Zero Touch Provisioning for NETCONF/RESTCONF Call Home

draft-ietf-netconf-zerotouch-13

NETCONF WG

IETF 98 (Chicago)

Recap

- At IETF 97, we reviewed a heavily updated draft with the expectation of being able to have a Last Call shortly.

- All we had to do resolve the “artifact issue”, which was plaguing the ANIMA voucher draft as well.

- The artifact issue did get resolved (using rc:yang-data), which led to a major refactoring to occur within this draft...

Updates Since IETF 97

- defined a standalone artifact to encode the old information-type into a PKCS#7 structure.
- this standalone artifact hardcodes a JSON-encoded instance document (to match the voucher draft).
- merged the previously standalone signature artifact into the above-mentioned PKCS#7 structure (just like SMIME).
- merged the previously standalone certificate-revocations artifact into the owner-certificate artifact (i.e. PKCS#7)
- eliminated support for voucher-revocations, to reflect the voucher-draft's switch from revocations to renewals.

Net-Net: Just 3 Artifacts Now

1. Zero Touch Information
   - a PKCS#7 structure
   - optional embedded signature

2. Owner Certificate
   - a PKCS#7 structure
   - with embedded certificate chain
   - with embedded revocations (optional)

3. Ownership Voucher
   - from ANIMA voucher draft
   - also a PKCS#7 structure

Other News

- Developed a fairly robust unit test to simulate the “removable storage” use case
- Had to write custom ’C’ code to pack/unpack some PKCS#7 structures

Open Issues

1. DHCP Sizing Issues

2. Artifact Signing Strategy

3. Naming Issues

DHCP Artifact Size Issue

- DHCPv4 requires the entire DHCP response to fit inside a single UDP packet (no fragmentation)
- Current approach *can* squeeze an unsigned redirect information artifact (PKCS#7), ~100 bytes to spare.
- Flat binary fields can represent the same information in less space (can relay more redirections)
- But keeping the current artifact definitions enables better support DHCPv6 and also on purpose-built networks.
- Comments?

Artifact Signing Strategy

- Artifacts:
  - ANIMA vouchers
  - Zerotouch bootstrapping data

- Both are *currently* using a signed PKCS#7 structure wrapping a JSON-encoded document.

- But ANIMA is discussing maybe moving to JWT or CWT...

- Should we follow suit or stick with PKCS#7?

Naming Issues

- Zero Touch Information?
  - this is a very lame artifact name!
  - artifact contains
    - redirect-information
    - bootstrap-information
  - Options
    - ZT Boot Data?

- PKCS#7 → CMS

Final Stretch

The draft is ready for Last Call now!

- the open issues are relatively minor.

Any final questions, comments, or concerns?