Anima IETF 93

draft-pritikin-anima-bootstrapping-keyinfra-02

Design Team Update

Added state diagrams
and updated document structure

- 3.1. Behavior of a new entity

Entity

- 3.3. Behavior of the Registrar

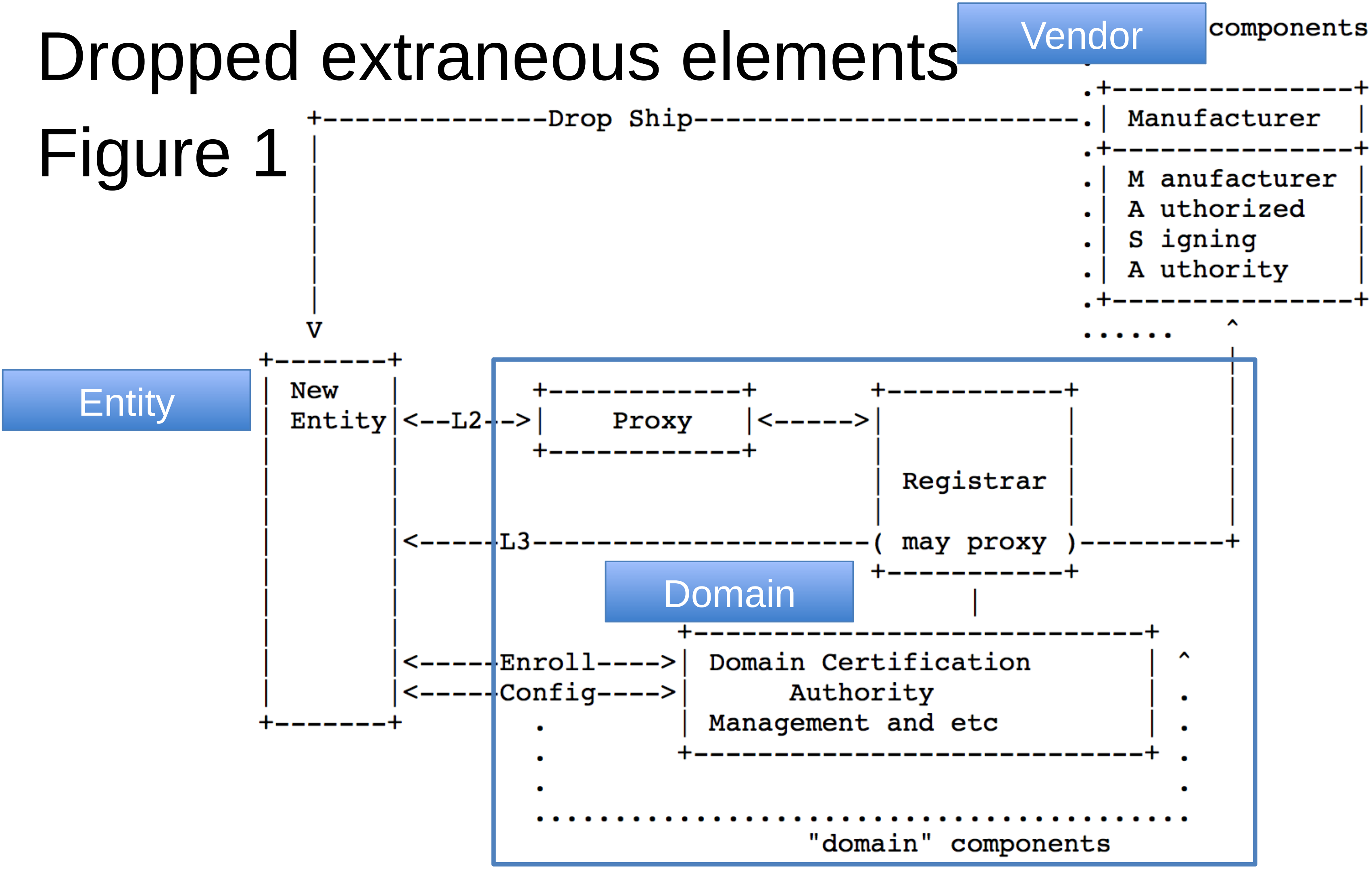
Domain

- 3.4. Behavior of the MASA Service

Vendor

Simplified Architecture diagram

- Dropped extraneous elements
- Figure 1



Vendor components

Manufacturer

Manufacturer Authorized Signing Authority

Drop Ship

Entity

New Entity

L2

Proxy

Registrar

(may proxy)

