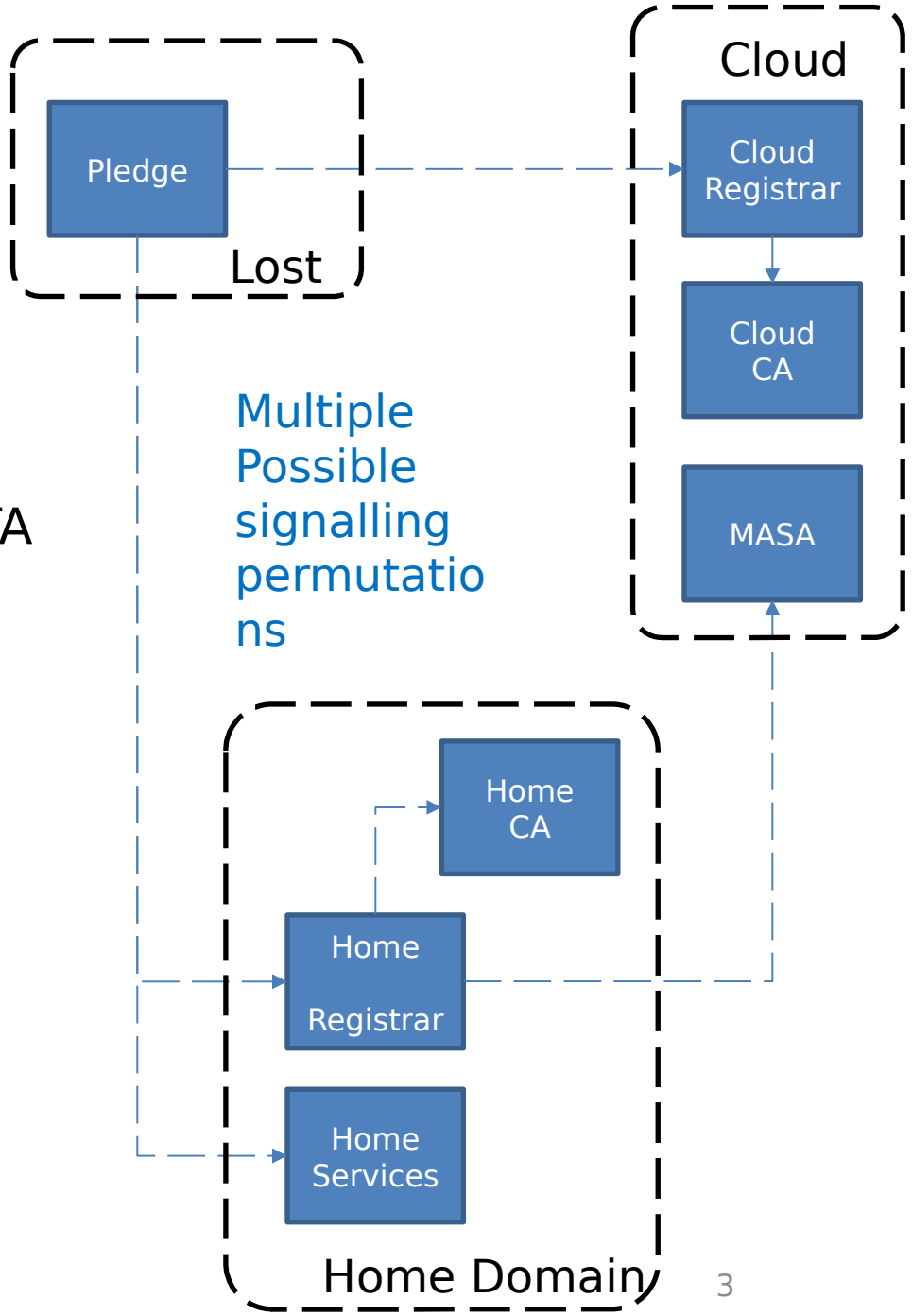
- draft-ietf-anima-bootstrapping-keyinfra does not fully specify default Cloud Registrar operation

- draft-friel-anima-brski-cloud does
  - reduced scenarios in -02 from four down to two unique

- 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

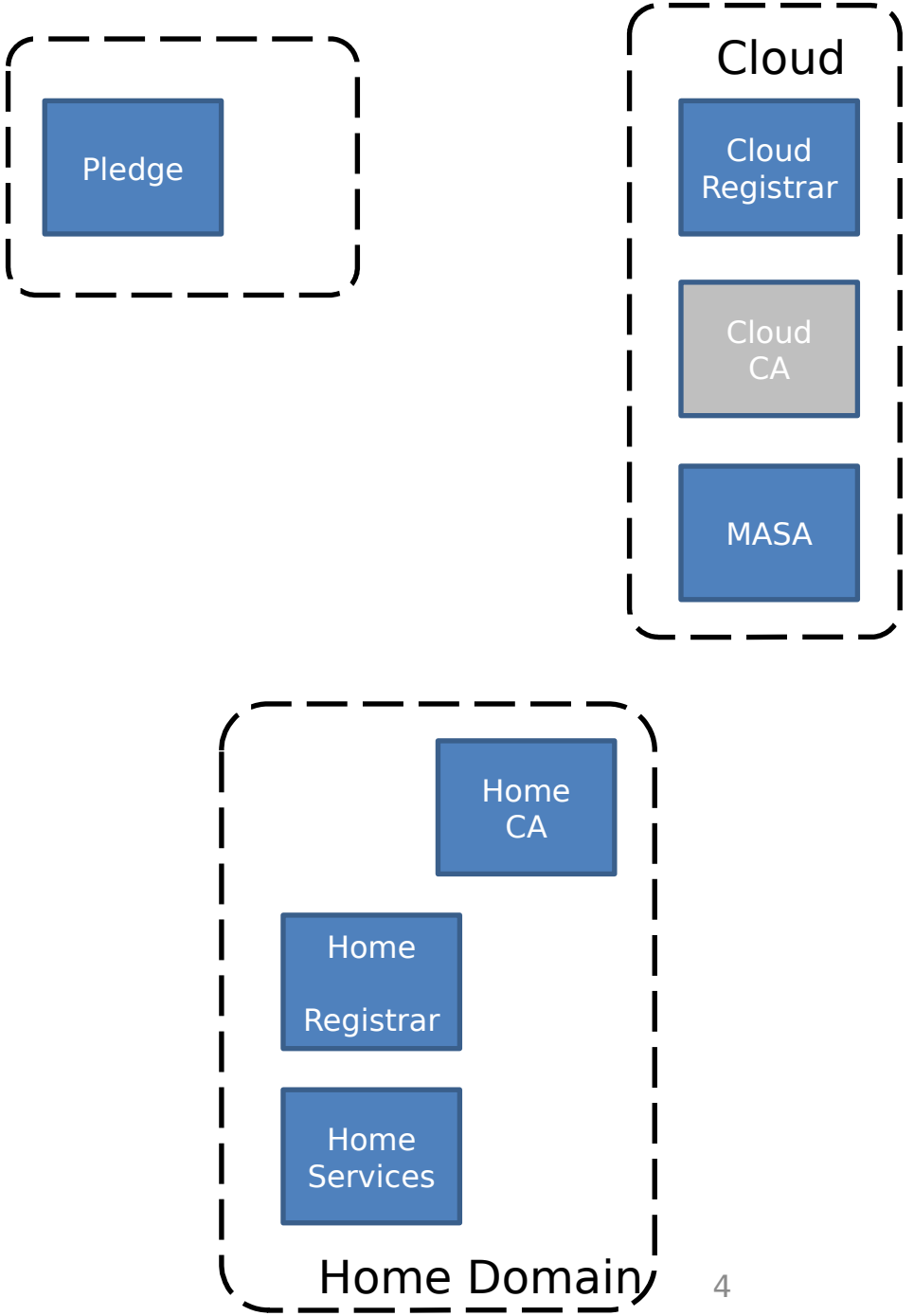
Architecture

- 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

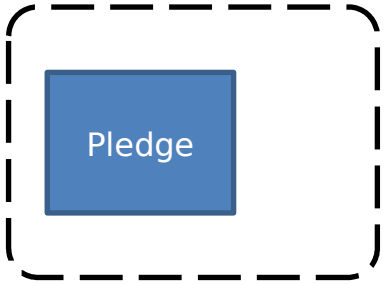
- Cloud Registrar replies with a ~~3xx~~ **307** to the Voucher Request
- Pledge completes full BRSKI flow against Home Network

