# GDOI Update
# Draft -06

Brian Weis

# GDOI Update Overview

- We asked for review of draft -05 in Anaheim.
  - Yoav Nir provided many useful technical and editorial comments and suggestions
- Draft -06 was published in Mid-July
- Vincent began a WGLC on July 19, closing today
  - Yoav is nearly satisfied with -06
  - Looking for more reviews!

# Summary of changes

- Added Thomas Hardjono as an author
- Re-wrote the Introduction, as the original RFC 3547 text badly needed updating
- Added a small Terminology section, probably should be expanded
- GDOI Applications section was expanded, and some text hinting at possible never realized use cases removed
  - Part of this description includes strategies on when a KS should distribute a KEK and/or TEKs

# Signature Key Usage

- Clarified a SHOULD NOT. Is it enough?

4.1. Use of signature keys

**In order to avoid overusing its authentication signature key,** the GCKS SHOULD NOT use the same key to sign the SIG payload in the GROUPKEY-PUSH message as was used for authentication in the GROUPKEY-PULL exchange.

# LKH

- Additional details describing LKH added (in some cases pointers to sections in RFC 2627
  - Also required moving the description of forward and backward access control nearer the beginning of the GROUPKEY-PULL section.

# GDOI Port Usage

- Clarified which port is used by GDOI (but this may not be clear enough):

**2.1. ISAKMP Phase 1 protocol**

**2.1.2. UDP port**

**IANA has assigned port 848 for the use of GDOI, which allows for an implementation to use separate ISAKMP implementations to service GDOI and IKEv1 [RFC2409]. A GCKS SHOULD listen on this port for GROUPKEY-PULL exchanges, and the GCKS MAY use this port to distribute GROUPKEY-PUSH messages. An ISAKMP phase 1 exchange implementation supporting NAT Traversal [RFC3947] may move to port 4500 to process the GROUPKEY-PULL exchange.**

# GROUPKEY-PULL

- Adjusted the GROUPKEY-PULL payload description
  - Removed optional CERT payload from figure and description
  - Added Delete payload (in text but missing from the figure)

```
Member                                  GCKS or Delegate
------                                  ----------------
                        <---- HDR*, SEQ, [D,] SA, KD, SIG
```

# ECDSA SIG Algorithms

- Better specified the ECDSA algorithms for used with the GROUPKEY-PUSH SIG payload. Algorithms are those from RFC 5903
  - SIG_ALG_ECDSA-256
  - SIG_ALG_ECDSA-384
  - SIG_ALG_ECDSA-521

# Algorithm Selection

- Added an Algorithm Selection section describing requirements on algorithms
- TEK

| Requirement | KEK Management Algorithm |
|---|---|
| MUST | GDOI_PROTO_IPSEC_ESP |

# Algorithm Selection (KEK)

| Requirement | KEK Management Algorithm |
|---|---|
| SHOULD | LKH |

| Requirement | KEK Algorithm (notes) |
|---|---|
| MUST | KEK_ALG_AES with 128-bit keys |
| SHOULD NOT | KEK_ALG_DES (1) |

| Requirement | KEK Signature Hash Algorithm (notes) |
|---|---|
| MUST | SIG_HASH_SHA256 |
| SHOULD | SIG_HASH_SHA1 (2) |
| SHOULD NOT | SIG_HASH_MD5 (3) |

| Requirement | KEK Signature Algorithm (notes) |
|---|---|
| MUST | SIG_ALG_RSA with 2048-bit keys |

# Next Steps

- Document has completed WGLC, but needs more review before progressing
  - Volunteers, please?