L3

Domain

Enroll

Config

Domain Certification Authority

Management and etc

"domain" components

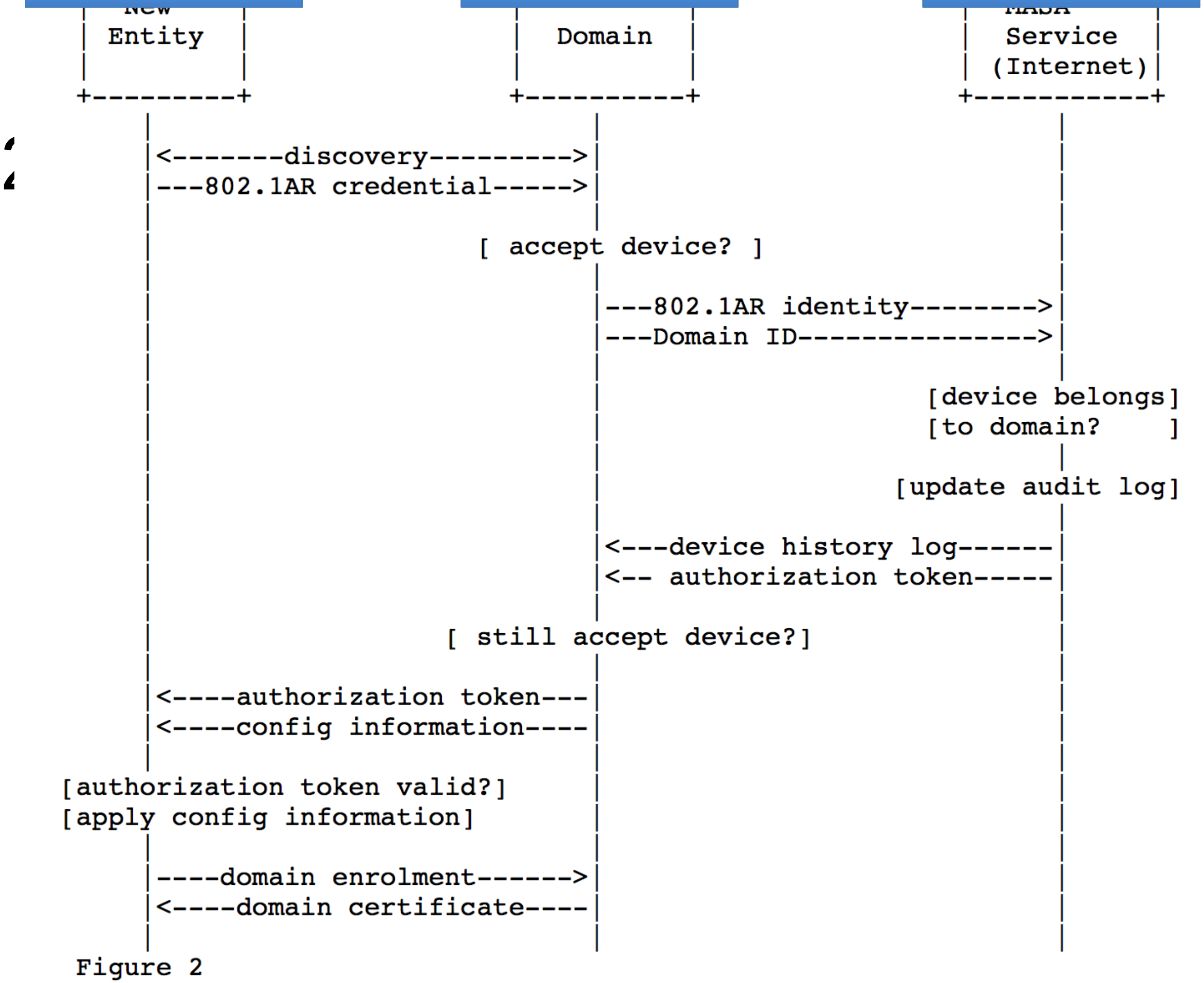
Aligned with Functional Overview

- Figure 2

Entity

Domain

Vendor



```
   |  New     |           |           |          |  MASA      |
   | Entity   |           |  Domain   |          |  Service   |
   |          |           |           |          | (Internet) |
   +----------+           +-----------+          +------------+
        |                        |                       |
        |<-------discovery--------->|                       |
        |---802.1AR credential----->|                       |
        |                        |                       |
        |              [ accept device? ]                 |
        |                        |                       |
        |                        |---802.1AR identity-------->|
        |                        |---Domain ID--------------->|
        |                        |                       |
        |                        |               [device belongs]
        |                        |               [to domain?    ]
        |                        |                       |
        |                        |             [update audit log]
        |                        |                       |
        |                        |<---device history log------|
        |                        |<-- authorization token-----|
        |                        |                       |
        |             [ still accept device?]            |
        |                        |                       |
        |<----authorization token---|                       |
        |<----config information----|                       |
        |                        |                       |
 [authorization token valid?]       |                       |
 [apply config information]        |                       |
        |                        |                       |
        |----domain enrolment------>|                       |
        |<----domain certificate----|                       |
        |                        |                       |
  Figure 2
```

