draft-kwatsen-netconf-zerotouch-01

Zero Touch Provisioning for NETCONF Call Home

Introduction

Zero Touch is a strategy for how to establish a secure network management relationship between a newly deployed network element, configured with just its factory default settings, and the new owner's Network Management System (NMS)

Current Status

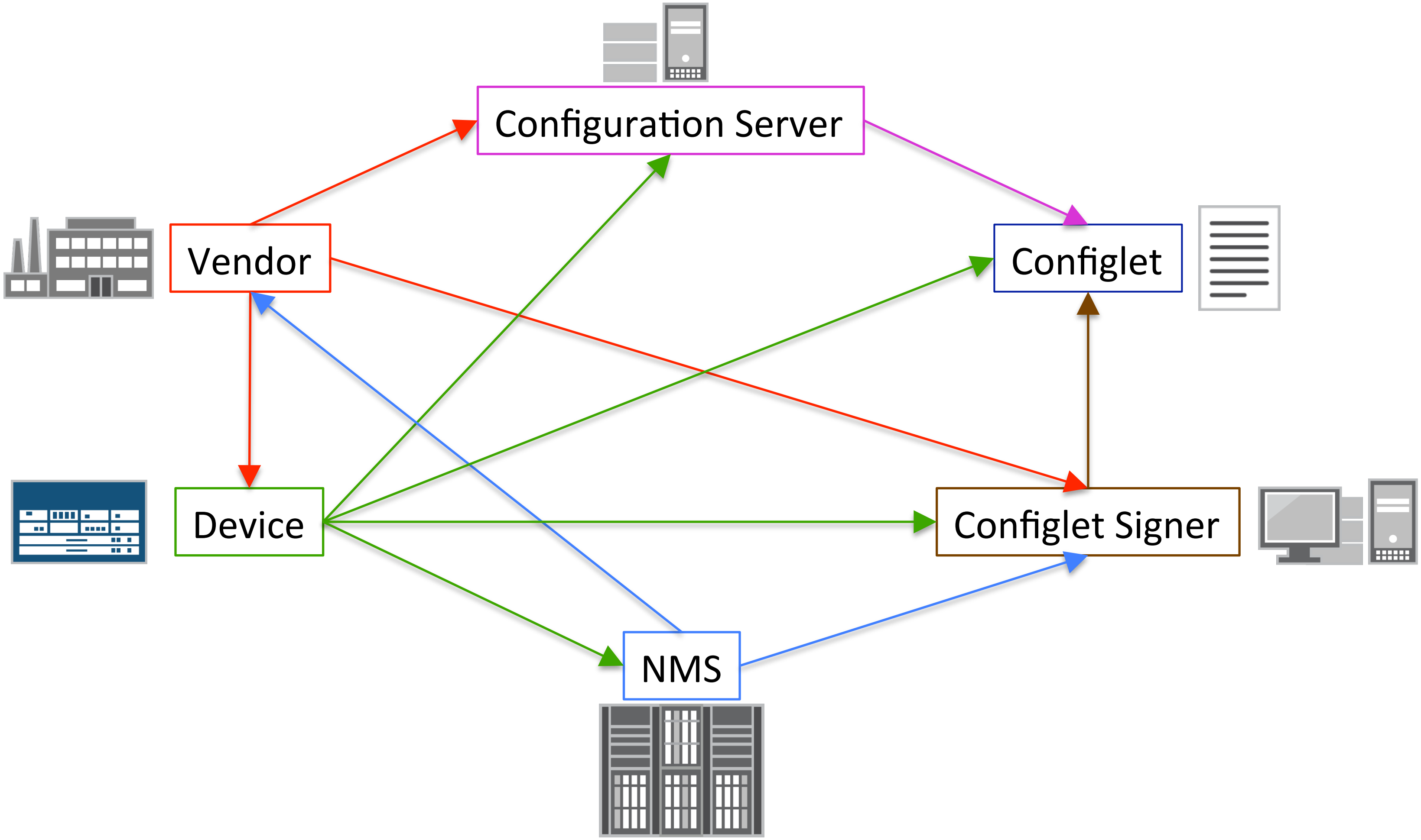
- First presented at IETF 88
  - – Significant interest in the room
    - Now a chartered WG work item

- Many discussions with stakeholders since
  - – Updated draft satisfies almost all interests
  - – New strategy, using “Configlets” instead of DNS
  - – Almost a complete rewrite from -00

Updates since -00

- Device now downloads configuration from URIs, instead of from DNS
- What device downloads is a YANG-defined XML document, instead of DNS records
- Downloaded information authenticated using an enveloped signature, instead of DNSSEC
- Supports delegating the signing and hosting roles to 3rd-parties

