GSAKMP Policy Token Spec

Draft-ietf-msec-tokenspec-sec-00.txt

Presented by Hugh Harney

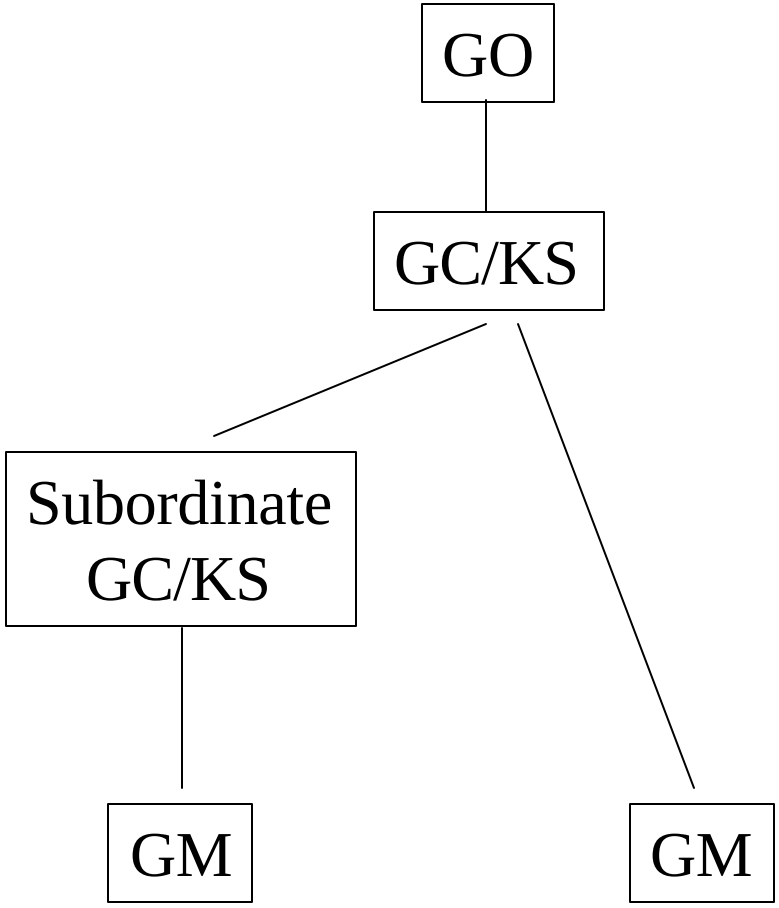
SPARTA, Inc.
(410) 872-1515 x203
hh@sparta.com

Agenda

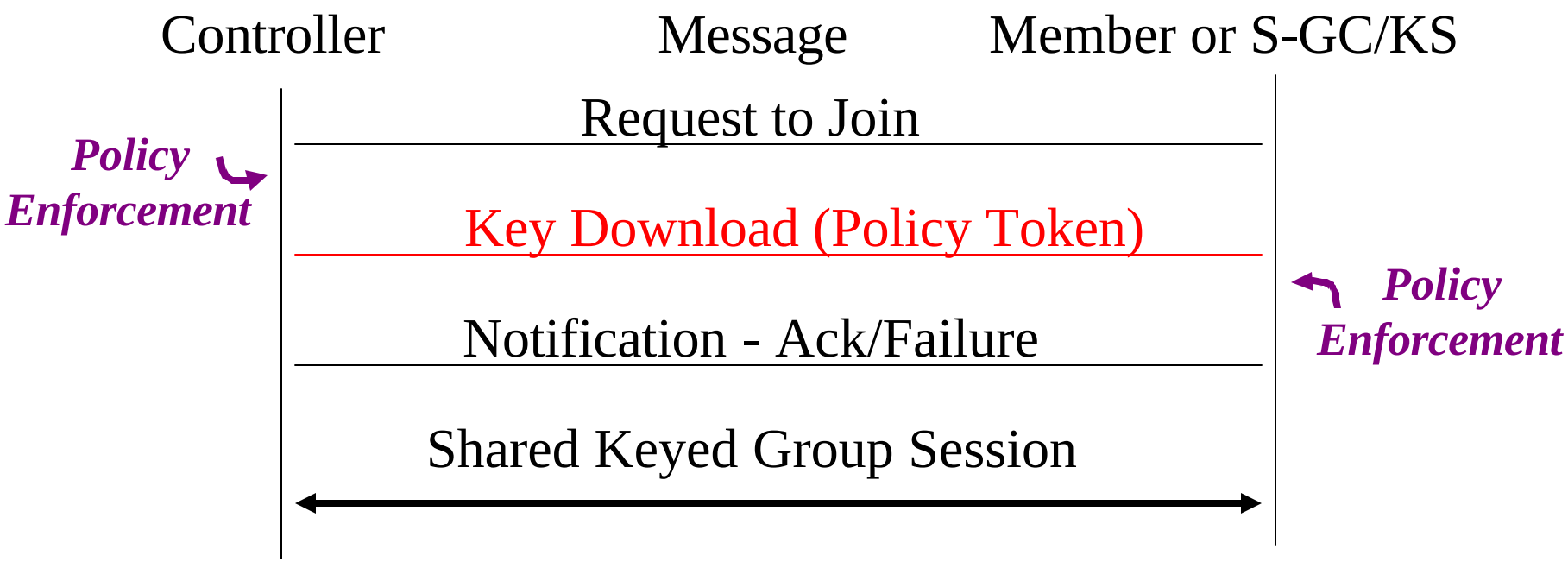
- GSAKMP Roles
- GSAKMP Policy Token Dissemination
- GSAKMP Token Spec.