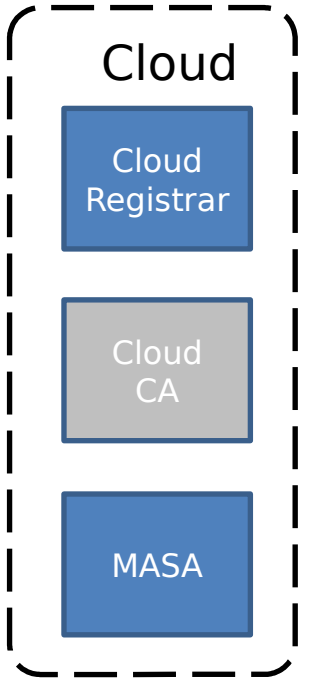


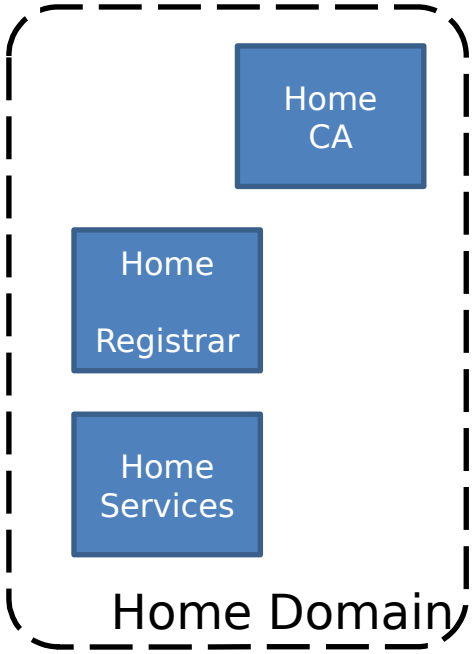
Scenario 1: Cloud Registrar Redirects

- 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

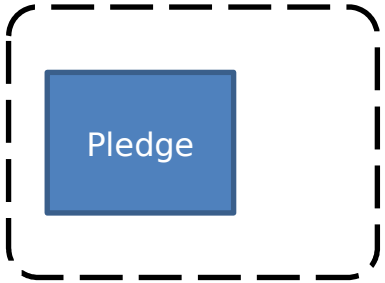


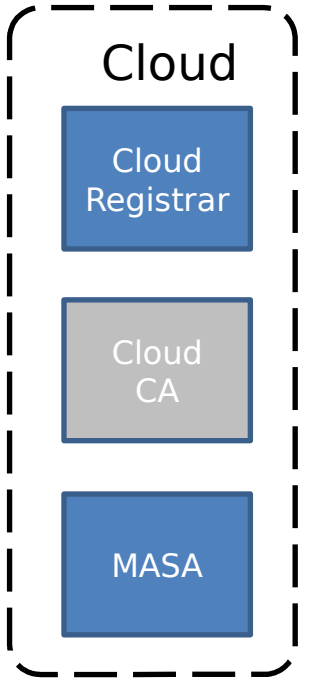




Scenario 1: Cloud Registrar Redirects

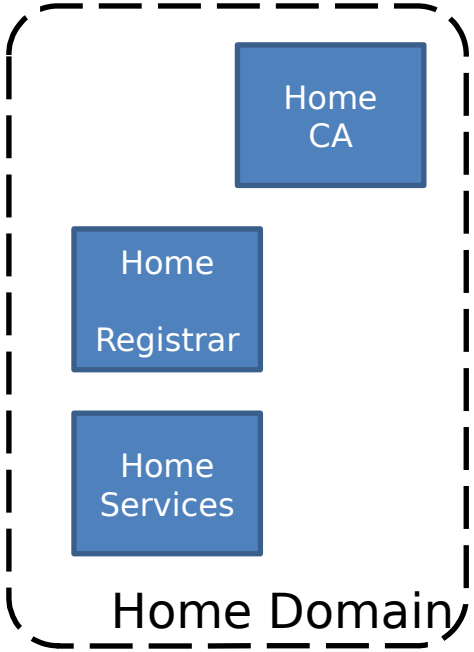
- Cloud Registrar replies with a ~~3xx~~ **307** to the Voucher Request
- Pledge completes full BRSKI flow against Home Network





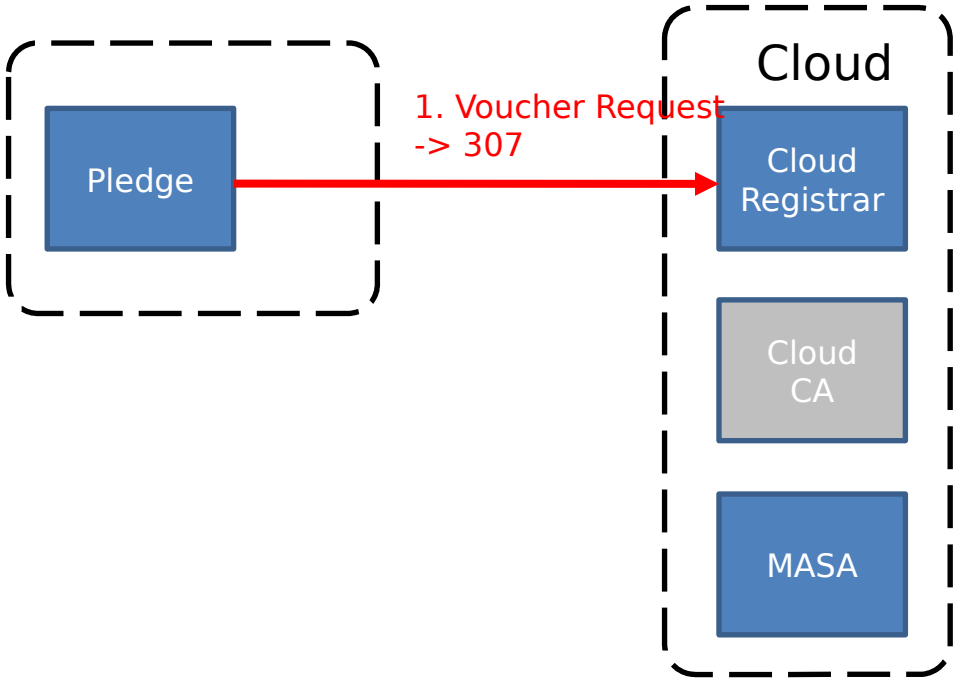
Solves problem that pledge has been deployed in a network with no join proxy, no ACP, no GRASP