Roles and Actors



Device Precondition

```
+-------------------------------------------------------------------+
|                            <device>                               |
|                                                                   |
|     +-------------------------------------------------------+     |
|     |                <immutable storage>                    |     |
|     |                                                       |     |
|     |  list of Configlet Signer trust anchor certificates   |     |
|     |  list of Configuration Server trust anchor certs      |     |
|     +-------------------------------------------------------+     |
|                                                                   |
|   +-----------------------------------------------------------+   |
|   |                    <other storage>                        |   |
|   |                                                           |   |
|   |  two sets of Configuration Server URIs                    |   |
|   |  device entity & associated intermediate certificate(s)   |   |
|   +-----------------------------------------------------------+   |
|                                                                   |
|                    +----------------------+                       |
|                    |  <crypto processor>  |                       |
|                    |                      |                       |
|                    |  device private key  |                       |
|                    +----------------------+                       |
|                                                                   |
+-------------------------------------------------------------------+
```

+ factory default configuration

When joining the network

The device MAY receive a URL to a software image

- The device MAY upgrade itself to this image, but
  - Image MUST be signed and device MUST validate the signature
  - The device MUST reboot itself with factory default configuration
    - To restart Zero Touch…

The device MAY receive URIs to Configuration Servers

- The device SHOULD use these URIs alongside its defaults
  - Precedence given within security schemes

Physical Presence

Before trying to download a Configlet from a Configuration Server

- Device, if it is able to, SHOULD first try to load a Configlet using a mechanism that asserts physical presence
  - E.g. Removable USB flash drive, near-field communication
- Such Configlets
  - Do NOT have to be signed
  - Do NOT have to contain the device's unique identifier

Device Boot Sequence

May also learn
URI for images
and Configlets

```
DEVICE     LOCAL DHCP        CONFIGURATION       NMS
  |          SERVER             SERVERS           |
  |             |                  |              |
  |             |                  |              |
  |------------>|                  |              |
  | Lease IP    |                  |              |
  |             |                  |              |
  |--------------------------+     |              |
  | Check Physical Presence  |     |              |
  |<-------------------------+     |              |
  |             |                  |              |
  |             |                  |              |
  |------------------------------->|              |
  | Iterate until Configlet found  |              |
  |             |                  |              |
  |             |                  |              |
  |----------------------+         |              |
  | Validate Configlet & |         |              |
  | Merge into “running” |         |              |
  |<--------------------+          |              |
  |             |                  |              |
  |             |                  |              |
  |---------------------------------------------->|
  | reverse-SSH or reverse-TLS     |              |
  |             |                  |              |
```

Configuration Server URI Lookup

- Lookup uses fingerprint to identify device
  - For instance, if the URI were:

    https://example.com/zerotouch?id=

  - then the device would try to access:

    https://example.com/zerotouch?id=<fingerprint>

- Fingerprint is generated using the SHA-256 algorithm over the device's entity certificate

Configlet Data-Model

- Reuses groupings from:
  - draft-kwatsen-netconf-server
    - For configuring call-home

- Mimics configuration from:
  - draft-ietf-netmod-system-mgmt
    - For configuring a user account

From draft-ietf-netmod-system-mgmt

```
+--rw system
       +--rw authentication
         +--rw user-authentication-order*   identityref
         +--rw user* [name]
           +--rw name       string
           +--rw password?   crypt-hash
           +--rw ssh-key* [name]
             +--rw name        string
             +--rw algorithm    string
             +--rw key-data     binary
```

From draft-kwatsen-netconf-server

```
+--rw call-home
   +--rw network-managers
      +--rw network-manager* [name]
         +--rw name                  string
         +--rw description?          string
         +--rw endpoints
         |  +--rw endpoint* [address]
         |     +--rw address    inet:host
         |     +--rw port?      inet:port-number
         +--rw transport
         |  +--rw ssh {outbound-ssh}?
         |  |  +--rw host-keys
         |  |     +--rw host-key* [name]
         |  |        +--rw name    string
         |  +--rw tls! {outbound-tls}?
         +--rw connection-type
            ...
         +--rw reconnect-strategy
            ...
```

Configlet Signature

- Enveloped signature using the W3C standard:

  "XML Signature Syntax and Processing”

- Signature block MUST also embed the Configlet Signer's certificate and any intermediate certificates leading to a Configlet Signer trust anchor
  - Because devices only know about trust anchors

NMS Precondition

```
+----------------------------------------+
|                <NMS>                   |
|                                        |
|  vendor's trusted CA certificate       |
|  serial numbers for expected devices   |
|  username to log into devices with     |
|  auth credentials to log into devices  |
|                                        |
+----------------------------------------+
```

NMS needs CA cert and serial-numbers from Vendor

Security Considerations

MANY!

- Substitution attack across devices not possible
- Substitution attack possible on same device
- Confidentiality assured using secure schemes
- Insecure schemes allowed
- Physical presence assertion allowed
- Network discovered URIs are allowed
- Etc.

IANA Considerations

- None

Open Issues

- Can’t reuse a grouping statement from draft-ietf-netmod-system-mgmt
- Should Configlet always be signed?

Questions / Concerns ?