RELOAD Base

Status and Changes -- IETF 85
Change 1: Cert Request Auth

• Username and password come from request form, not HTTP auth

• Already clear in 11.3 bullet 1 and following text. No change ...
Change 2: Clarification of hash value in 7.4.3

• Old def:
  hash_value: A digest of the value using hash_algorithm.

• New def:
  hash_value: A digest of the value using hash_algorithm on the value field of the DataValue including its 4 leading length bytes
Change 3: Refresh of finger table in 10.7.4.2

- Clarified text, made base 1 instead of base 0 for search.
Change 4: Delete multi-broad- and any-cast

- Marc is working on it; -24 should have it moved to a separate draft. See slide at end of this deck....
Change 5: Connection table

- Changed “Connection Table” to “Neighbor Table”
Change 6: Signing of configuration table 11.1

- Clarified that configuration file is always signed.
Change 7: Config path name 11.1

- Changed path: 
  
  \./well-known/p2psip-enroll

  to

  \./well-known/reload-config

- Changed DNS SRV name: 
  
  p2psip-enroll

  to

  reload-config

- Change port name, add UDP assignment
Change 8: self-signed certificates with multiple Node-IDs in 11.3.1

- The index of the node-ID MUST be prepended as a 4-byte big-endian integer to the DER representation of the user’s public key and taking the high-order bits.
Other changes

• Updated references and fixed many typos.
• Changed ForwardingOptionsType to ForwardingOptionType (was mixed up)
• Replaced PDU acronym with appropriate nouns
Open Issue 1: Re-issuing certificates

- [S]ection [11].3: "The enrollment server SHOULD maintain a mapping of users to node-ids and if the same user returns (e.g., to have their certificate re-issued) return the same Node-ID, thus avoiding the need for implementations to re-store all their data when their certificates expire."

- How does this work if the user requested multiple certificates from the same login?

- How does this work if the number of Node-Ids requested changes?

- Concluded to take this to list at -84 ....
Open Issue 2
(from notes in XML)

- Check if the Qualcomm IPR issued and if anything can be done
Open Issue 3
(from notes in XML)

• in NODE–MULTIPLE, you need to generate and text all i which seems lame
Open Issue 3
(from notes in XML)

- JoinReq and LeaveReq have a node ID in them and it is a potential confusing and useless – should we remove this.