Reduced security operational modes

- s6.1. New Entity security reductions

  touch based

  - s6.2. Registrar security reductions

  accept lower authentication / logging

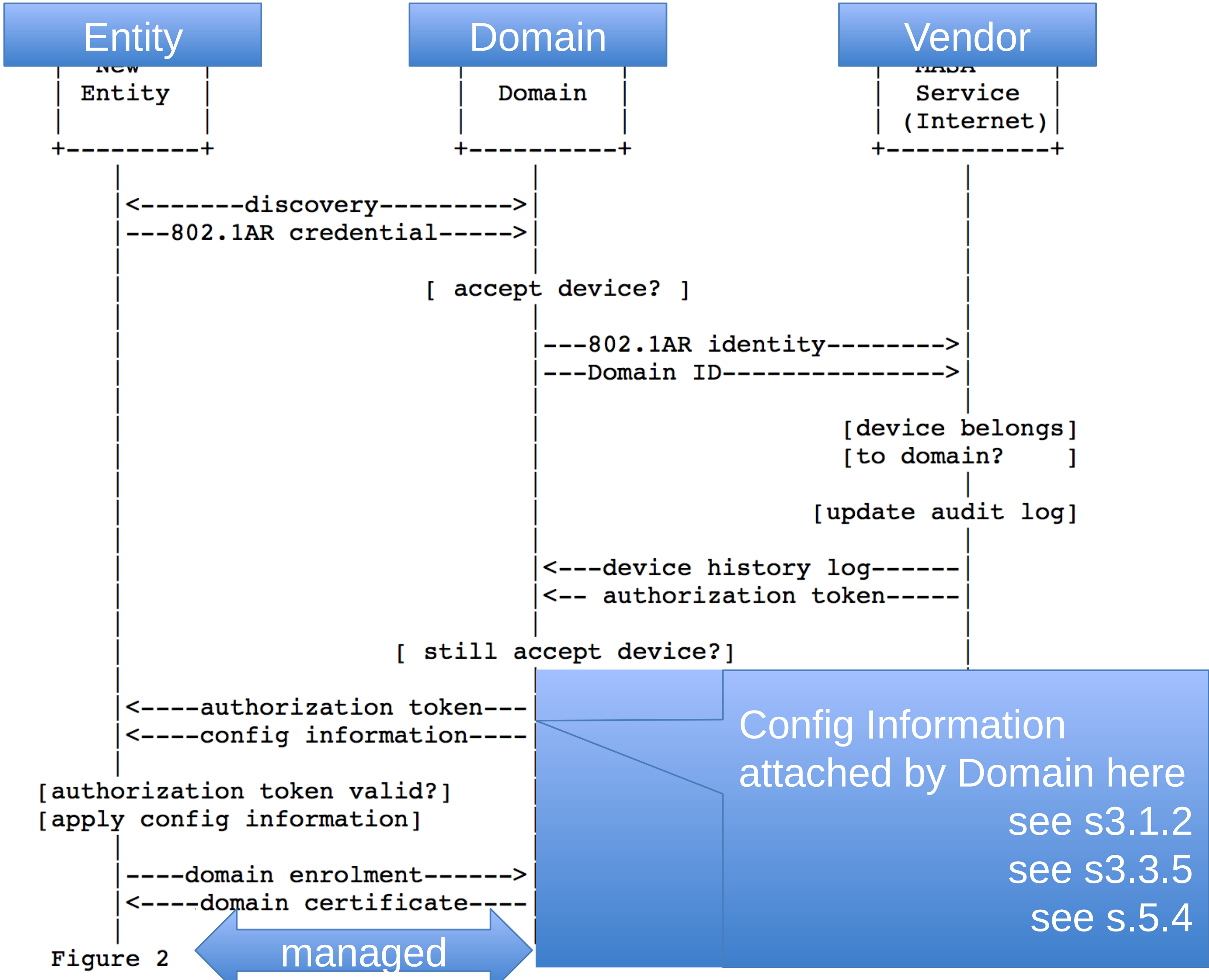
  permanently claim the device

  - s6.3. MASA security reductions

  not verifying ownership

  accept permanent claims

added bootstrap config discussion



Entity

Domain

Vendor

```
      New                                      MASA
 |   Entity   |        |   Domain    |      |  Service   |
 |            |        |             |      | (Internet) |
 +----------+          +-----------+        +------------+
      |                        |                     |
      |<-------discovery--------->|                  |
      |---802.1AR credential----->|                  |
      |                        |                     |
      |                 [ accept device? ]           |
      |                        |                     |
      |                        |---802.1AR identity-------->|
      |                        |---Domain ID--------------->|
      |                        |                     |
      |                        |             [device belongs]
      |                        |             [to domain?    ]
      |                        |                     |
      |                        |            [update audit log]
      |                        |                     |
      |                        |<---device history log------|
      |                        |<-- authorization token-----|
      |                        |                     |
      |               [ still accept device?]        |
      |                        |
      |<----authorization token---
      |<----config information----
      |
 [authorization token valid?]
 [apply config information]
      |
      |----domain enrolment------>
      |<----domain certificate----
      |
  Figure 2
```

