# Zero Touch Provisioning for NETCONF/RESTCONF Call Home

draft-ietf-netconf-zerotouch-02

NETCONF WG
IETF #92 Dallas, TX, USA

# Issues with Draft -01

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

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

3. Undefined how a 3rd-party signing entity would validate Ownership
    - Implies a real-time lookup into a Vendor's database
    - Unclear how this would be easy to implement
    - Draft offers no support for identifying *who* is making the request or being able to know *which* vendor to ask for a given unique identifier

# 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

# Updates since IETF 91

- Replaced the need for a Configuration Signer with the ability for each NMS to be able to sign its own configurations, using Vendor-signed Ownership Vouchers and an Owner certificate.

- Renamed “Configuration Server” to “Bootstrap Server”, a more representative name given the information downloaded from it.

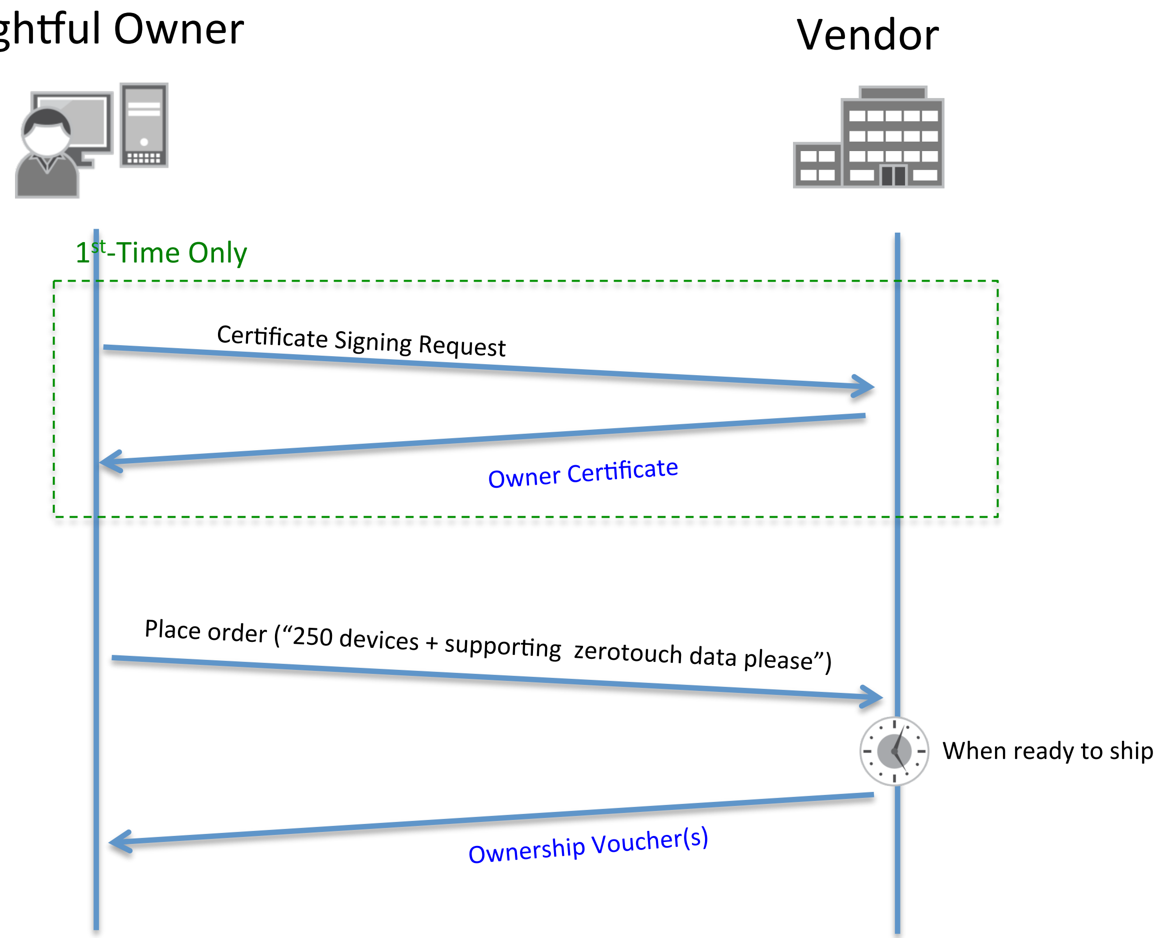
- Replaced the concept of a “Configlet” by defining a southbound interface for the Bootstrap Server using YANG.

- Removed the IANA request for media types.

# Solution Details

draft-ietf-netconf-zerotouch-02

# Owner Places A Zero-Touch Order



Rightful Owner

Vendor

1st-Time Only

Certificate Signing Request

Owner Certificate

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

When ready to ship

Ownership Voucher(s)

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

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 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