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



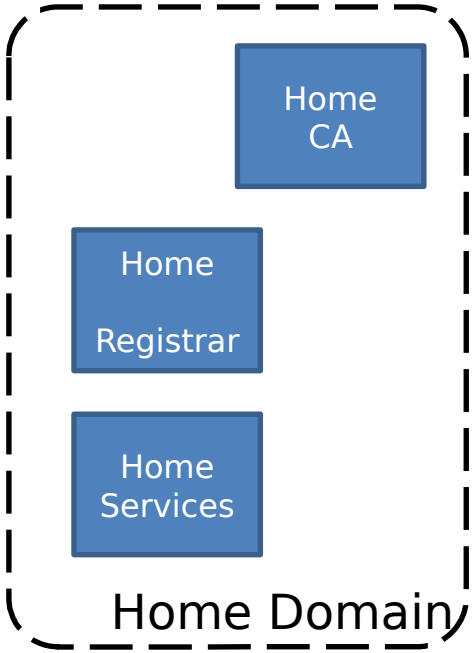
Scenario 1: Cloud Registrar Redirects

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



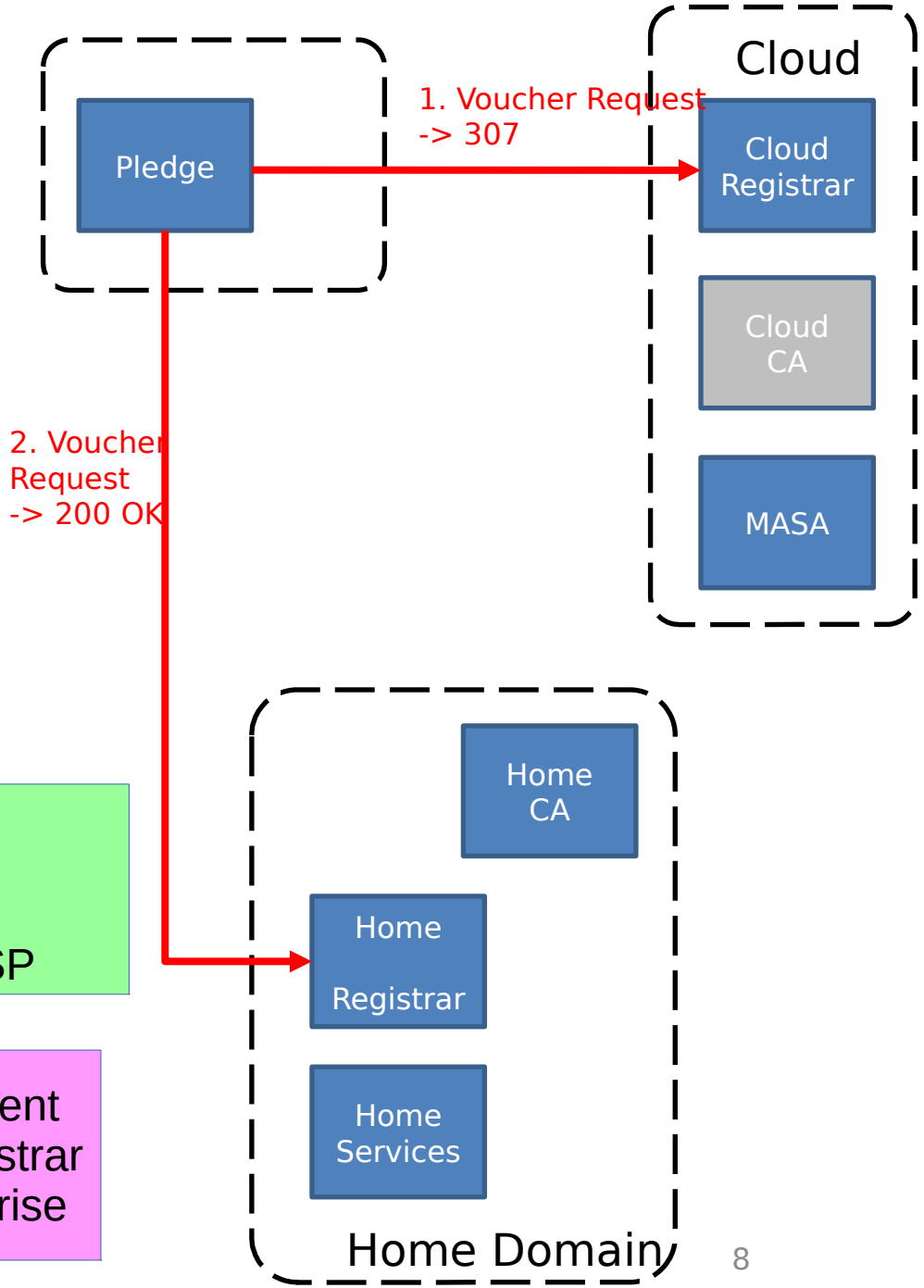
Solves problem that pledge has been deployed in a network with no join proxy, no ACP, no GRASP

