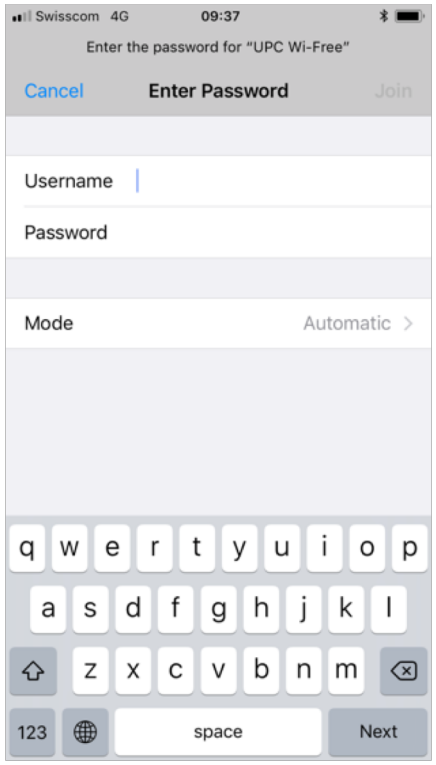
Securing IoT Devices on our networks

Eliot Lear
IETF 103

Why is IoT different?

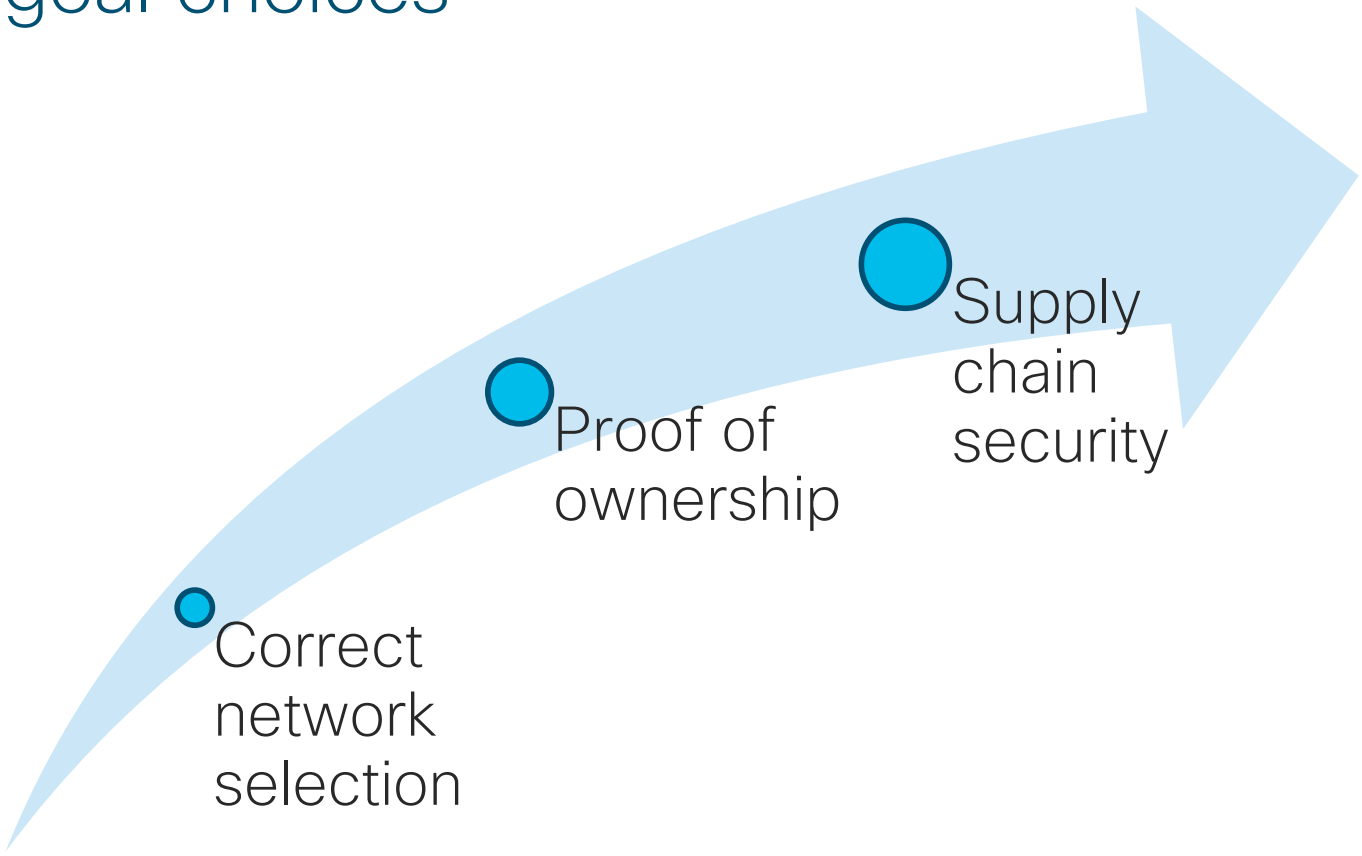


Questions that need answering

What is this thing?	• What is the device's identity? Does this particular thing belong on the network? • What type of thing is it?
Who is responsible for it?	• If something breaks, who should be called?