managed

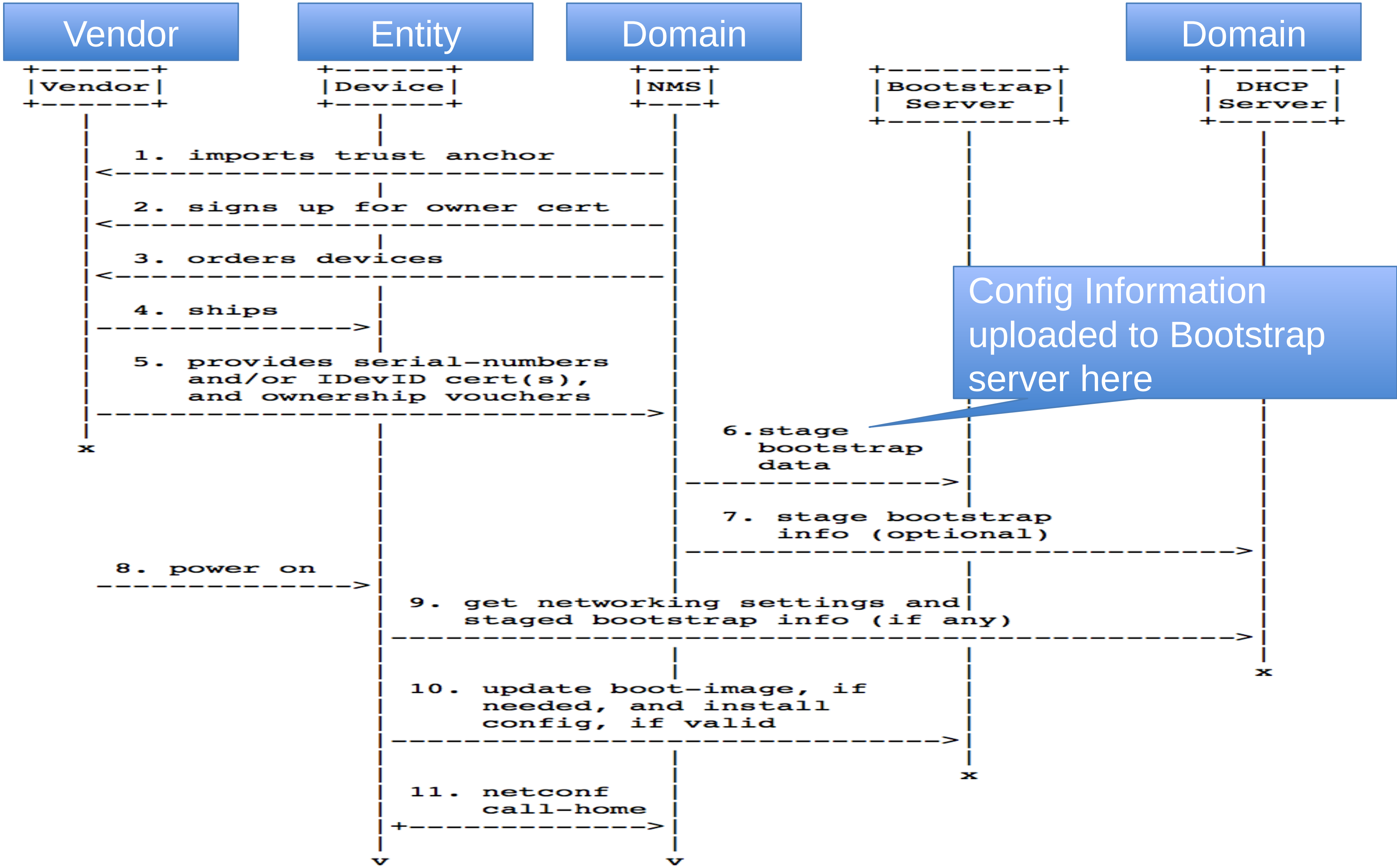
Config Information attached by Domain here

