Zero Touch Provisioning for NETCONF/RESTCONF Call Home

draft-ietf-netconf-zerotouch-19

NETCONF WG

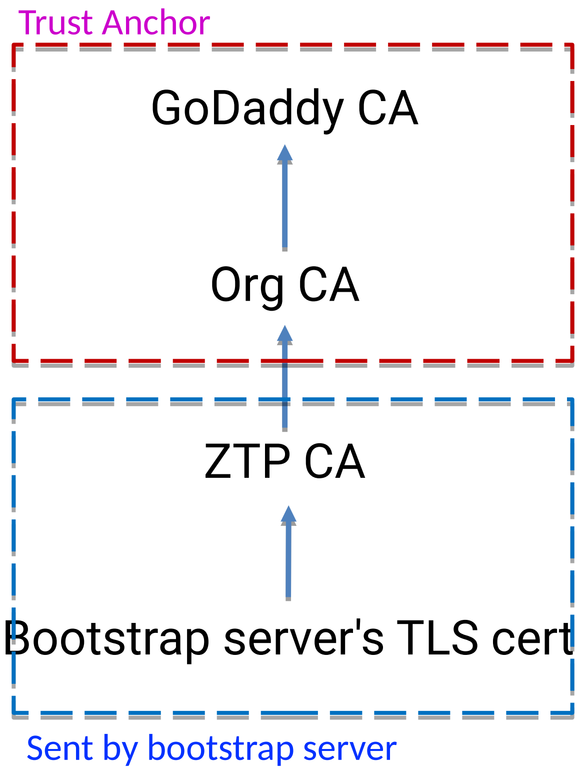
IETF 100 (Singapore)

Updates Since IETF 99

- Reverted back to the device always sending its IDevID certificate to bootstrap servers, even if it doesn’t trust the bootstrap server, as it’s better for the device to give its identity to a potentially bad bootstrap server than it is for the bootstrap server to give device-specific config to a potentially spoofed device.
- Moved data-tree to an RPC (get-bootstrapping-data)
- Added ”untrusted-connection” parameter to the “get-bootstrapping-data” RPC so as to alert the bootstrap server that either signed data (of any type) or unsigned redirect info is needed.
- Added the "ietf-zerotouch-device" module
- Fixed 'must' expressions, by converting 'choice' to a 'list' of 'image-verification', each of which now points to a base identity called "hash-algorithm".

Last Call Comments (1)

Redirect Information needs to support returning a partial certificate chain, rather than just the single root certificate, to support deployments using public CAs.



Trust Anchor

GoDaddy CA

Org CA

ZTP CA

Bootstrap server's TLS cert

Sent by bootstrap server

Proposed Fix:

```
+--:(redirect-information)
   +--ro redirect-information
      +--ro bootstrap-server* [address]
         +--ro address            inet:host
            +--ro port?             inet:port-number
            ~~+--ro trust-anchor?   binary~~
            +--ro trust-anchor?   pkcs7
```

Ideally the pkcs7 type is defined in a module like ietf-crypto-types (discussed more in the Keystore presentation)

Last Call Comments (2)

- The DHCP Option text specifying the allowable URI contents and error handling for the DHCP4&6 options can be improved.

- Proposal:
  - remove a MUST in the URI description
    - so that there is no implication of a server-side processing requirement
  - add language for how clients handle errors when processing a list of URIs.

- Full proposal sent to list.

Final Stretch

All Last Call comments have been addressed on list. It seems that a simple draft-update is all that is needed now before being forwarded to IESG (even if referencing an ietf-crypto-types module).

Any final questions, comments, or concerns?