What access does it need?	• With which devices should it communicate?
Is it doing what it should be doing?	• With which devices is it actually communicating? • Is it behaving as designed?

Steps needed to get a device to join a network

Design goal choices



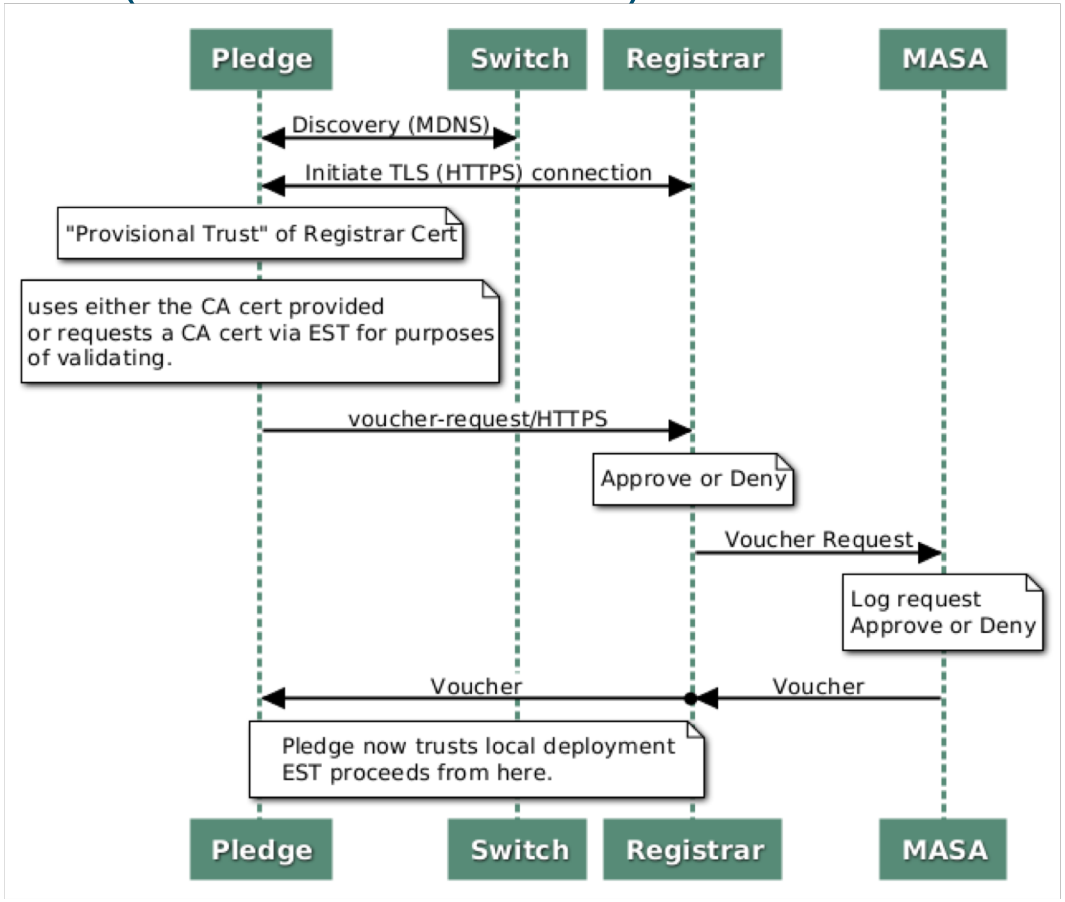
Basic concept: a voucher (RFC 8366)