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



Scenario 1: Cloud Registrar Redirects

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

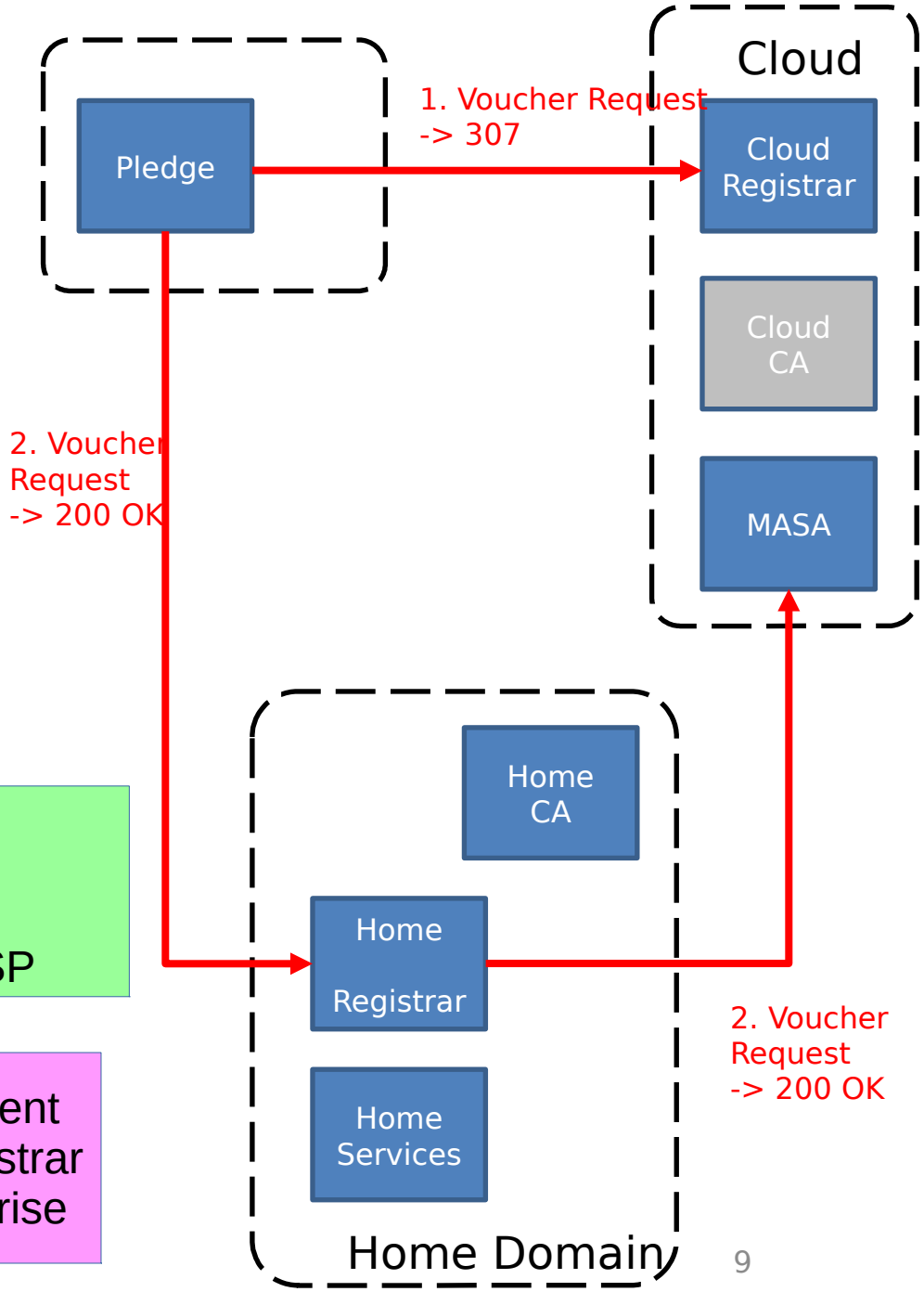


Solves problem that pledge has been deployed in a network with no join proxy, no ACP, no GRASP

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

Scenario 1: Cloud Registrar Redirects

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

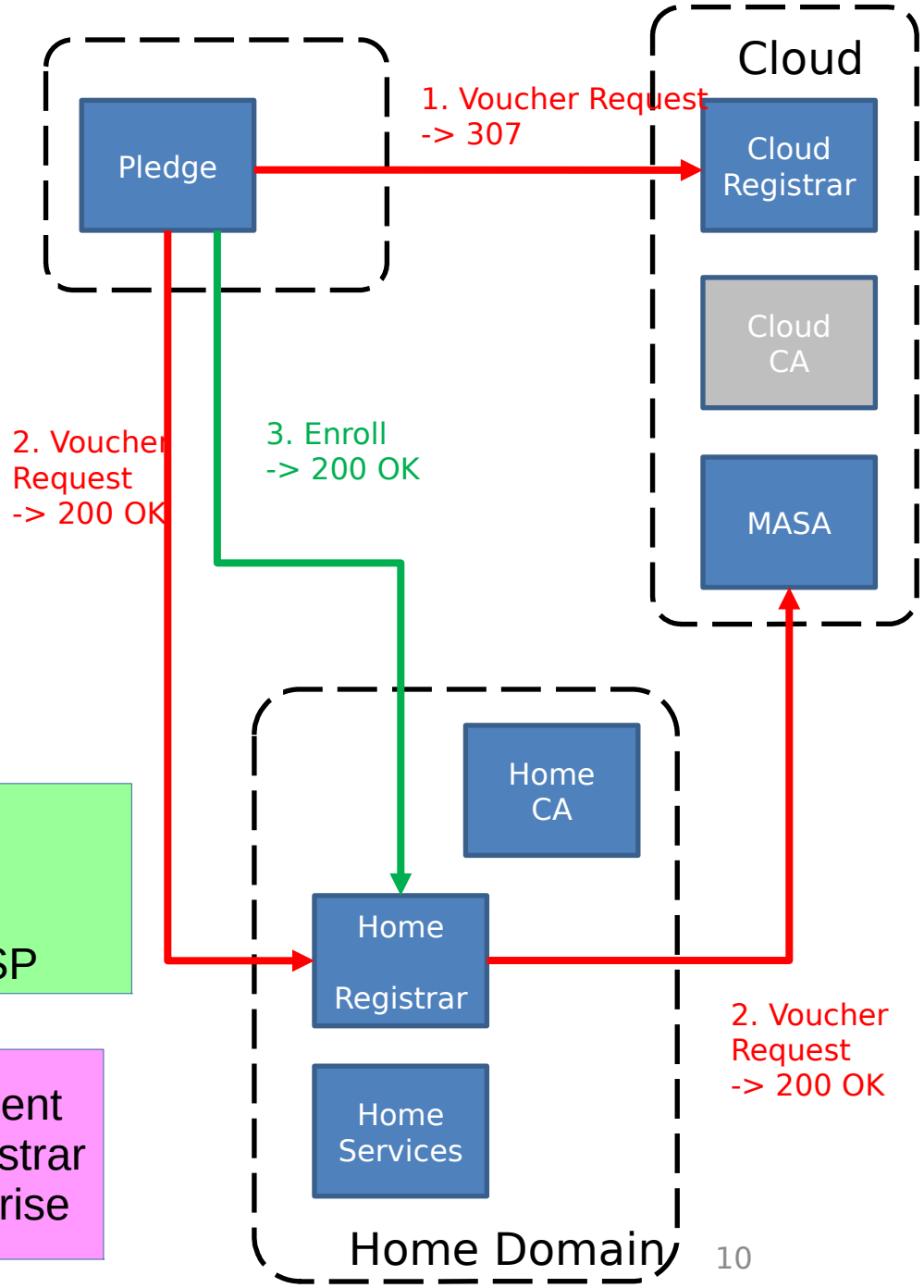


Solves problem that pledge has been deployed in a network with no join proxy, no ACP, no GRASP

