Bootstrapping Key Infrastructures

Max Pritikin
IETF 91, 10 Nov 2014
Aloha!

Security **or** Usability?

Both!

It is a shared problem

- Netconf

  “Develop a zero touch configuration document (a technique to establish a secure…”
- Homenet

  “consider security aspects and the impact on manageability”
- 6tisch

  “zero-touch join: new nodes must recognize the network without explicit provisioning”
- Anima

  “Security has many aspects that need configuration and are therefore candidates to become autonomic.”

And more!

Key exchange requires Integrity

- This is well understood

  http://en.wikipedia.org/wiki/Key_exchange

  "The problem of key exchange has not yet been solved"

- A solution has not being proposed

Build on the methods we have

- Physically secured links
- Previously deployed keys/Trust-Anchors
- ~~Out-of-band channels~~ (discounted due to usability implications)

These are usability challenges
Not everybody can balance rocks

Vendors will do the hard balancing
IETF will make the hard decisions

draft-pritikin-anima-bootstrapping-keyinfra

What are the entities? What do they **do**?

Do:

No user interface
"Zero Touch"
Flexible but fixed behavior

All decisions
No crypto by user

Minimal Decisions
Minimal required behavior
Flexible features
No lock-in (?)

New Entity
e.g. Device

Domain Registrar

Cloud
e.g. Manufacturer

MASA

This is a simplified discussion

draft-pritikin-anima-bootstrapping-keyinfra

What do they **know**?

Know:

Manufacturer TA
802.1AR Certificate
Nonce

Manufacturer TA(s)
Domain TA
Access Control List

Manufacturer TA(s)
Log

Goal: add Domain TA

This is a simplified discussion

draft-ietf-netconf-zerotouch-01

For Comparison

Do:

No user interface
"Zero Touch"
Flexible but fixed behavior

No crypto by user
Build config

s6.2 Ownership validation

New Entity e.g. Device	Domain Registrar	Cloud e.g. Manufacturer
Know:		
Manufacturer TA 802.1AR Certificate	Manufacturer TA(s) Domain TA	**Who owns which device**

Goal: **add config**

Any errors are attributable to me

draft-richardson-6tisch-security-architectur

For Comparison

Do:

No user interface
"Zero Touch"
Flexible but fixed behavior

No crypto by user
Requests cert chain specific to device

s1.4.2 Ownership validation

New Entity
e.g. Device

Domain Registrar

Cloud
e.g. Manufacturer

Know:

Manufacturer TA
802.1AR Certificate

Manufacturer TA(s)
Domain TA

Who owns which device

Goal: **establish TLS**

Any errors are attributable to me

Recap slide

draft-pritikin-anima-bootstrapping-keyinfra

Do:

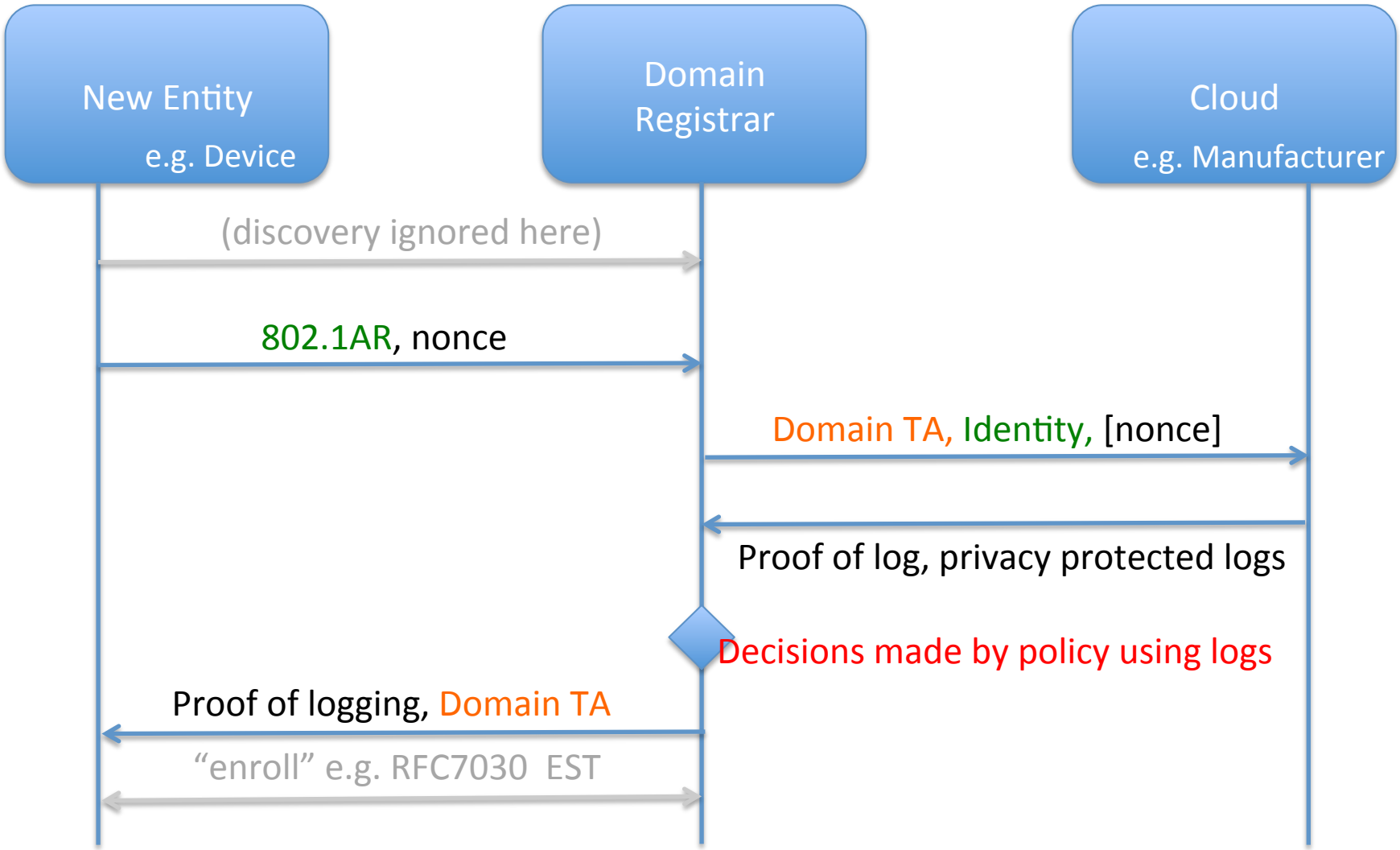
New Entity e.g. Device	Domain Registrar	Cloud e.g. Manufacturer
No user interface "Zero Touch" Flexible but fixed behavior	All decisions No crypto by user	Minimal Decisions Minimal required behavior Flexible features No lock-in (?)
Know:		MASA
Manufacturer TA 802.1AR Certificate Nonce	Manufacturer TA(s) Domain TA Access Control List	Manufacturer TA(s) Log

Goal: add Domain TA

This is a simplified discussion

draft-pritikin-anima-bootstrapping-keyinfra

How?



Benefits

- Flexible Device behavior
- Decisions at Domain Registrar
- Privacy protected logs
  The requirement is that Domain Registrar can recognize unexpected and nonceless log entries
- Flexible Cloud behavior
  Nonceless entries support time shifting
  Greater sales integration allows policy enforcement at the cloud

- Flexible use cases
  Solves bootstrap of key infrastructure
  Anima, NETCONF, Homenet, 6tisch etc can build on this

- Minimum viable feature set is easy to achieve

Thank you