module: ietf-voucher

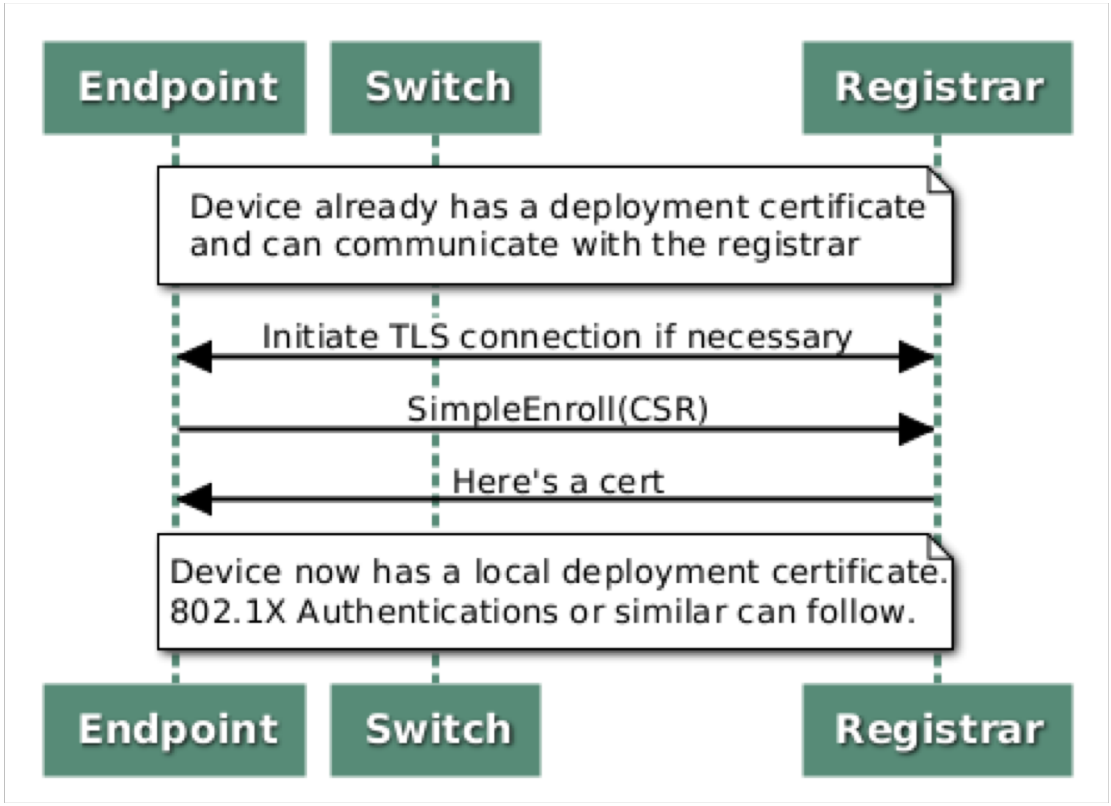
```
yang-data voucher-artifact:
   +---- voucher
      +---- created-on                    yang:date-and-time
      +---- expires-on?                   yang:date-and-time
      +---- assertion                     enumeration
      +---- serial-number                 string
      +---- idevid-issuer?                binary
      +---- pinned-domain-cert            binary
      +---- domain-cert-revocation-checks?  boolean
      +---- nonce?                        binary
      +---- last-renewal-date?            yang:date-and-time
```

Bootstrapping with wired (ANIMA BRSKI)

- Pledge=Device
- Registrar=Store of known devices (tied to AAA infrastructure)
- MASA=”Manufacturer Authorized Signing Authority”
- EST –enrollment over secure transport