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

Scenario 1: Cloud Registrar Redirects

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

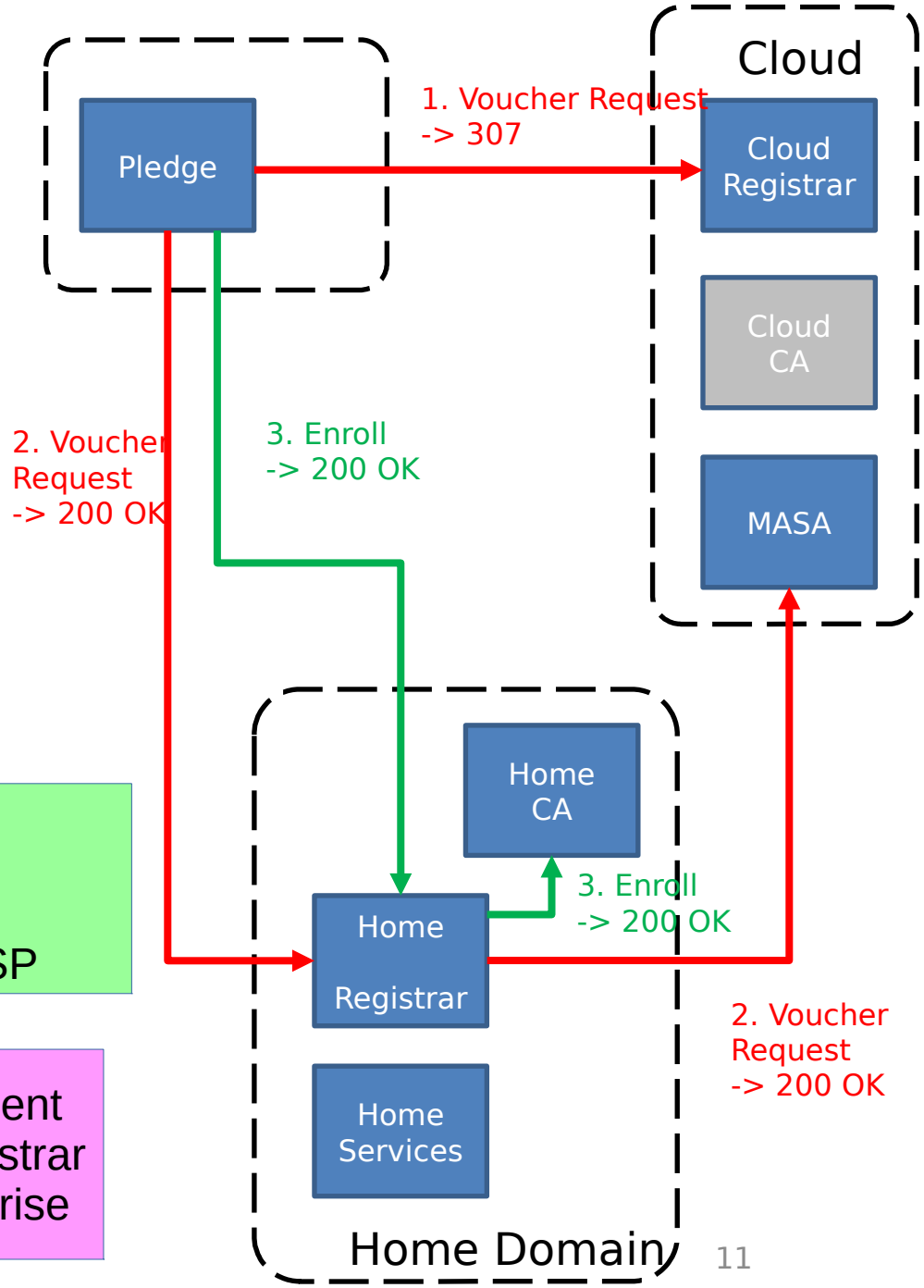


Solves problem that pledge has been deployed in a network with no join proxy, no ACP, no GRASP

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

Scenario 1: Cloud Registrar Redirects

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

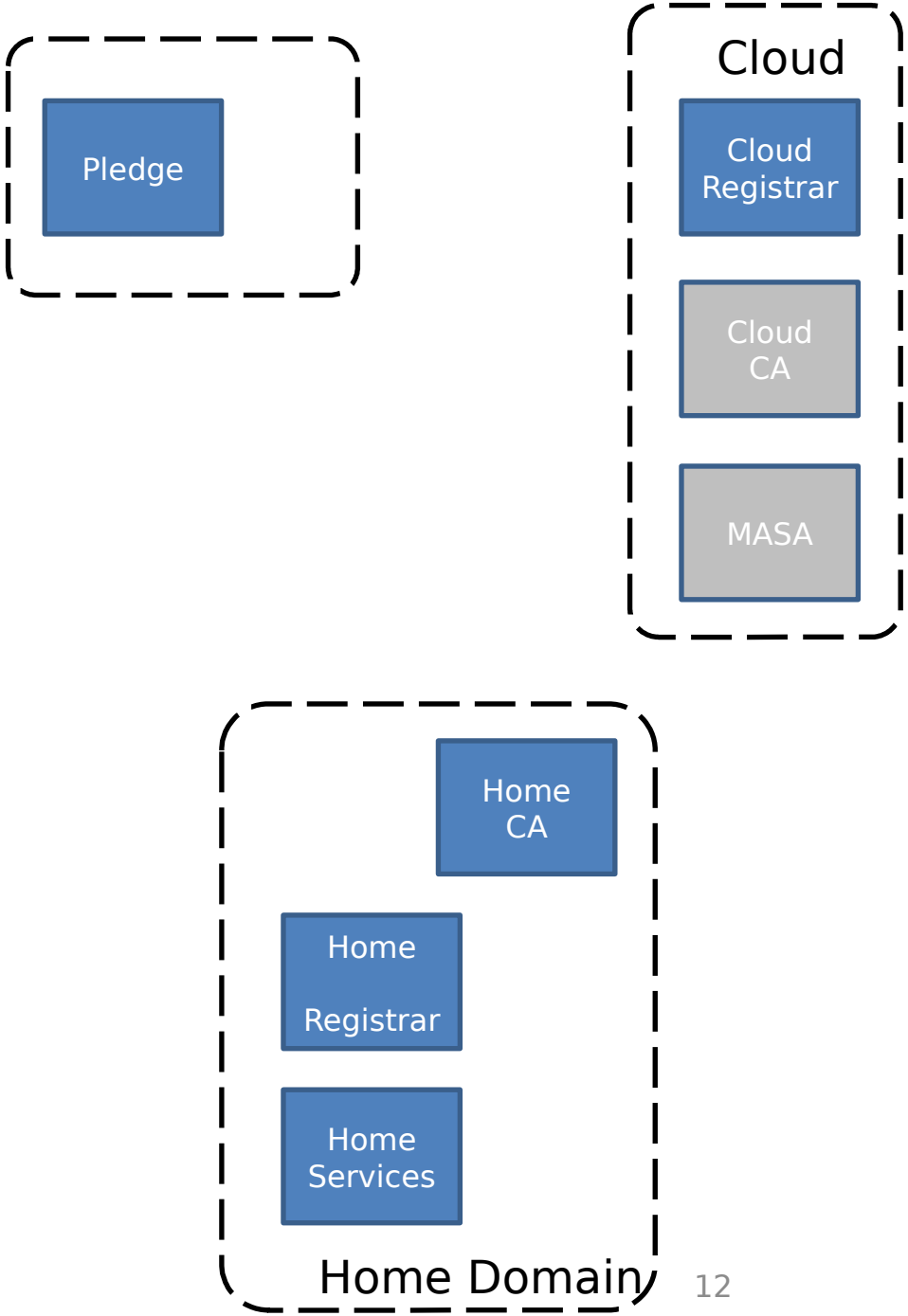


Solves problem that pledge has been deployed in a network with no join proxy, no ACP, no GRASP

