

NETCONF Zero Touch Update for ANIMA

ANIMA WG
IETF #92 Dallas, TX, USA

Issues with Draft -01

1. Owners of equipment had to interact with a 3rd-party to get their configurations signed
 - Loss of privacy

1. Configuration is locked to enumerated set of devices
 - Loss of portability

1. Undefined how a 3rd-party signing entity would validate who is the rightful owner of a device
 - Implies a real-time lookup into a Vendor's database
 - Unclear how this would be easy to implement
 - Draft offered no support

Solution (Draft -02)

Replace 3rd-party signing authority with:

- Rightful Owners can now sign their own configurations
- Devices use Vendor-provided “voucher” to authenticate rightful Owners

Fixes:

1. No more is there a 3rd-party signing entity
2. No more does an initial configuration have to be for an enumerated set of devices
3. No more does Vendor need to provide a real-time lookup service

Security Independent of Bootstrapping Process

- A set of signed files
 - Doesn't matter how obtained (protocol independent)
 - optical, IP, L2, L3, USB flash drive, NFC, etc.
- Zero Touch draft's *protocol* is mostly an HTTPS-based file-server
 - With additional ability for device to post success/failure notifications
- TLS (HTTPS) only used for privacy
 - Any CA trust anchor will do (e.g., VeriSign)
 - HTTP WWW-Authenticate header may be used (if desired)

Owner Places A Zero-Touch Order

Rightful Owner



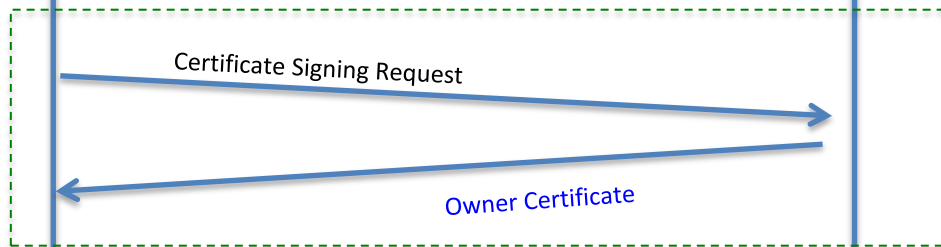
Vendor or Delegate



1st-Time Only

Owner Certificate

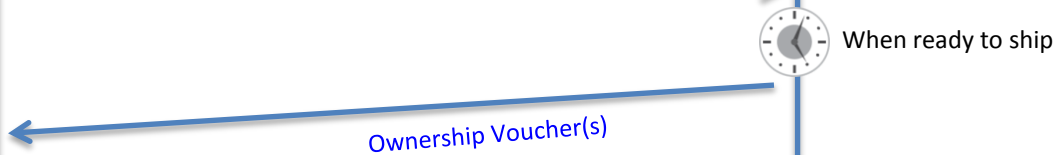
Owner ID: 1234
Owner PubKey
Expiration Date: none
Vendor's Signature



Ownership Voucher

Owner ID: 1234
List of Device IDs
Expiration Date: TBD
Vendor's Signature

Place order ("250 devices + supporting zerotouch data please")



