The Tale of Two Protocols: Deep Thoughts on Onboarding Challenges

Eliot Lear

IETF 110

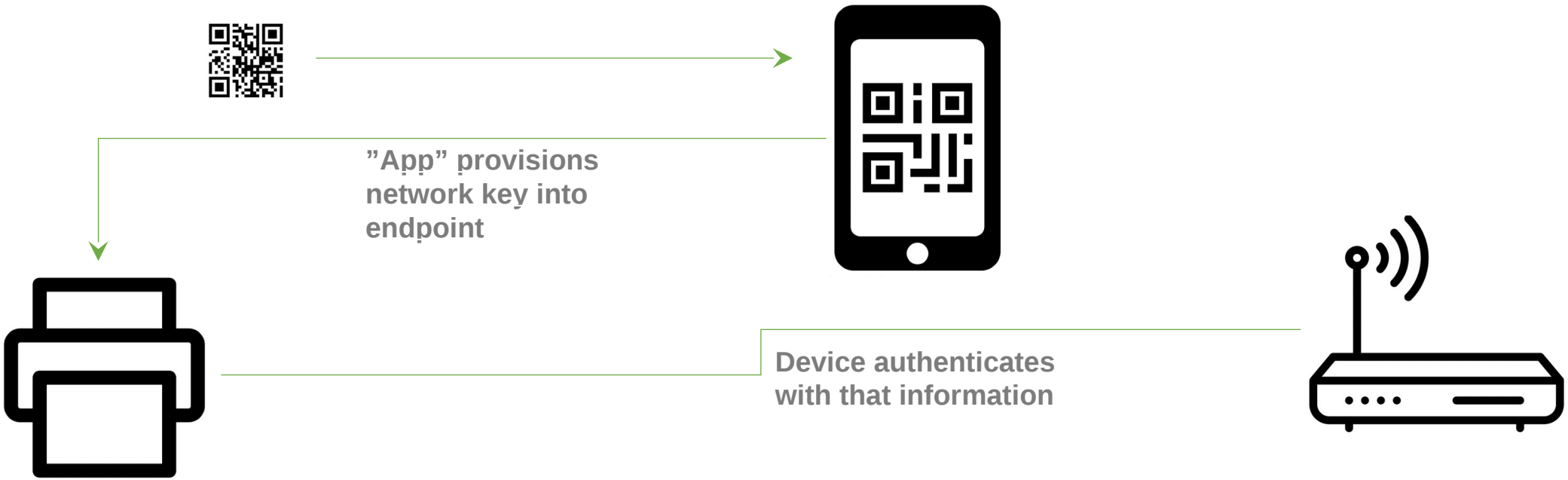
Basic Questions

- How does a device know it should trust a network
- How does a network know that this device is authorized?

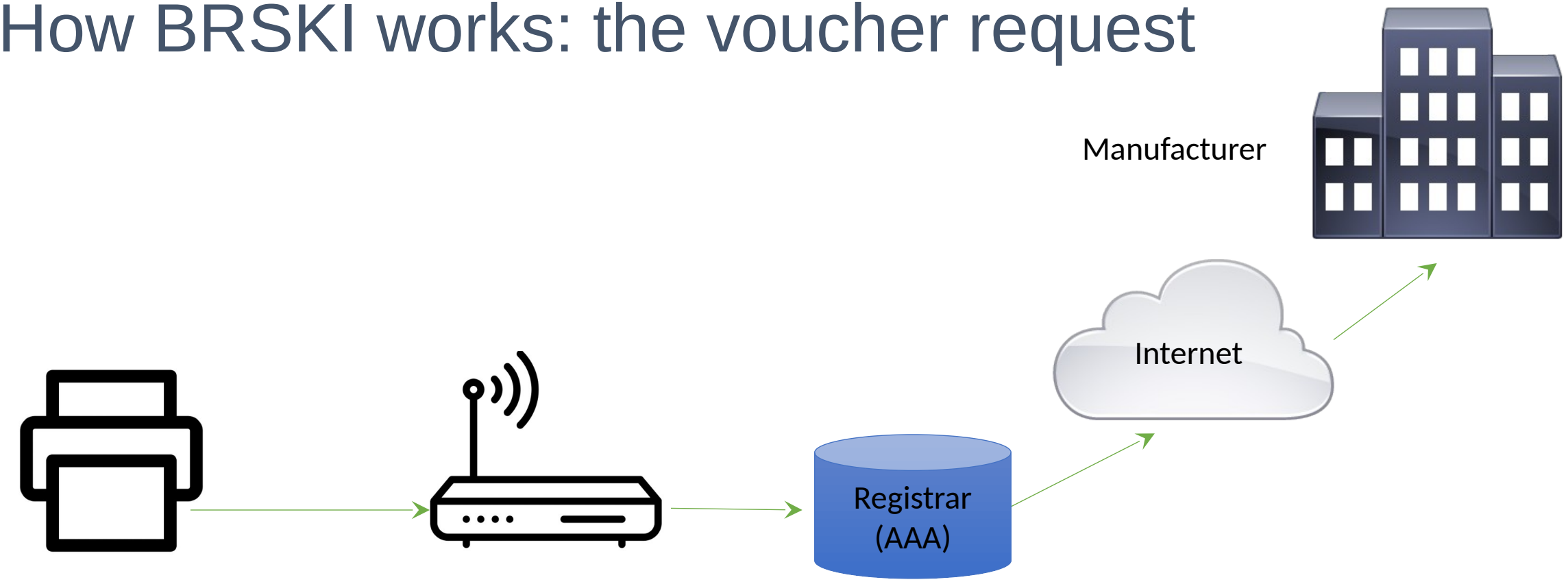
Two protocols:

- DPP – Wifi Alliance’s Device Provisioning Protocol (DPP)
- BRSKI – draft-ietf-anima-bootstrapping-keyinfra

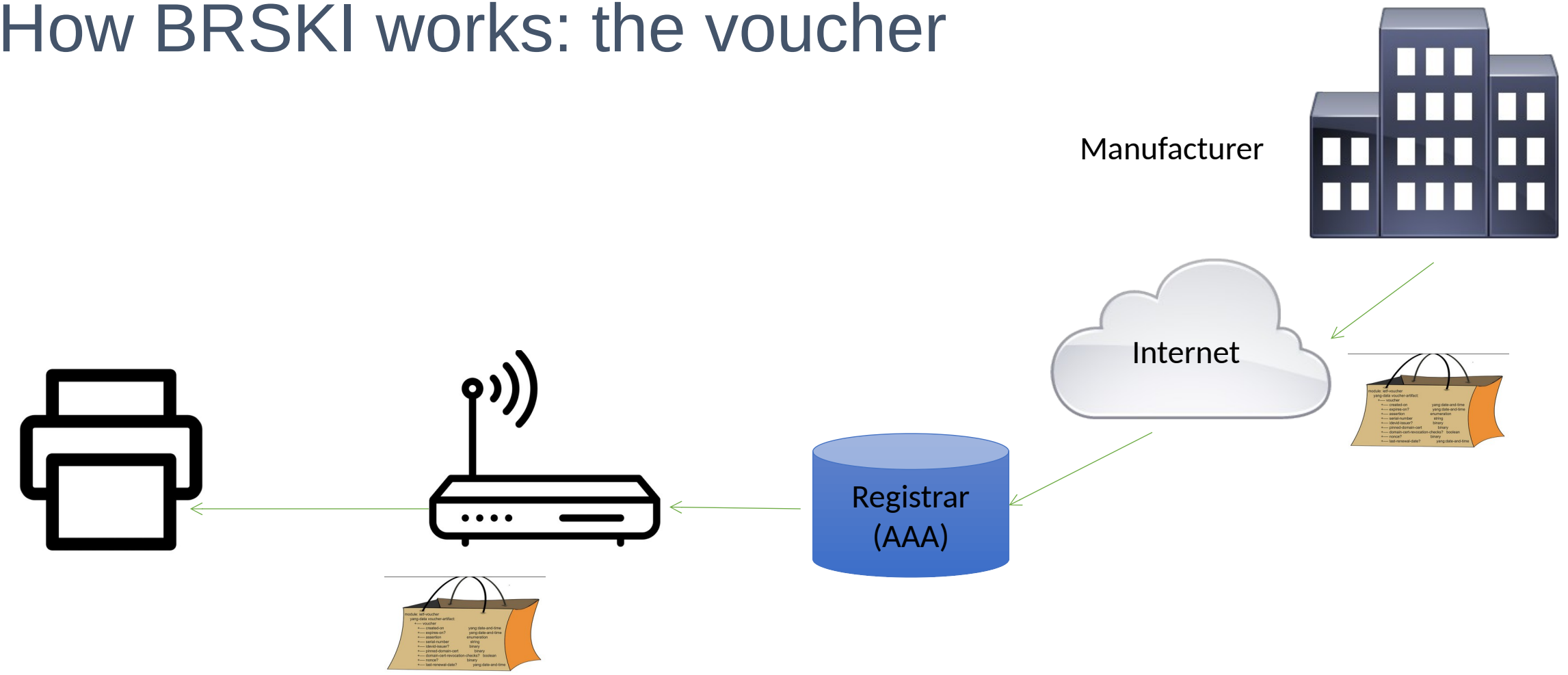
Basic DPP “Consumer” Layout