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

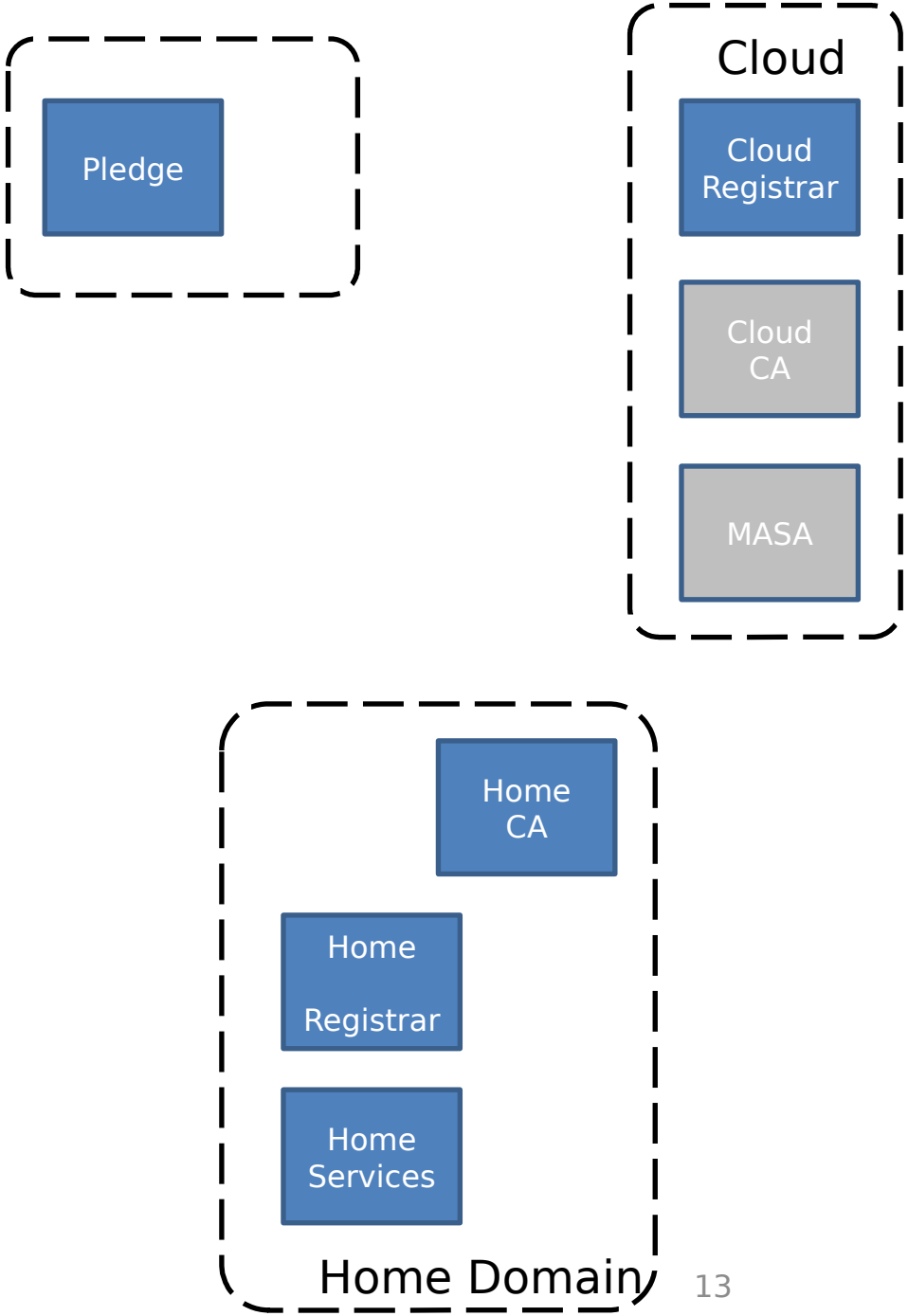
- Cloud Register issues Voucher
  - voucher contains extension pointing to Enterprise EST server
- Enterprise EST server performs enrollment based upon IDevID trust



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

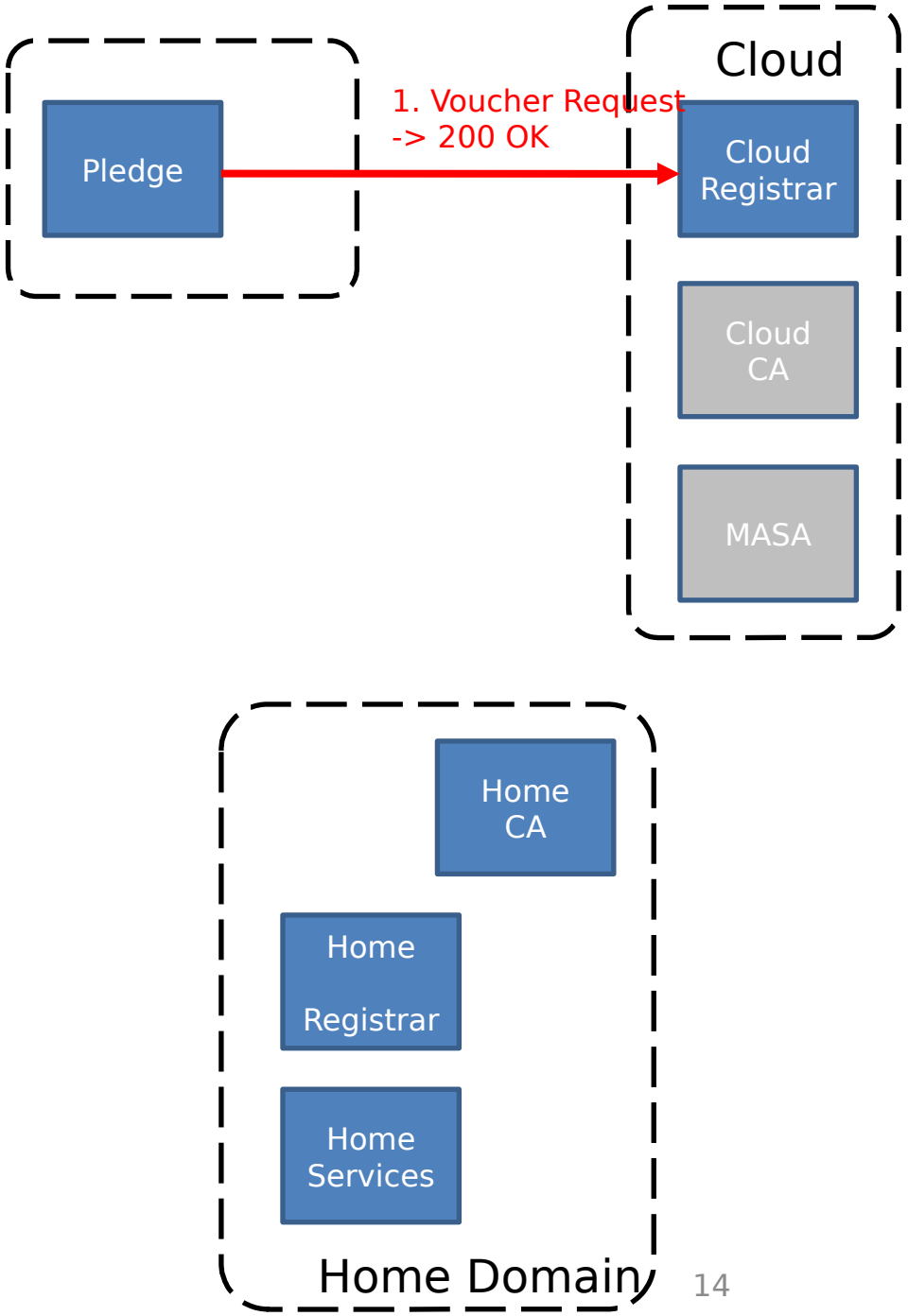
Solves problem that enterprise does EST (RFC7030), but does not yet do BRSKI.



