Group Policy Token

with Application to GSAKMP

draft-ietf-msec-policy-token-sec-00.txt

General

- Signed in CMS format
- Specified in ASN.1
- The core of the token structure aligns with msec architecture
- Flexibility and extensibility in protocol and mechanism choices for each SA
- Appendix of draft carries one example of each type of SA
  - GSAKMPv1 Registration (and De-Registration) SA
  - GSAKMPv1 Rekey SA
  - SRTP Data SA

Core Structure

```
Token ::= SEQUENCE {
        tokenInfo       TokenID,

        registration    SEQUENCE OF Registration,

        rekey           SEQUENCE OF GroupMngmtProtocol,

        data            SEQUENCE OF DataProtocol
}
```

- Example
  - Group 456
  - Registration
    - GSAKMPv1 with suite A, etc., OR
    - GDOI with AES, etc., OR
    - GSAKMPv1 with mechanisms x, y, z
  - Rekey
    - GSAKMPv1 with LKH and AES, etc., AND
    - GSAKMPv20 with SSD and Bob's Encryption
  - Data
    - Secure RTP
    - IPsec with ESP AES-CM

GSAKMPv1 Registration

```
GSAKMPv1RegistrationInfo ::= SEQUENCE {
        joinAuthorization       JoinAuthorization,
        joinAccessControl       SEQUENCE OF AccessControl,
        joinMechanisms          JoinMechanisms,
        transport               Transport
}
```

- *joinAuthorization* says who is allowed to be Group Controller, etc.
- *joinAccessControl* says who (by rules or list) can join the group
- *joinMechanisms* gives the GSAKMPv1 mechanisms that may be used in this group for registration
- *transport* indicates how the GSAKMPv1 messages are carried (*e.g.,* UDP)

GSAKMPv1De-Registration

```
GSAKMPv1DeRegistrationInfo ::= SEQUENCE {
        leaveMechanisms         LeaveMechanisms,
        terse                   BOOLEAN,
        transport               Transport }
```

- Similarly, *leaveMechanisms* provide the GSAKMPv1 security mechanisms used when leaving a group
- *terse* indicates whether the protocol is operated in terse or verbose mode for errors

GSAKMPv1 Rekey

```
GSAKMPv1RekeyInfo ::= SEQUENCE {
        authorization       RekeyAuthorization,
        mechanism           RekeyMechanisms,
        rekeyEventDef       RekeyEventDef, -- tells the GCKS when to rekey
        rekeyMethod         RekeyMethod, -- e.g., LKH
        rekeyInterval       LifeDate, -- member knows when to rejoin
        reliability         Reliability, -- what mech will be used to increase
                                         the likelihood of rekey delivery
        subGCKSInfo         SubGCKSInfo -- what subordinate gcks needs
}
```

SRTP Data SA

```
srtpDataSAInfo ::= SEQUENCE {
        masterKeyID         OCTET STRING (SIZE (4)),
        masterSaltKeyID     OCTET STRING (SIZE (4)),
        encrTransform       EncryptionTransform,
        authTransform       AuthenticationTranform OPTIONAL,
        tagLength           INTEGER,
        prefixLength        INTEGER,
        pRF                 PRF,
        encrKeyLength       INTEGER,
        authKeyLength       INTEGER,
        sessionSaltLength   INTEGER,
        keyDerivRate        INTEGER,
        sRTPPacketMax       INTEGER,
        sRTCPPacketMax      INTEGER,
        mKI                 OCTET STRING OPTIONAL,
        tOfROM              OCTET STRING OPTIONAL }
```