How BRSKI works: the voucher request



How BRSKI works: the voucher



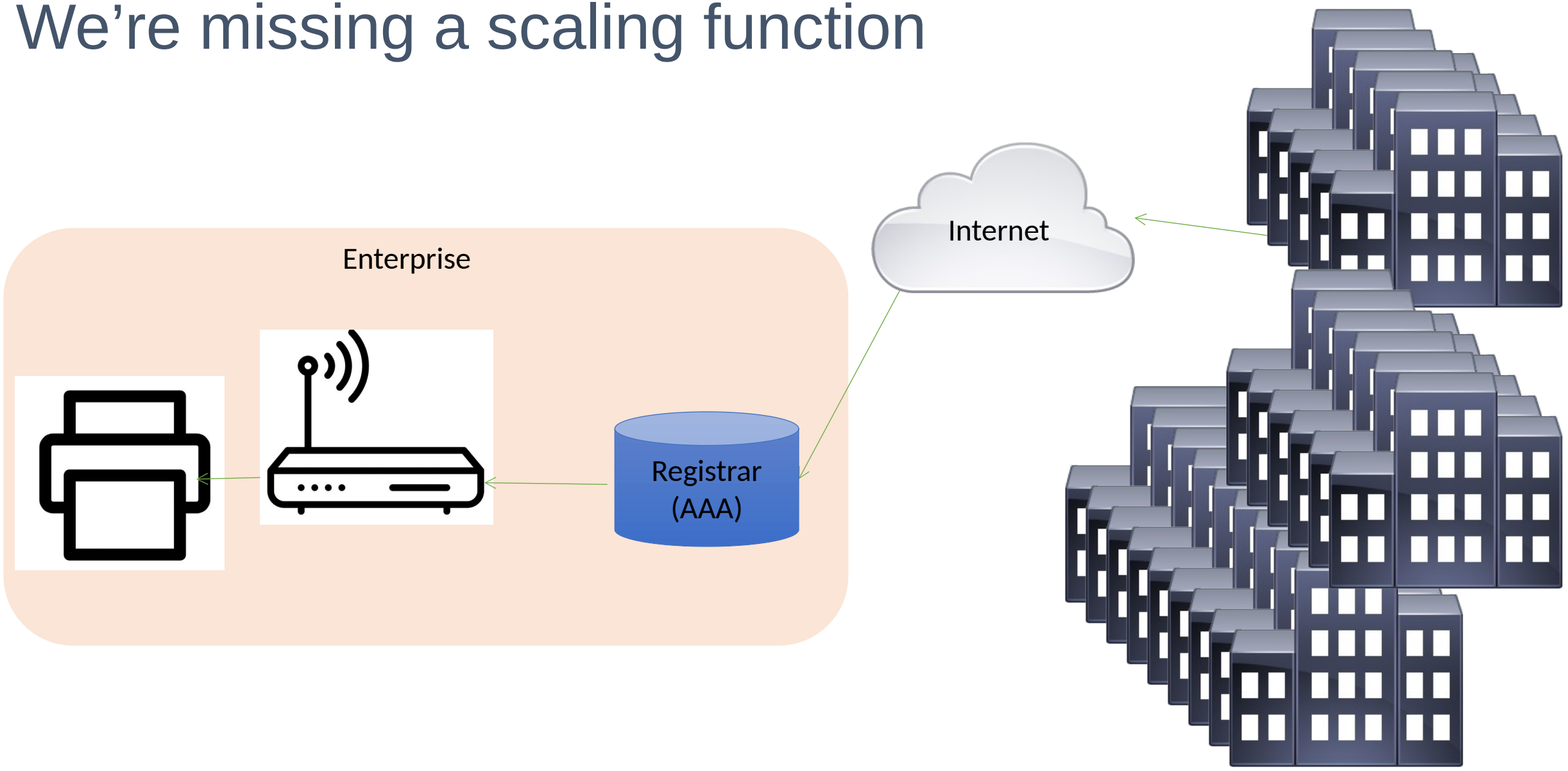
Next Step: provision a deployment certificate

