Zero Touch Provisioning for NETCONF/RESTCONF Call Home

draft-ietf-netconf-zerotouch-11

NETCONF WG

IETF 97 (Seoul)

Recap

- At IETF 96, we reviewed a mildly updated draft and its 7 open issues.

- Happy to report that all 7 issues are now in the REVIEW state (i.e. the fix is in the current draft)

Updates Since IETF 96

11. Factored ownership voucher and voucher revocation to a separate document: draft-kwatsen-netconf-voucher.
12. Removed the <configuration-handling> options 'edit-config' and 'yang-patch', and removed the default value.
13. Defined how a bootstrap server can return signed data (i.e. the XML/JSON encoding issue).
14. Added recommendation for removable storage devices to use open standards based file systems when possible.
15. Replaced the notification-type enumerations "script-[warning/error]" with "[pre/post]-script-[warning/error]".
16. Switched owner-certificate to be encoded using the pkcs#7 format.
17. Replaced the md5/sha1 fingerprints with a sha256, inside a choice statement for future extensibility.

And made a ton of editorial changes (e.g., adding a section on Artifact Groupings), as the entire draft was reviewed with a fine toothed comb.

Open Issues

There are no formal issues open, but...

- I was never able to use the `openssl` command line tool to create just a 'bag of CRLs', which might translate to implementation complexity.

- should likely use CMS instead of PKCS#7 (SEC DIR review?)

- I wonder if draft's use of YANG to define a artifact format is okay.
  - this issue is discussed in the "voucher" draft presentation

- A couple people questioned if operators would accept the solution.

Final Stretch

This draft is ready for last call.

- There is already a request for an early OPS directorate review

- Has anybody implemented, or plan to implement, any part of it?

- Are there any lingering questions or concerns?