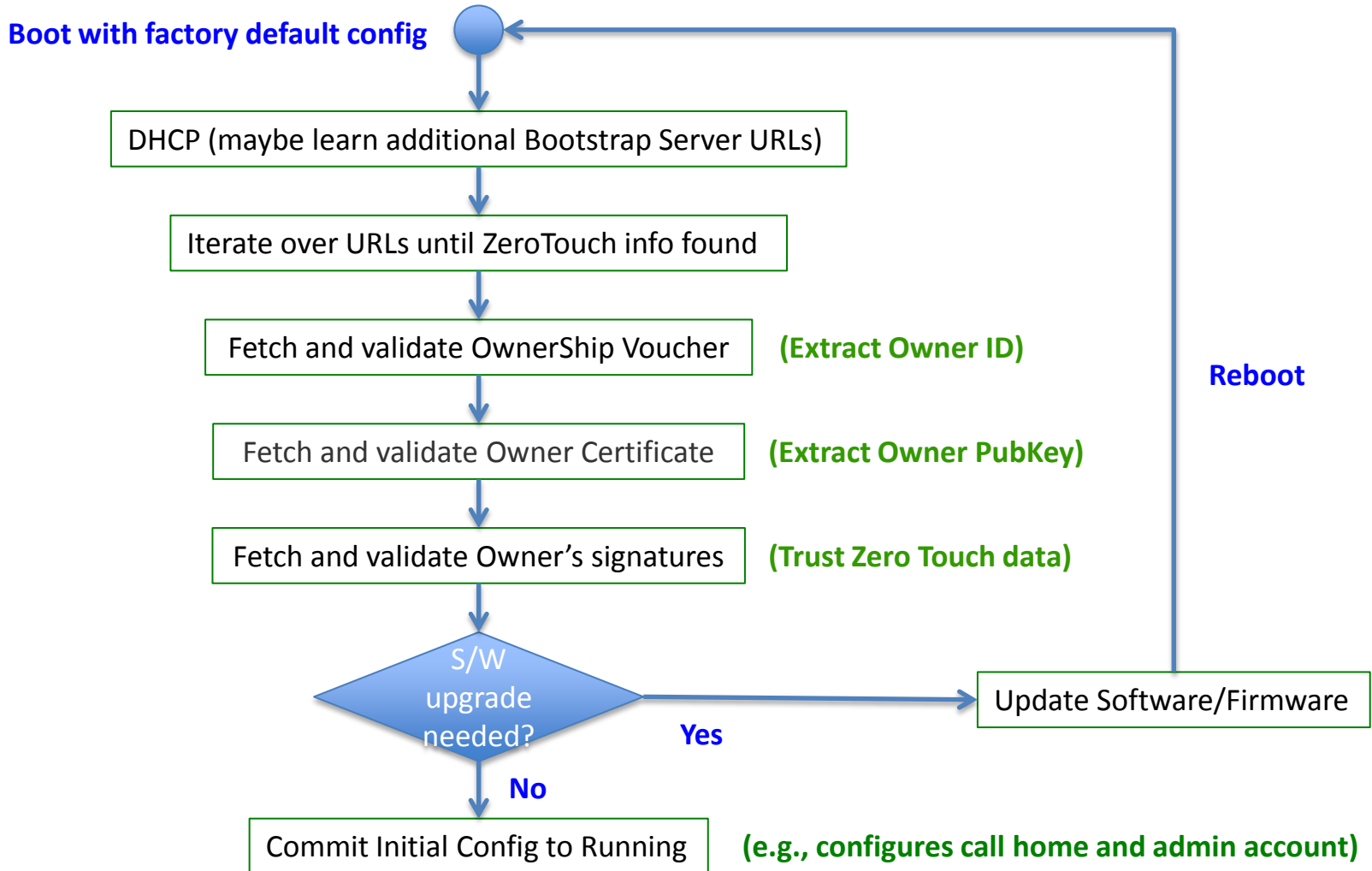
Could be encrypted with the Owner's PubKey, if privacy needed

Owner Stages Network for Zero Touch

1. Update NMS with list of expected device identifiers from [Ownership Voucher\(s\)](#)
2. (Optional) Owner MAY configure a local DHCP server with additional URLs devices should try, with the “ZeroTouch Information” option (IANA assignment pending)
3. Update Bootstrap Server with per-device information:
 - [Ownership Voucher](#)
 - [Owner Certificate](#)
 - Initial configuration, signed by Owner’s Private Key
 - Boot image, already signed by Vendor

All this can be encrypted with Device Public Key if needed

Bootstrap Sequence



Relationship to bootstrapping-keyinfra-01

- Clear Overlap
 - Both drafts begin with device having an IDevID
 - Both drafts involve Manufacturer delegating trust
 - Both drafts end with mutually authenticated trust
- Differences and fuzzy lines
 - Importance of protocol
 - Importance of IDevID certificate
 - Validating data vs. proving identity to the network
 - Ownership voucher vs. MASA
 - Image + config vs. certificate distribution
 - Network infrastructure vs. IoT
 - SDN orchestration vs. autonomic

Meeting in the Middle

- Zero Touch draft definitely should incorporate the progression: link-local → DHCP → DNS
- Bootstrapping draft might leverage Ownership Voucher as a means to implement the MASA
- Both drafts, or another, could define some overarching principles enabling multiple mechanisms
 - E.g., it's OK for a device to have multiple mechanisms, so long as a DoS attack on one doesn't lead to a less-secure mechanism.

Questions / Concerns / Suggestions ?