see s3.1.2

see s3.3.5

see s.5.4

netconf-zerotouch bootstrap server



Vendor

Entity

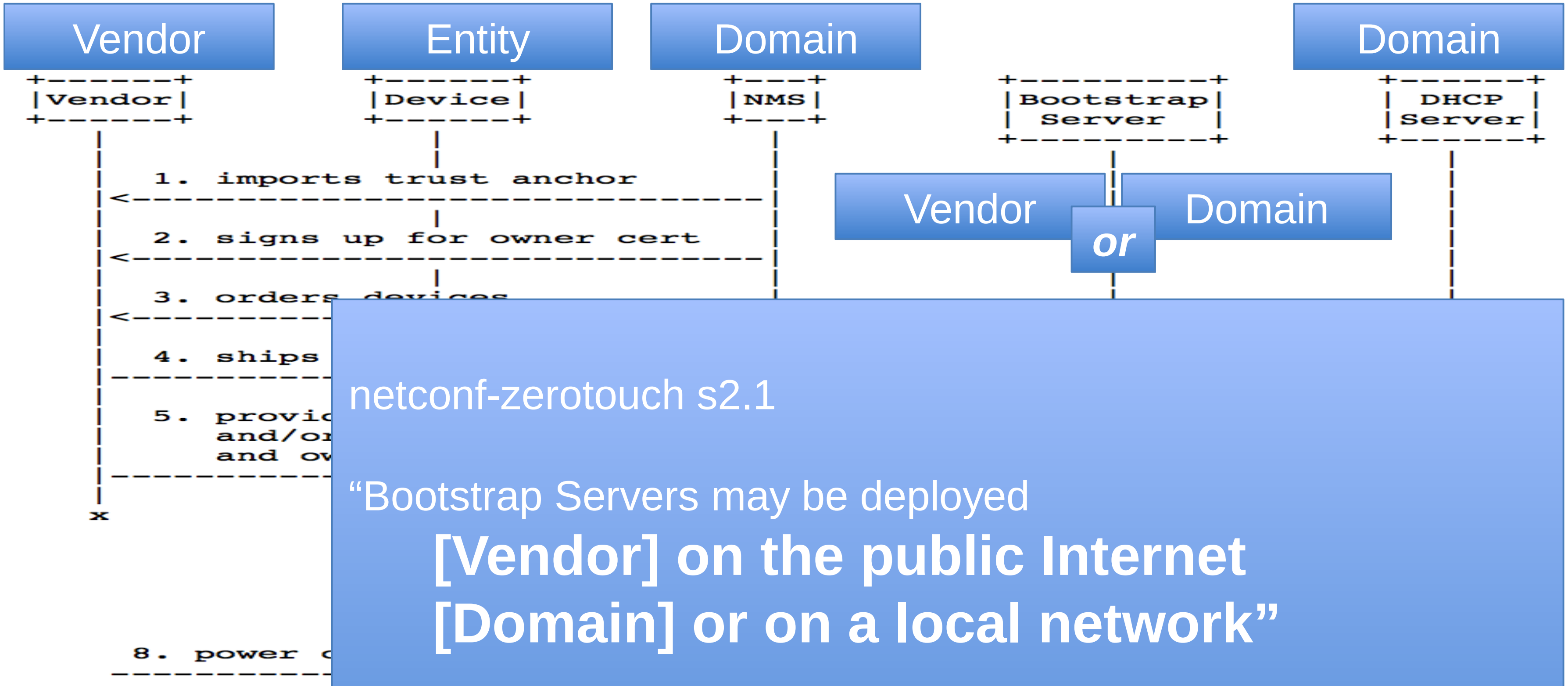
Domain

Domain

```
 +------+        +------+         +---+        +---------+       +------+
 |Vendor|        |Device|         |NMS|        |Bootstrap|       | DHCP |
 +------+        +------+         +---+        | Server  |       |Server|
    |               |               |          +---------+       +------+
    |               |               |               |               |
    |  1. imports trust anchor      |               |               |
    |<------------------------------|               |               |
    |               |               |               |               |
    |  2. signs up for owner cert   |               |               |
    |<------------------------------|               |               |
    |               |               |               |               |
    |  3. orders devices            |               |               |
    |<------------------------------|
    |               |               |
    |  4. ships     |               |
    |-------------->|               |
    |               |               |
    |  5. provides serial-numbers   |
    |     and/or IDevID cert(s),    |
    |     and ownership vouchers    |
    |------------------------------>|               |               |
    |               |               |  6.stage      |               |
    x               |               |    bootstrap  |               |
                    |               |    data       |               |
                    |               |-------------->|               |
                    |               |               |               |
                    |               |  7. stage bootstrap           |
                    |               |     info (optional)           |
                    |               |------------------------------>|
      8. power on   |               |               |               |
     -------------->|               |               |               |
                    | 9. get networking settings and|               |
                    |    staged bootstrap info (if any)             |
                    |---------------------------------------------->|
                    |               |               |               |
                    |               |               |               x
                    | 10. update boot-image, if     |
                    |     needed, and install       |
                    |     config, if valid          |
                    |------------------------------>|
                    |               |               |
                    |               |               x
                    | 11. netconf   |
                    |     call-home |
                    |+------------->|
                    |               |
                    v               v
```

Config Information uploaded to Bootstrap server here

netconf-zerotouch bootstrap server



Vendor

Entity

Domain

Domain

Vendor

Domain

or

netconf-zerotouch s2.1

“Bootstrap Servers may be deployed

[Vendor] on the public Internet

[Domain] or on a local network”

“Devices may be preconfigured with a list of well-known Bootstrap Servers. Additional Bootstrap Servers (i.e. not in the device's preconfigured list) must be **discovered from a DHCP server.**”