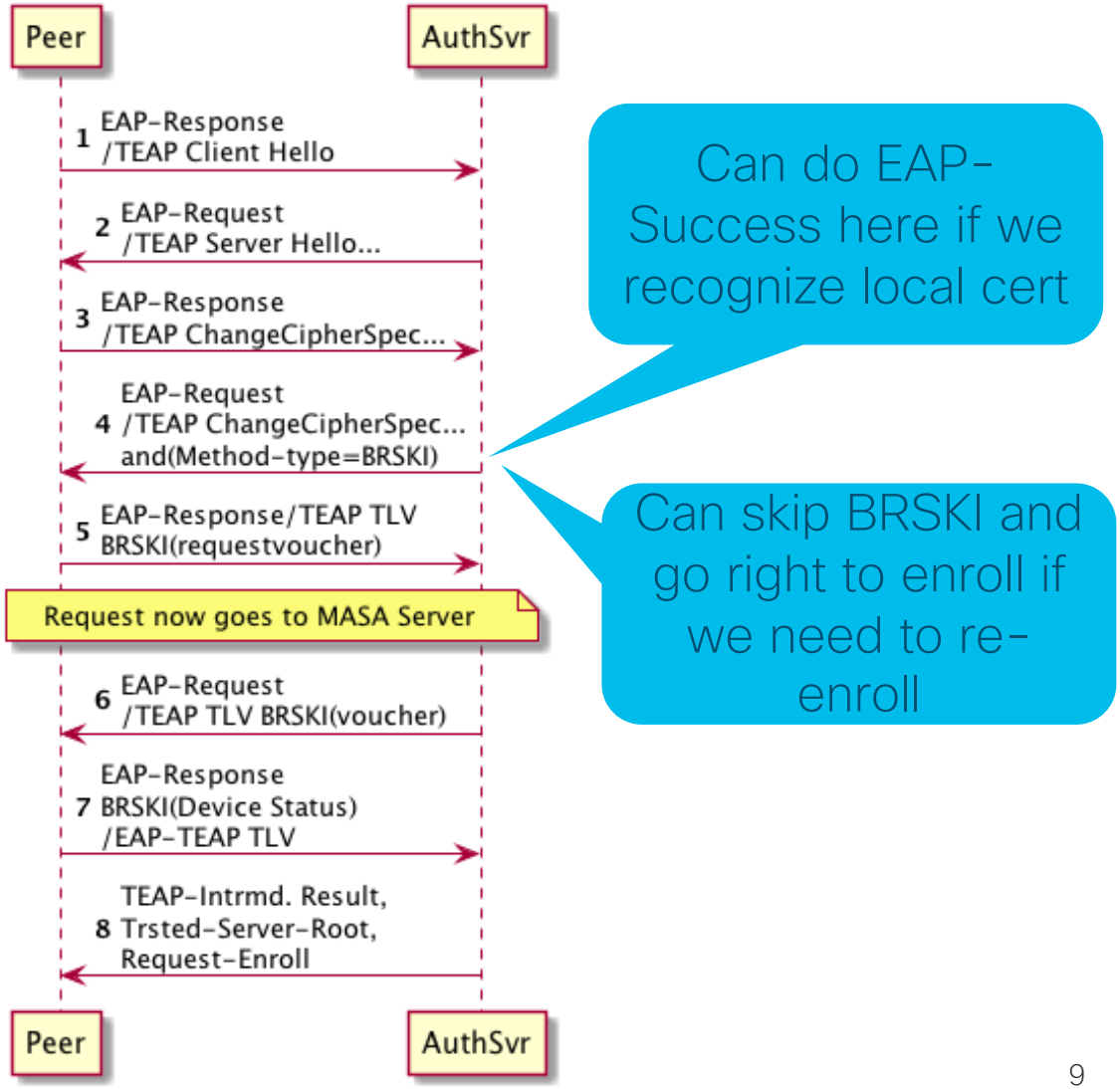
Client gets a certificate via EST (RFC 7030)