Some Comparisons

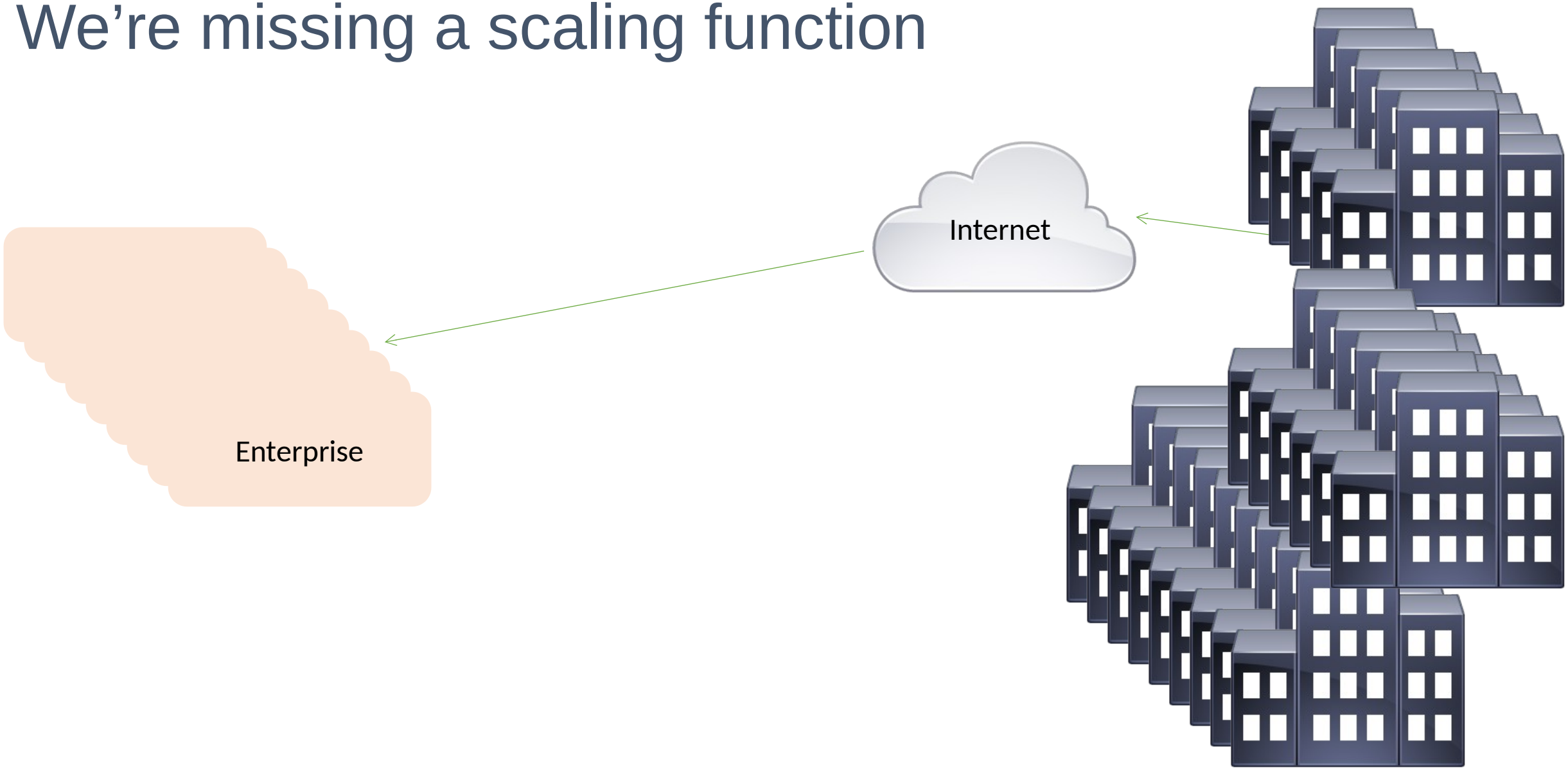
DPP
One step provisioning with an industry standard QR code
Can work with or without Internet connectivity
Ownership transfers are a matter of resetting the device and reusing the QR code
Challenge: how to get to zero step provisioning?

BRSKI
Can be **zero** step provisioning
Requires Internet connectivity
Big challenge: how does MASA bind registrar to a particular purchaser?
How to onboard device without immediate Internet access?

We’re missing a scaling function



We’re missing a scaling function



Some thoughts

- 8366 voucher and DPP key are much closer to the same when credentials are delivered at time of sale.
- The system is much more resilient when onboarding doesn’t require immediate Internet access
  - Requires non-nonced vouchers in BRSKI case
- We need a new architectural element to introduce manufacturer and deployment

  Federations do this nicely.
- This element must be optional