GDOI MIB attributes

Sheela Rowles

IETF 74

March 25, 2009

Organization

GDOI MIB

- GCKS Object
  - GCKS configuration
  - GCKS policy
  - GCKS statistics
- GM Object
  - Configuration
  - Policy
  - Statistics

GCKS configuration

- KEK policy
  - Encryption algorithm
  - Hash algorithm
  - Rekey Lifetime
  - Retransmission Lifetime
- TEK Policy
  - Transform
  - Hmac algorithm
  - IPsec lifetime
  - Tunnel/transport

- Global Policy
  - List of groups

GCKS policy

- KEK
  - SPI
  - Group Members registered
  - Last sequence number sent

GCKS statistics

- Number Group Members registered
- Number Group Members re-registered
- Number Rekeys sent for a group

Group Member Configuration

- Group Identity
- List of configured key servers

Group Member Policy

- Key Server address
- Downloaded KEK policy
  - SPI
  - Encr algorithm
  - Hash algorithm
  - Remaining lifetime
- List of TEKs
  - SPI
  - Flow to be protected
  - 2407 SA attributes

Group Member Statistics

- Number of re-registration attempts
- Number of rekeys received
- Last sequence number

Next Steps

- Is this a reasonable item for the WG to take on?

- There are no standardized IKE or IPsec MIBs