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

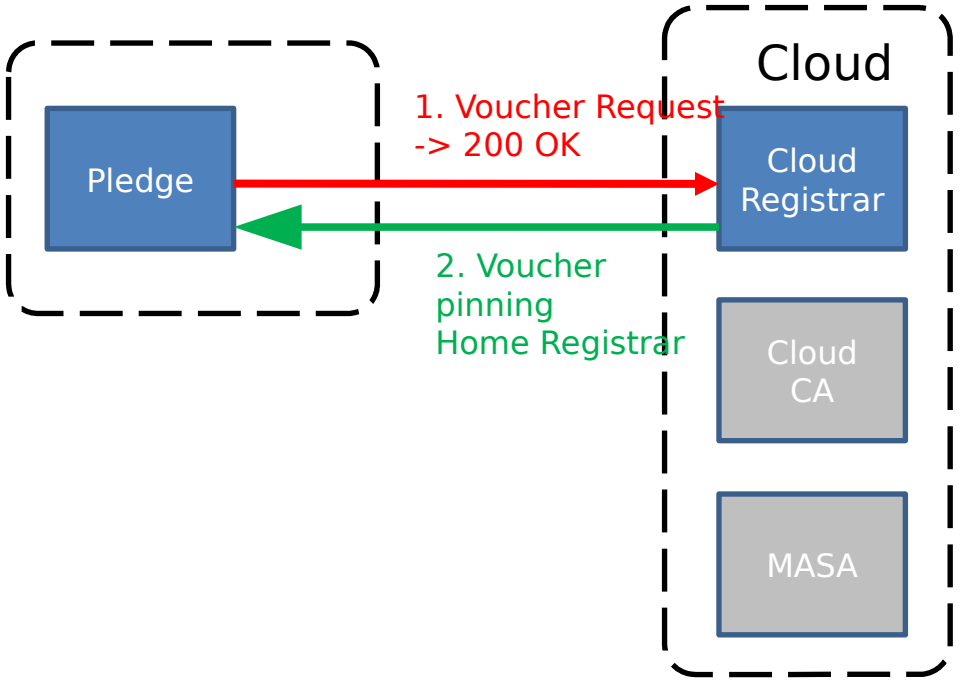
Solves problem that enterprise does EST (RFC7030), but does not yet do BRSKI.

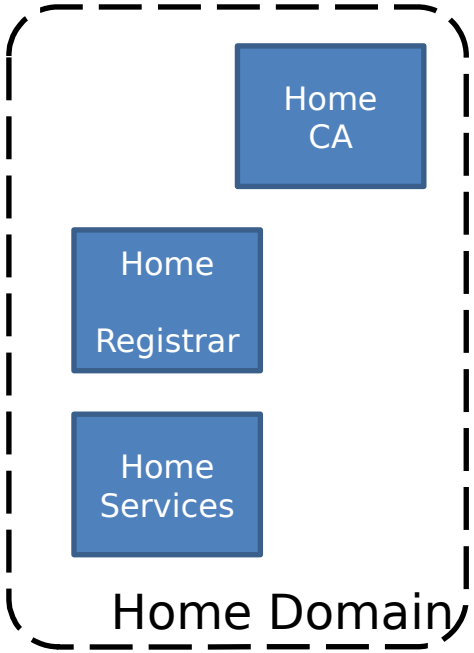


Scenario 2: Cloud Registrar Issues Voucher Enterprise CA issues LDevID

- 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.