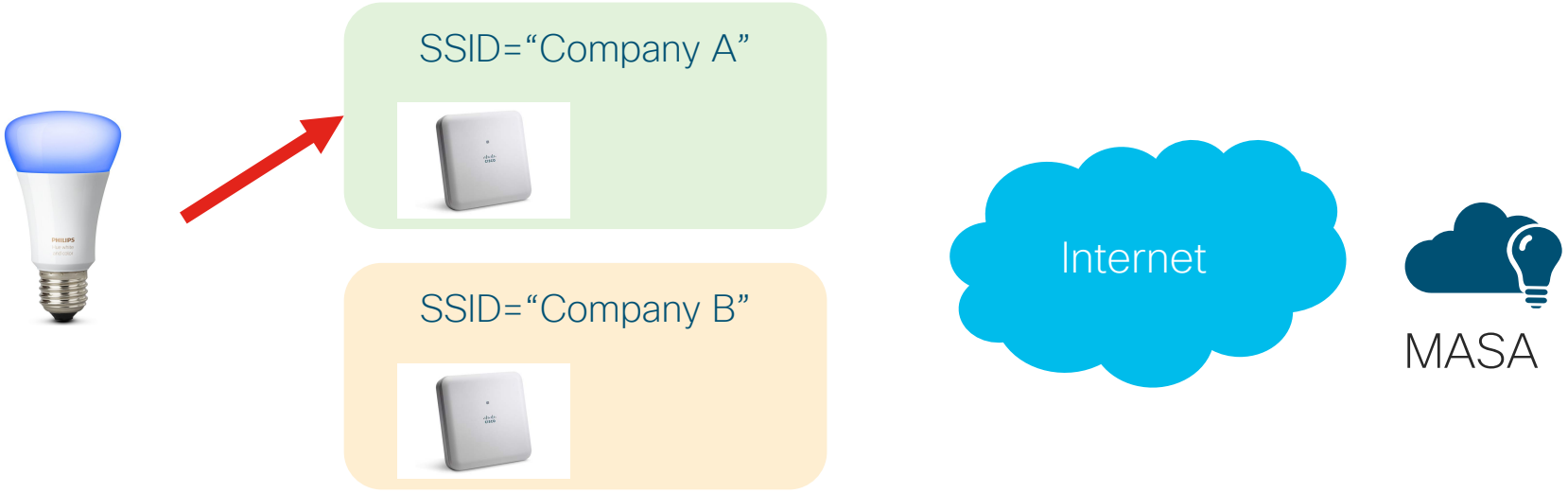
Getting there with wireless

- Use existing management path in the network: EAP
- Keep onboarding capabilities in interface “bring up”
- Reuse as much as possible

draft-lear-eap-teap-brski



Does MASA know lightbulb was sold to Company B?



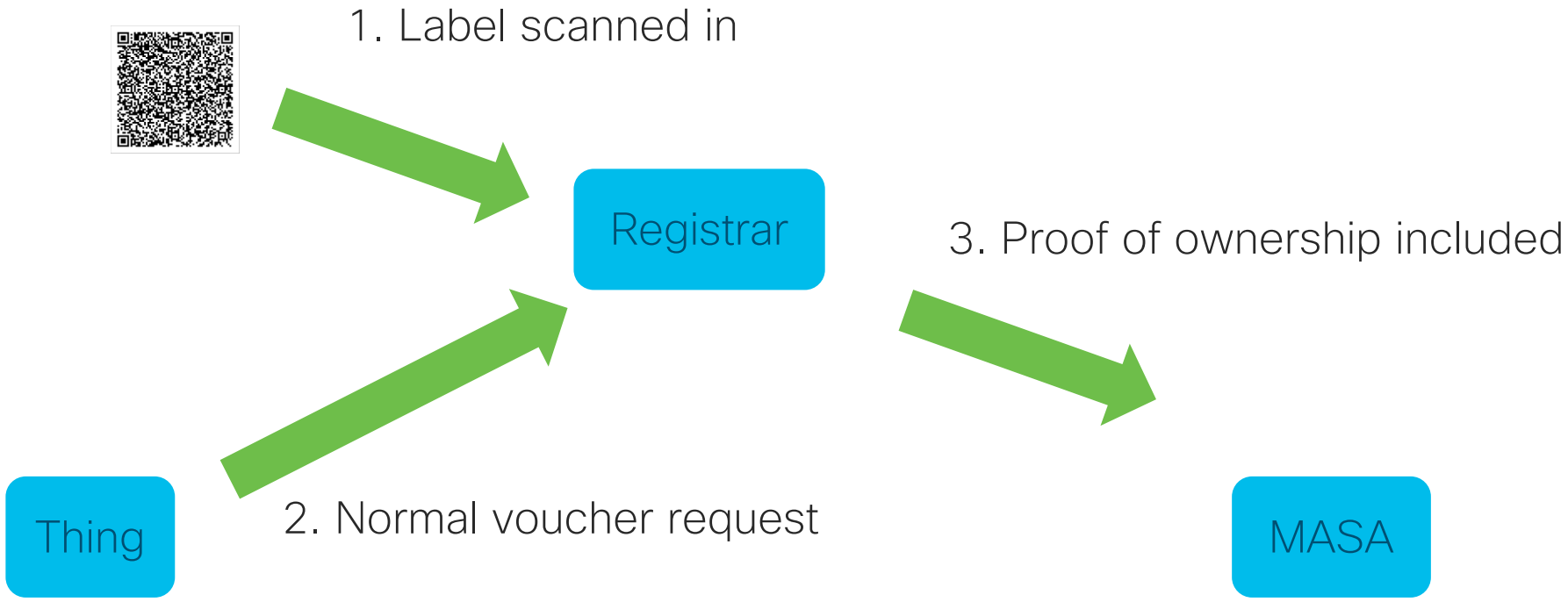
What if the Internet isn't there?