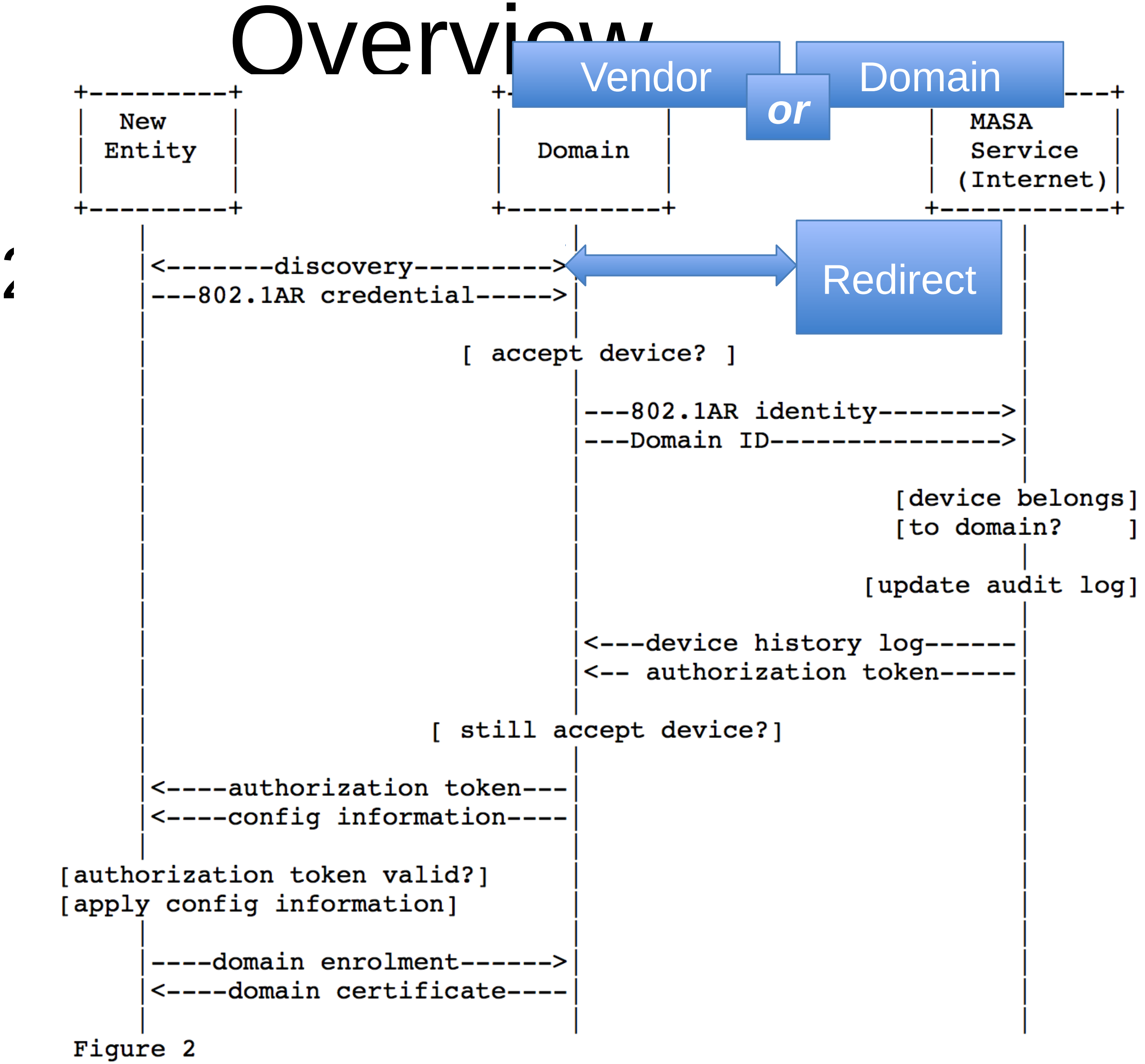
Bootstrap->redirect

- Don’t put (full) config in the bootstrap
  - It is either a security issue [exposes config to vendor]
  - Or a complexity issue [config encryption]

- Make it just a redirect
  - What is in the redirect? A URL?
  - Model after DNS/TLS: No need for security until after redirect?
  - ‘Ownership Voucher’ is sent after redirect
- anima-bootstrapping treats redirect as part of discovery
  - but doesn’t say much about discovery. This is an important enough use case to add…

Aligned with Functional Overview

- Figure 2



```
+----------+                +-                          ---+
|   New    |                |           |             |   MASA    |
|  Entity  |                |  Domain   |             |  Service  |
|          |                |           |             |(Internet) |
+----------+                +-----------+             +-----------+
     |                            |                          |
     |<-------discovery--------->|                           |
     |---802.1AR credential----->|                           |
     |                            |                          |
     |                    [ accept device? ]                 |
     |                            |                          |
     |                            |---802.1AR identity------->|
     |                            |---Domain ID-------------->|
     |                            |                          |
     |                            |                  [device belongs]
     |                            |                  [to domain?     ]
     |                            |                          |
     |                            |                [update audit log]
     |                            |                          |
     |                            |<---device history log-----|
     |                            |<-- authorization token----|
     |                            |                          |
     |                  [ still accept device?]              |
     |                            |                          |
     |<----authorization token---|                           |
     |<----config information----|                           |
     |                            |                          |
[authorization token valid?]      |                          |
[apply config information]        |                          |
     |                            |                          |
     |----domain enrolment------>|                           |
     |<----domain certificate----|                           |
     |                            |                          |
 Figure 2
```

Ownership Voucher vs AuthZ Token

anima-bootstrap	netconf-zerotouch	Notes
nonce		necessary for devices w/o clocks
	created-on, expires-on	allows long term ownership voucher that expire
serial-number	unique-id	allows entity to confirm validation is for itself multi-vendor support might require vendor-id
domain-id <hash of domain pubkey>	owner-id <string> The owner-id value must match the value in the owner-certificate below	domain-id is

Bootstrap Configuration vs Configuration Information

anima-bootstrap	netconf-zerotouch	Notes
Exact format undefined (“from netconf”)		
	Exact format undefined (“using standards-based YANG modules”)	

It is tempting to optimize the msg flow by combining full config here but this author believes we are best served by limiting to just:

- Information necessary to bootstrap key infrastructure
- Information necessary to contact management system

Q&A

-