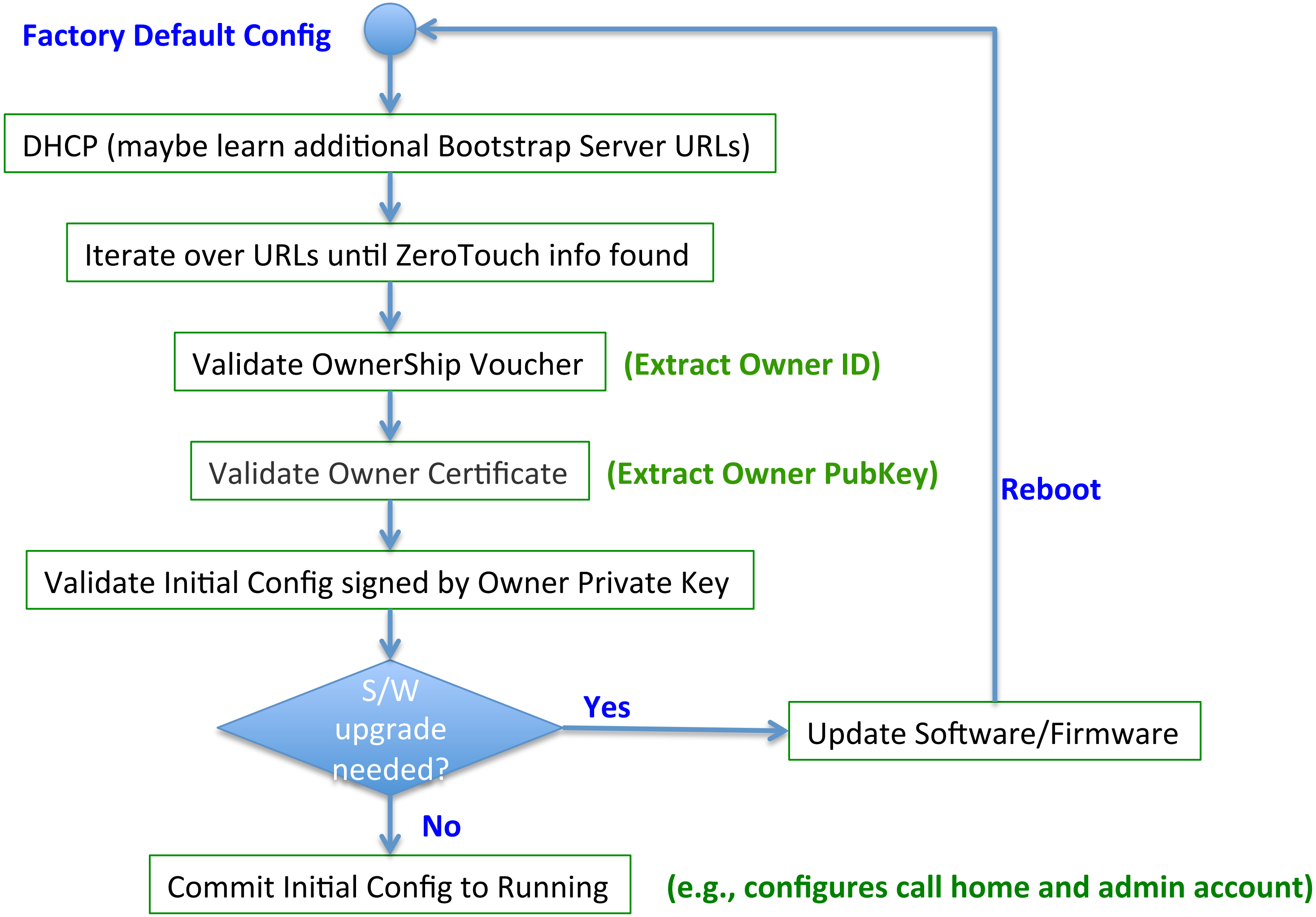
# Bootstrap Server Southbound REST API

```
module: ietf-zerotouch-bootstrap-server
     +--ro devices
        +--ro device* [unique-id]
           +--ro unique-id            string
           +--ro ownership-voucher
           |  +--ro voucher       binary
           |  +--ro issuer-crl?   string
           +--ro owner-certificate
           |  +--ro certificate    string
           |  +--ro issuer-crl?    string
           +--ro boot-image!
           |  +--ro name         string
           |  +--ro path         string
           |  +--ro signature    string
           +--ro configuration
              +--ro config
              +--ro signature    string
  rpcs:
     +---x notification
        +---w input
           +---w unique-id    string
           +---w type         enumeration
           +---w message?     string
```

# Southbound API via RESTCONF

```
GET https://example.com/restconf/data/ietf-zerotouch-bootstrap-server:\
devices/device=123456/ownership-voucher

GET https://example.com/restconf/data/ietf-zerotouch-bootstrap-server:\
devices/device=123456/owner-certificate

GET https://example.com/restconf/data/ietf-zerotouch-bootstrap-server:\
devices/device=123456/boot-image

GET https://example.com/restconf/data/ietf-zerotouch-bootstrap-server:\
devices/device=123456/configuration

POST https://example.com/restconf/operations/ietf-zerotouch-bootstrap-\
server:notification
```

# Bootstrap Sequence



Factory Default Config

DHCP (maybe learn additional Bootstrap Server URLs)

Iterate over URLs until ZeroTouch info found

Validate OwnerShip Voucher

(Extract Owner ID)

Validate Owner Certificate

(Extract Owner PubKey)

Validate Initial Config signed by Owner Private Key

S/W upgrade needed?

Yes

Update Software/Firmware

Reboot

No

Commit Initial Config to Running

(e.g., configures call home and admin account)

# Open Issues for many months

- **#5: Validate if Vendors can support owner-validation service**
  - This is now possible, since draft defines specific requirements

- **#6: Consider alternative to using XMLSIG and XMLENC?**
  - XMLSIG is replaced by a binary-based signing algorithm
  - XMLENC may by replaced as well, but isn’t defined yet (is it important)?

# New Issues just Opened

- #8: Need to define binary-signing algorithm (not XMLSIG)
  - **New** state (will move to **Open**)

- #7: Apply editorial suggestions from on list
  - In **Editorial** state

(Coloring same as on GitHub)

# Next Steps

- Present updated solution to ANIMA WG today
  - immediately after upcoming break!
- Close previously mentioned open issues
  - Any more issues?
- Submit Zero Touch -03 in a few weeks
  - after Call Home and Server Model updates

Questions / Concerns / Suggestions ?