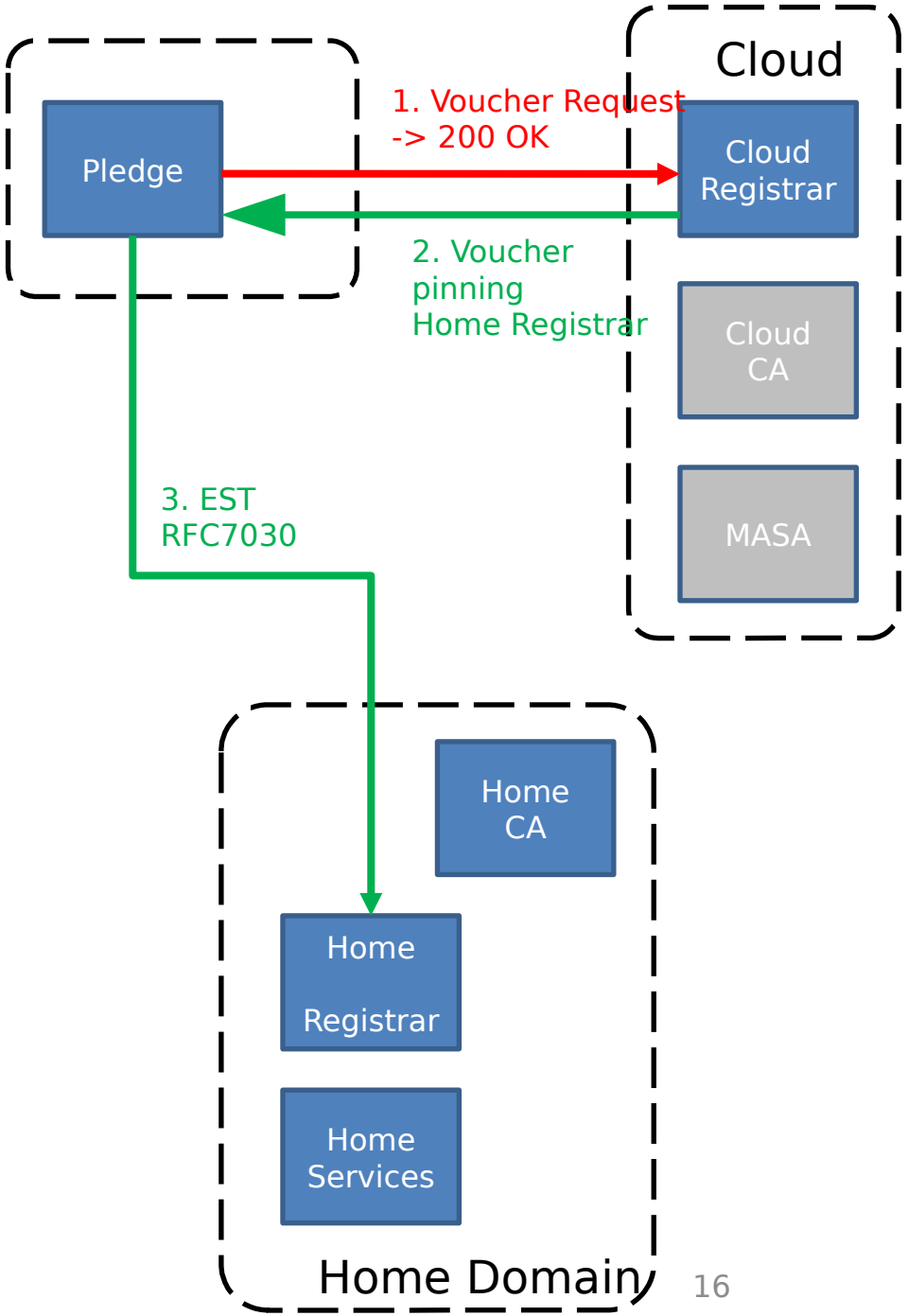




Scenario 2: Cloud Registrar Issues Voucher Enterprise CA issues LDevID

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

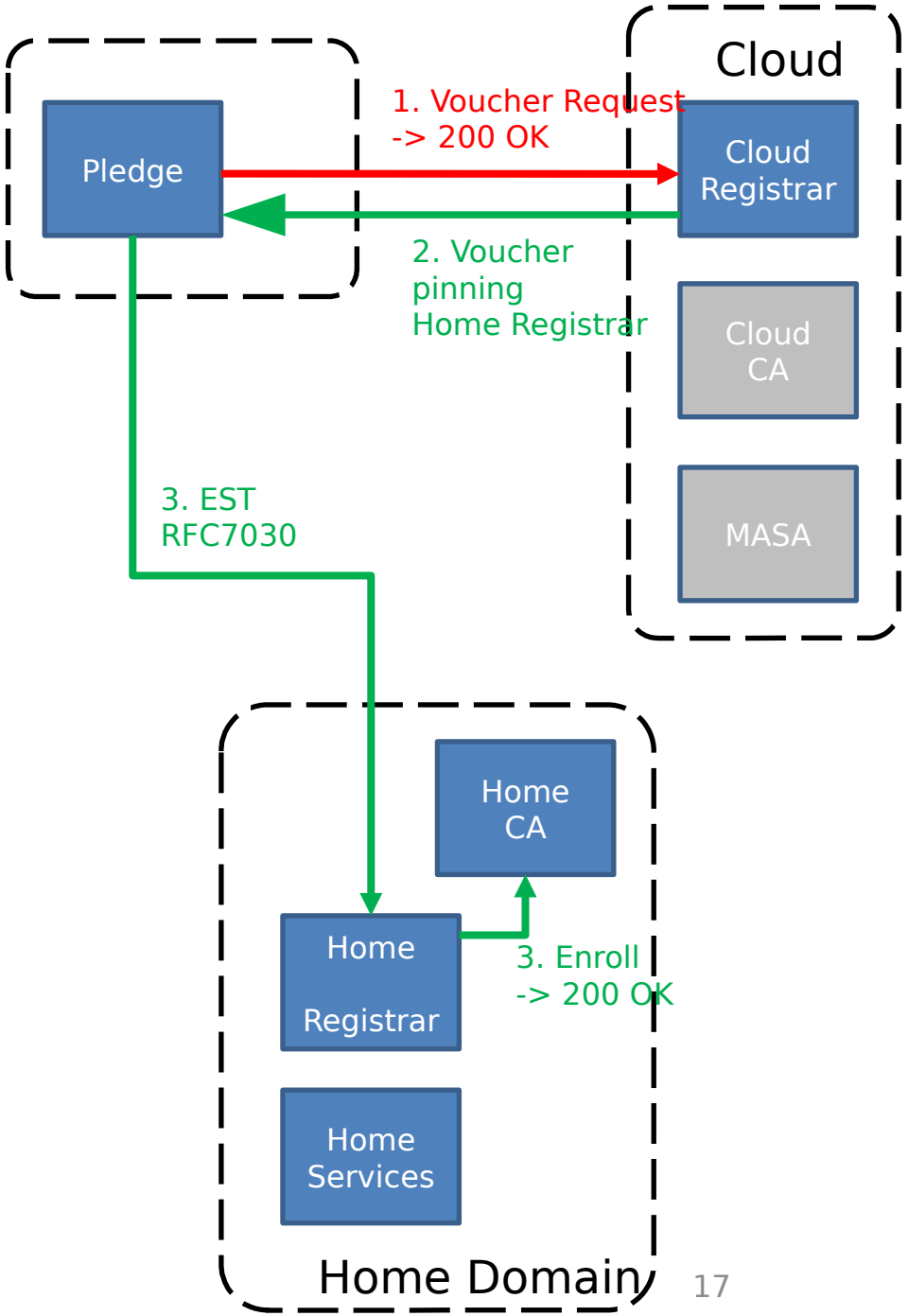
Solves problem that enterprise does EST (RFC7030), but does not yet do BRSKI.



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.

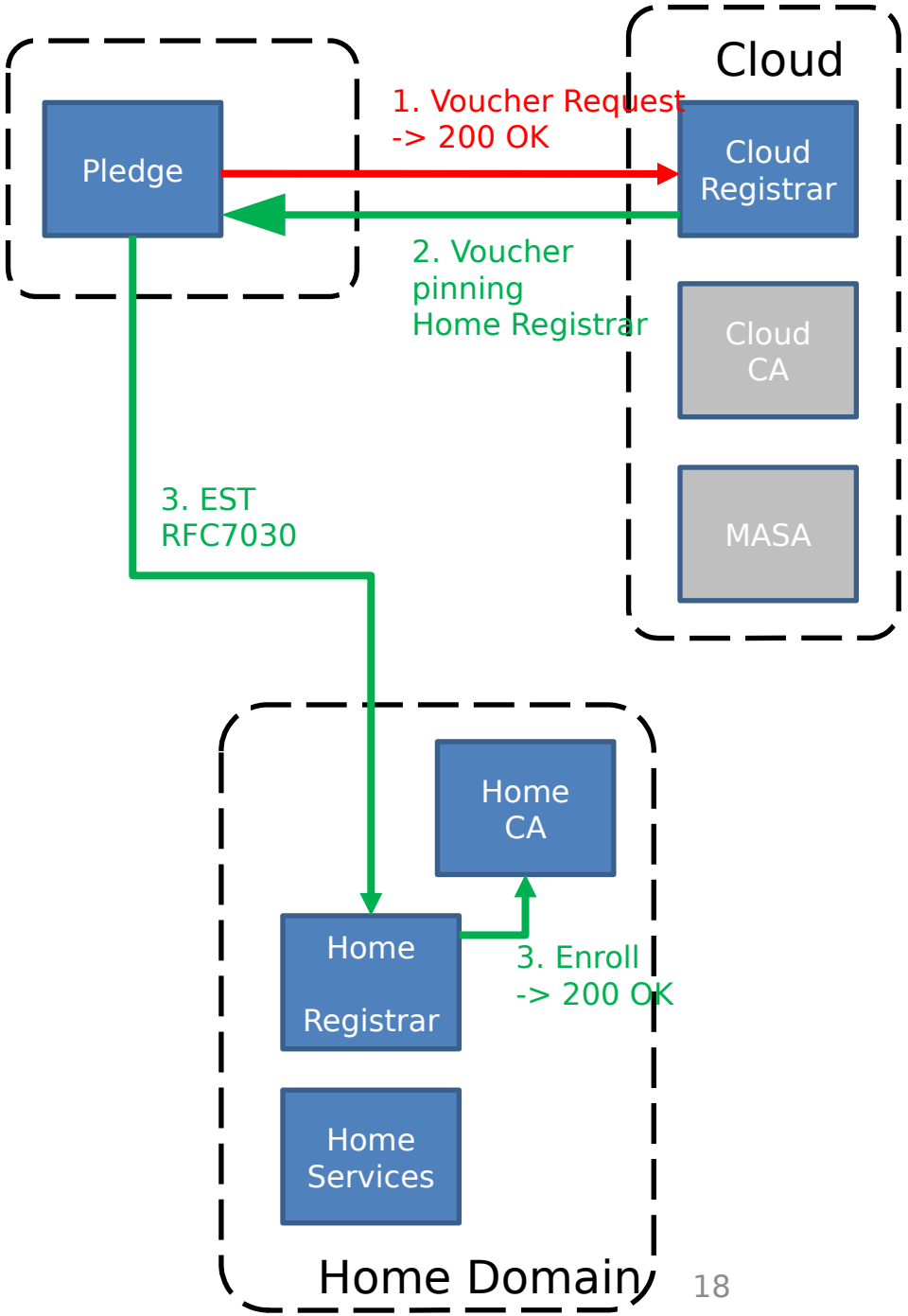


Scenario 2: Cloud Registrar Issues Voucher Enterprise CA issues LDevID

- 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.



Work remaining to do

1) properly articulate the applicability for each use case
2) define the voucher extension (YANG) for the RFC7030 extension needed for scenario 2.
3) consider if supporting CMP (SCEP?) is desired, and how to do this for scenario 2

Next steps

WG could consider adoption if

it agrees with the problem statement.