draft-kk-mpvd-ndp-support-01

MIF WG – IETF88

Jouni Korhonen
Suresh Krishnan
Sri Gundavelli

Background

- A protocol solution proposal for draft-ietf-mif-mpvd-arch using IPv6 NDP.
- Complimentary work to draft-kkb-mpvd-dhcp-support-01

- We assume you read the drafts..

Design choices in -01

- A generic “PVD container/range” NDP option:
  - PVD_CO marks the start of a PVD
  - PVD_ID marks the end of a PVD.
  - Can carry existing NDP options.
  - Carries the PVD Identity, optional security information etc..

- An RA/RS may contain zero or more PVD containers:
  - Multiple PVDs may be in one RA/RS..
  - An RS may contain zero or more PVD containers to solicit information from a specific PVD:

Design choices in -01 cont'd

- Reuse selected parts of existing security mechanisms: SEND RFC6494/6495/3971
  - Does not mandate implementation of SEND, though!
  - Mostly reuse the SEND Subject Key Identifier way of finding public keys.

- Defines the security principles:
  - PVD container content may be signed to prove the authenticity of the advertised information and to provide integrity protection.
  - Replay protection left for the "carrier protocol" to solve.

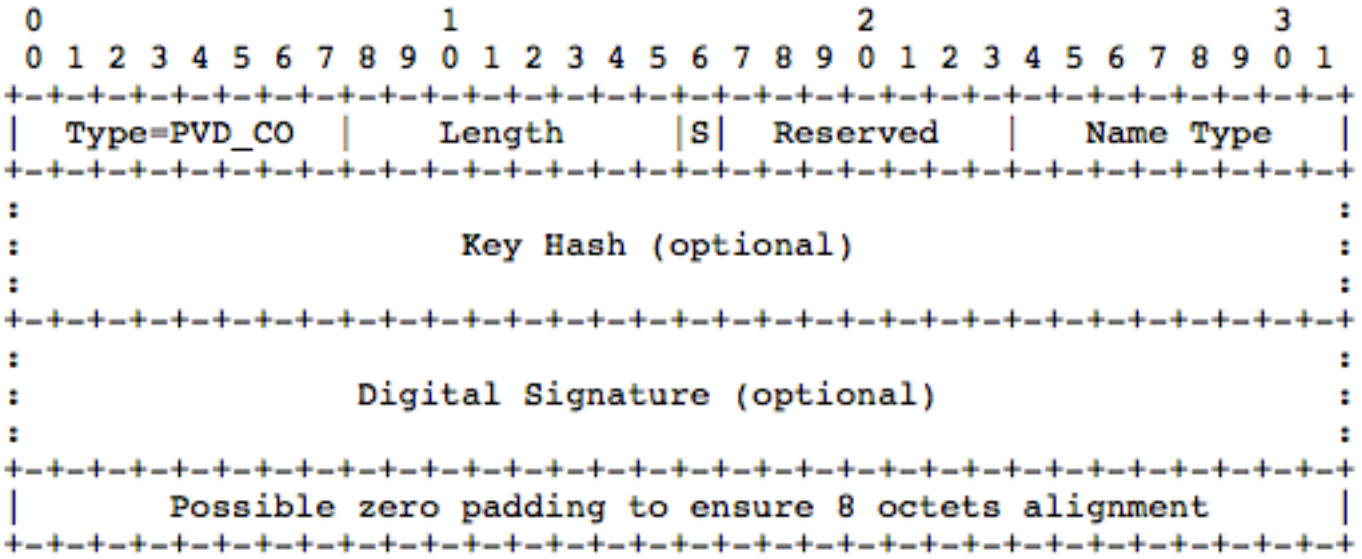
Changes from -00

- Change of PVD_CO option not to contain sub-options but mark the start of options belonging to the PVD.

- Replacing the PVD Identity encodings defined in -00 to a common PVD-ID “blob” defined in draft-kkbg-mpvd-id-00.

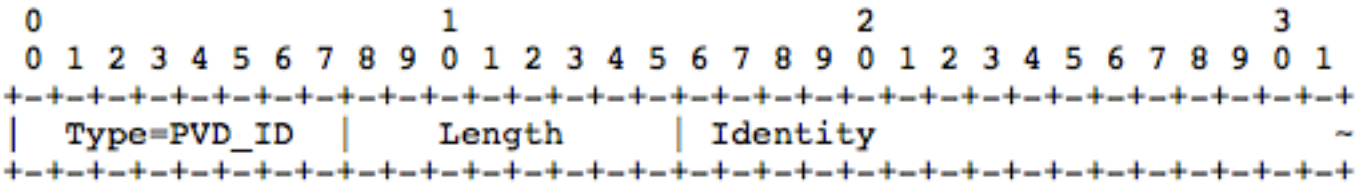
- Minor tweaks..

PVD Container Option



- Marks the starts of ND options belonging to a specific PVD; options follow as-is.
- PVD unaware clients just skip the option and process the subsequent NDP options as any NDP options..
- Option follows the normal ND option padding requirements.

PVD Identifier Option



- Marks the end of NDP options belonging to a PVD identified by the “Identity”.
- PVD unaware clients just skip the option..
- “Identity” is a binary blob, whose encoding is defined in draft-kkbg-mpvd-id.

Issues to think more..

- PVD_CO handling in case of PVD unaware host implementations:
  - Just skip the option and handle “PVD encapsulated” NDP options as any NDP options or.. (now in -01)
  - Craft PVD_CO in a way that an unaware host implementation would skip all “PVD encapsulated” NDP options (doable with PVD_CO Length tweaking).. (was in -00)
- Replay protection as part of the PVD container or left for the “carrier protocol” to deal with?
- Clarifying the case where a router advertises multiple PVDs – how to do signing of options.
- Trust anchors, certificate chains or something else..

Questions ?