GDOIv2

Lakshminath Dondeti

ldondeti@nortelnetworks.com

IETF-60, August 2004, San Diego

GDOIv2

- Based on IKEv2 and GDOI
- No relationship with IKEv2 except it is influenced by that protocol and shares payload and message formats
  - Not a “DOI”; no concept of that in IKEv2
  - Does not share a port with IKEv2 etc.
- Similar to IKEv2, a complete and independent spec

Why another group key distribution protocol?

- A GKD that shares message and payload formats, and code base with IKEv2
  - Has same benefits as IKEv2
    - simple, efficient, secure
    - Complete specification in a single document etc.
- Similar to GDOI for IKE
- Add fixes proposed by Cathy M., to protect against rogue GCKSs gaining illegal access to other secure groups

GDOIv2

- GSA_INIT_EXCH (same as IKEv2)
  - Member→GCKS: M1: HDR, SAi1, KEi, Ni
  - GCKS→Member: M2: HDR, SAr1, KEr, Nr, [CERTREQ]
- GSA_AUTH_EXCH (drawn from IKEv2 & GDOI)
  - Member→GCKS: M3: HDR, SK{ G-ID, IDi, [ID_CERT,] [ID_CERTREQ,] AUTH, [IDr,] [GM_CERT,] [GCKS_CERTREQ,] [POP_I] }
  - GCKS→Member: M4: HDR, SK{ IDr, [ID_CERT,] AUTH, GSA, KD [,SEQ] [GCKS_CERT,] [,POP_R] }

POP payload construction

- POP-HASH-M3
  - "KeyPad:GDOIv2-POP-M3" || Ni-Payload || Nr-Payload || prf(SK_pi, IDi-Payload)
- POP-HASH-M4
  - "KeyPad:GDOIv2-POP-M4" || Ni-Payload || Nr-Payload || prf(SK_pr, IDr-Payload)
- The member or the GCKS signs POP-HASH-M3 or POP-HASH-M4
- Similar to POP construction in GDOI & AUTH payload construction in IKEv2

Next steps

- **Requesting WG standards track status**
- Should be fairly straightforward work:
  - Draws from IKEv2 spec
  - Draws from GDOI and Cathy M.'s analyses of that protocol
  - Add support for emerging requirements, if any