SSID="Company A"

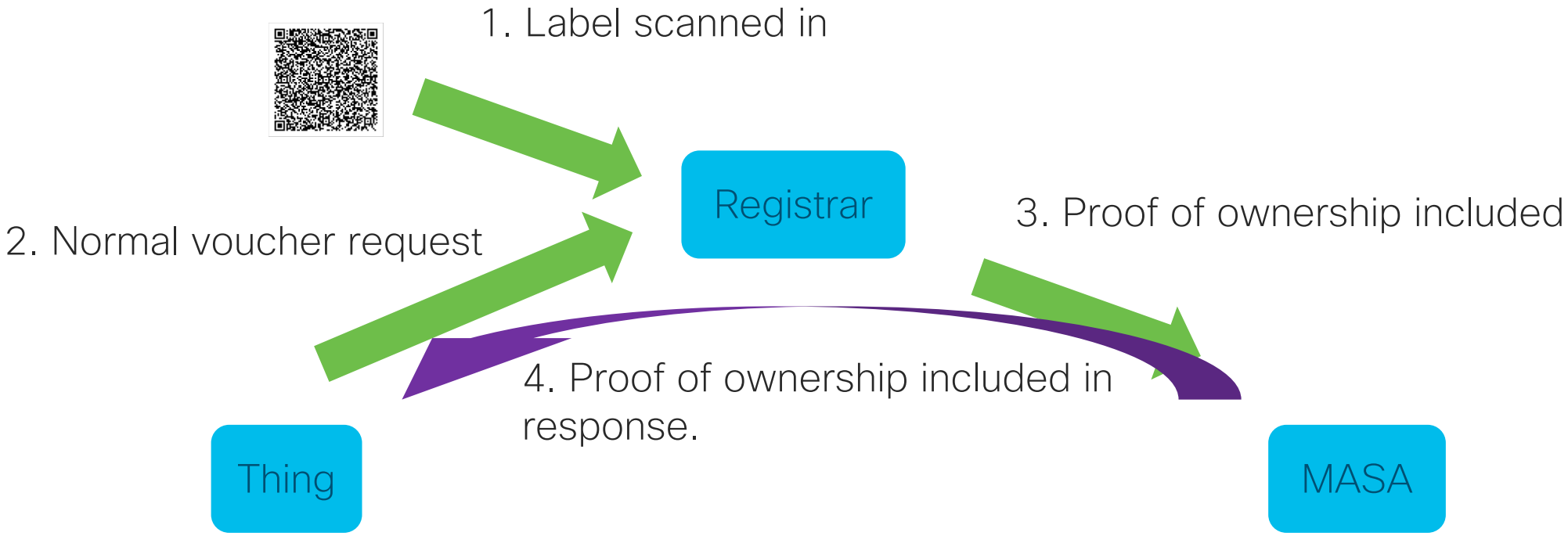
SSID="Company B"

