MIB Specification for GDOI Protocol

By

Kavitha Kamarthy
GDOI MIB Draft

• Defines a high level Management Information Base for Group Domain of Interpretation (RFC 3547)

• GDOI is used to establish secure group communications in IPSec VPNs.
Why standardize GDOI MIB

• GDOI is a standard (RFC 3547)
• Management is a very important aspect for the administrators
• Using a standardized GDOI MIB will help manage devices independent of vendor who manufactured the devices.
SNMP Components

• **Agent**: Software module that resides in a managed device and respond to manager requests for data object values and send notifications to managers.

• **Managed Device**: A network node that contains an SNMP agent and resides on a managed network.

• **Management entity/Managers**: responsible for communicating with networked devices that implement SNMP agents.
SNMP Components (cont)

• **MIB** describes data objects and notification objects to be managed by an agent within a device
SNMP Components
GDOI Definitions/Terminology

• **Group**: Uniquely identified by group identity and defines group security policies

• **Group Member**: Entity that registers to the Key server to download the policies

• **Group controller/Key Server**: Entity that holds the policies of the group and sends rekeys on new policies to the Group Members
GDOI Definitions/Terminology (cont)

- GDOI: protocol that runs between a group member and key server and establishes security associations among authorized group members
- TEK: Traffic Encrypting Key
- KEK: Key Encrypting Key
Structure of GDOI MIB Module

- GDOI Group
  - Group Member
    - KEK SAs
    - TEK SAs
  - Key Server
    - KEK SAs
    - TEK SAs
Tables Defined

• **Group Table** *(gdoiGroupTable)* – Sequence of GdoiGroupEntry

• **Key Server Table** *(gdoiKeyServerTable)* - Sequence of GdoiKeyServerEntry

• **Group Members Table** *(gdoiGmTable)* – Sequence of GdoiGmEntry
Tables (cont.)

• **Key Server KEK policy Table** (gdoiKsKekTable) – Sequence of GdoiKsKekEntry

• **Key Server TEK Policy Table** (gdoiKsTekTable) – Sequence of GdoiKsTekEntry

• **Group Member KEK policy Table** (gdoiGmKekTable) – Sequence of GdoiGmKekEntry

• **Group Member TEK Policy Table** (gdoiGmTekTable) – Sequence of
Key Server Notifications

- gdoiKeyServerNewRegistration
- gdoiKeyServerRegistrationComplete
- gdoiKeyServerRekeyPushed
- gdoiKeyServerNoAuthenticationKeys
Group Member Notifications

- gdoiGmRegister
- gdoiGmRegistrationComplete
- gdoiGmReRegister
- gdoiGmRekeyReceived
- gdoiGmIncompleteCfg
- gdoiGmNoIpsecFlow
- gdoiGmRekeyFailure
Request

• Is this WG willing to take on this work?