GSAKMP Roles

- Group Owner
  - Policy Creation Authority
- Group Controller/Key Server
  - Policy enforcer
  - Policy dissemination
- Subordinate GC/KS
  - Policy enforcer
- Group Member
  - Policy enforcer



GSAKMP Policy Token Dissemination



GSAKMP Token Specification - Top level

- Identification
  - Uniquely identify policy token and group
- Authorizations
  - Identifies
    - Group Owner
    - Authorized rekey initiator
    - Sub GC/KS s
- Access Control
  - Who is allowed into the group
- Mechanisms
  - What are the allowed mechanisms for this group
  - Pass through policy for crypto application (IPSec)
- Signature
  - Verification of policy token veracity

Identification Fields

- **Token ID**
  - **Version (Policy Token version)**
  - **Protocol ID (GSAKMP or other)**
  - **Group ID (Unique identity of cryptographic group)**
    - **Network Identifier (multicast IP address if appropriate)**
    - **Serial number**
  - **Time (Group Owner Time)**

Authorization Fields

- Group Owner Name: explicit
  - Owner Name PKI
- Rekey Controller Name: explicit or rules
  - Rekey Controller Name PKI
- Key Server Authorizations : explicit or rules

Access Control Fields

- Access control
  - Inclusionary
    - Permission level
    - Rules based on certificates
      - Names (X.509 Subject field)

        NAME (Explicit or Rule)

        PKI
  - Exclusionary
    - Permission Level
    - Rules based on certificates
      - Name rules

        NAME (Explicit or Rule)

        PKI

Mechanism Fields

- GSAKMP Key API
  - Key use (Encryption)
    - Algorithm
    - Mode
    - Key length
    - Key lifespan
    - Key type
    - Key Creation methodology
  - Group Specific Data (PF Key Data)
    - Type (IPSec)
      - Number of SAs
      - Secure Associations (SAD/SPD)

Internal for GSAKMP

- Key Management SA (GSAKMP security suite)
  - Encryption
  - Rekey
- Rekey Information
  - Frequency
  - Rollover
    - Type
    - Time
- Unicast SA (Management messages)
  - Encryption
  - Rekey
- Group Specific Data (PF Key Data)
  - Type (IPSec)
    - Number of SAs
    - Secure Associations (SAD/SPD)

Signature Fields

- Signature
  - Name
    - Group Owner Name
    - Certificate serial number
  - PKI
    - Type (type of certificate)
    - Key length
    - Serial number (for issuer cert)
    - Issuer PKI Length
    - Issuer PKI (x.509 subject data for issuer)
  - Signature Data (Group Owners Signature over Policy Token)