MASA

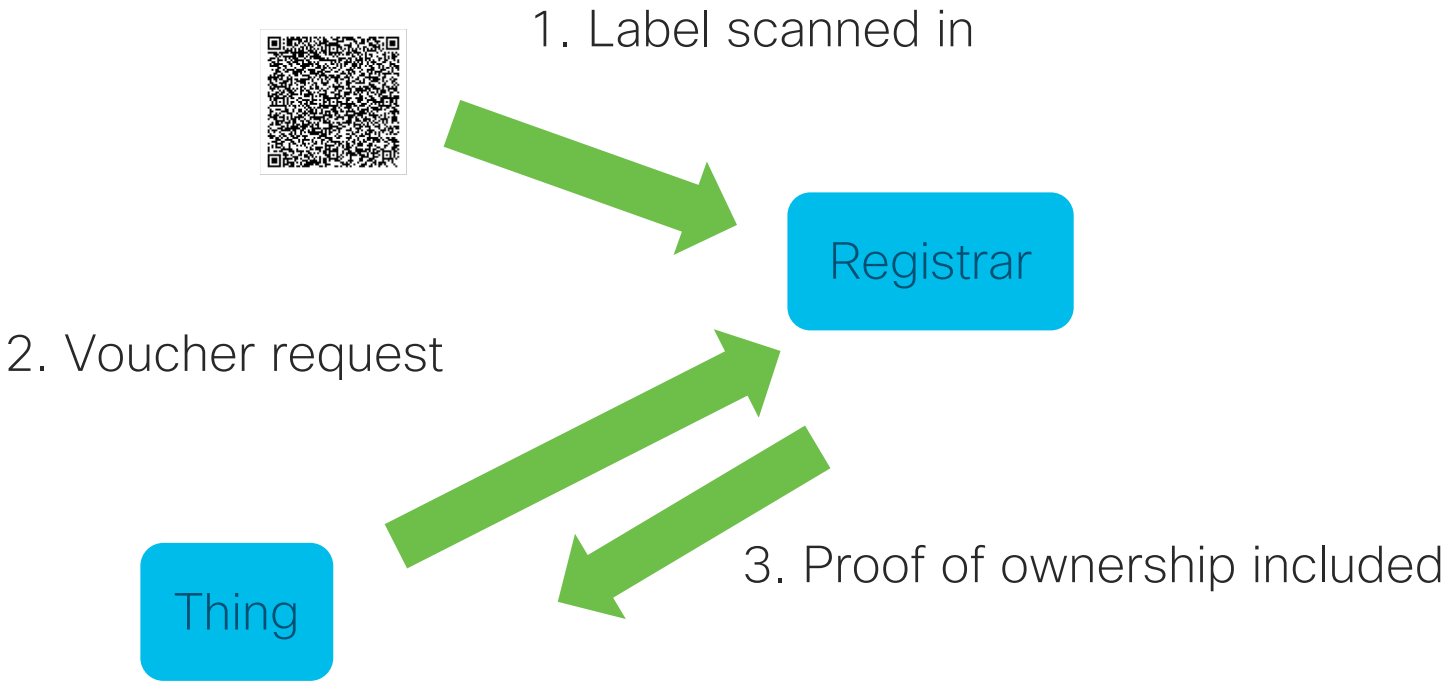
MASA tests proof of ownership



Thing tests proof of ownership



No MASA

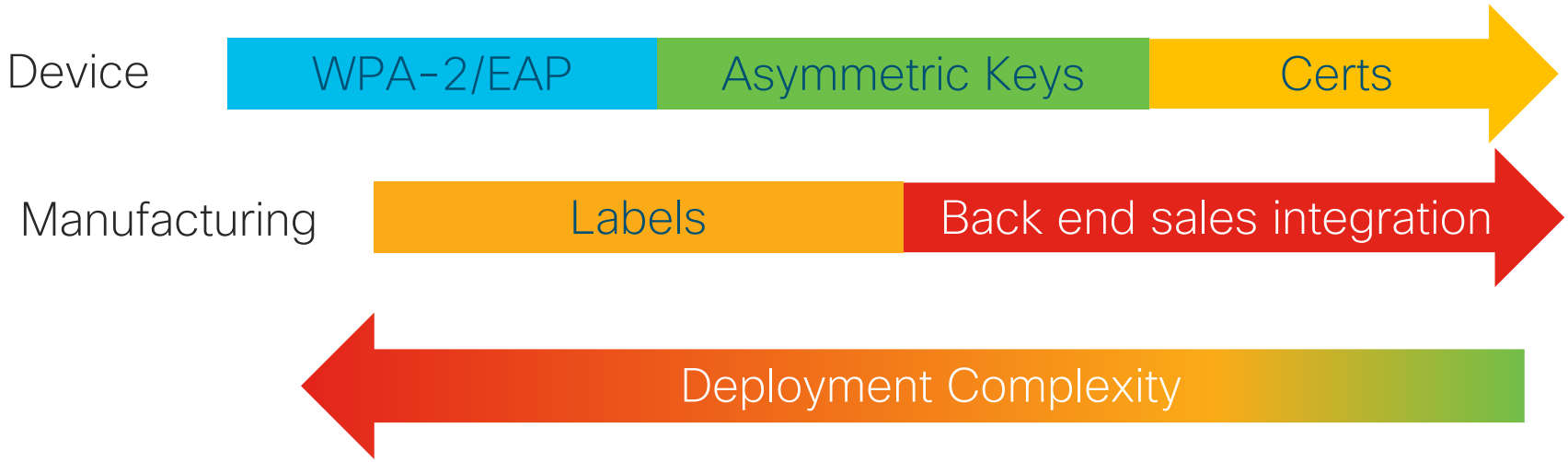

1. Label scanned in
Registrar
2. Voucher request
Thing
3. Proof of ownership included

Approaches to onboarding

	WPS	Simple Serial #	DPP	BRSKI w/ sales integration	BRSKI no sales integration	BRSKI with POP
Correct Network Selection	Yes	Yes	Yes	Yes	No	Yes
Onboard without Internet access	Yes	Yes	Yes	No	No	Yes
Proof of ownership	No	No	No	Yes	Yes**	Yes***
Supply chain security	No	No	No	Yes	Yes***	Partial
Hands free*	No	No	No	Yes	Yes	No
Well secured	No	Maybe	Yes	Yes	Yes	Yes
Status	Here	Not planned	Std	Partially standardized	Partially standardized	Beginning
Key type	None	Ser #	Asym.	X.509	X.509	X.509 + private
Manufacturing complexity	Nvram	Serial#	Public Key + label/BOM	Cert+Back End Integration	Cert	Cert+label/BOM

*Hands free = no label or BOM integration
**Assumes protection of proof of ownership
***Assumes Internet access to enterprise AAA at some point

Lines of complexity



Key Observation

- All of this revolves around a formal assertion handed to the device- **a voucher**
- Making the voucher extensible for different forms of authentication/pop seems ideal

```
yang-data voucher-artifact:
   +---- voucher
      +---- created-on                    yang:date-and-time
      +---- expires-on?                   yang:date-and-time
      +---- assertion                     enumeration
      +---- serial-number                 string
      +---- idevid-issuer?                binary
      +---- pinned-domain-cert            binary
      +---- domain-cert-revocation-checks? boolean
      +---- nonce?                        binary
      +---- last-renewal-date?            yang:date-and-time
```

Questions

- Which methods should we standardize?
  - Thing tests proof of ownership
  - MASA test proof of ownership
  - No MASA involved
- Can manufacturers reasonably use…
  - 802.1X?
  - EAP-TLS/EAP-TEAP?
  - X.509 Certificates?
  - COSE/JOSE objects?
- Can we merge some of these capabilities with EAP-NOOB?

Drafts

- draft-ietf-anima-bootstrapping-keyinfra-16 (core draft)
- draft-friel-anima-brski-over-802dot11-01 (some options)
- draft-lear-eap-teap-brski-01 (BRSKI over EAP)
- draft-lear-brski-pop-00 (proof of possession)