

GSAKMP Update

draft-ietf-msec-gsakmp-sec-04.txt

Changes

- New Contributor
 - Harney, Meth, Colegrove, Schuett, McDaniel, Kenny, Cruikshank, Iyengar, Gross
- New Sections
- New Messages
- More processing details
 - Messages
 - Payloads

Architecture Section

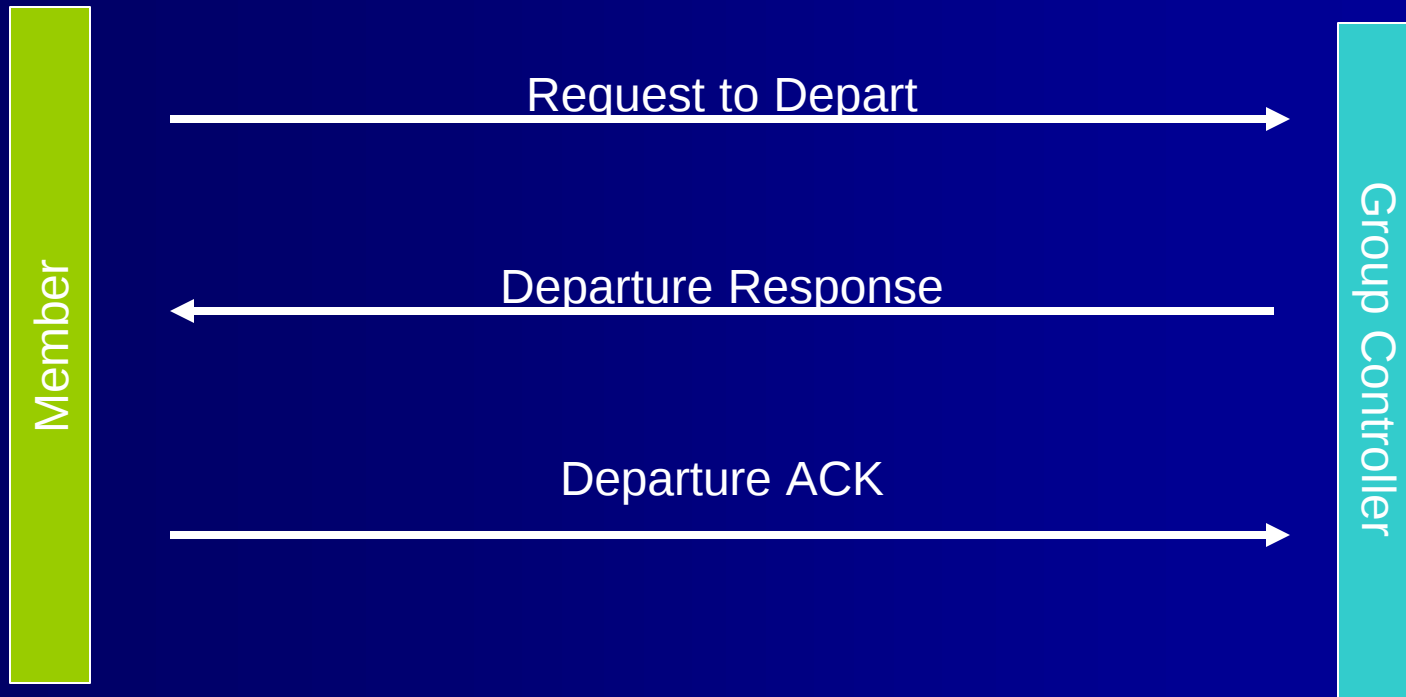
- Trust Model – roles and responsibilities
- Security Policy
- Distributed Operation
- Concept of Operation
- GSAKMP and NAT
 - Largely IPsec-centric

Departure

- Discussions on leaving a group
 - Eviction
 - Rekey event
 - Voluntary Departure without Notice
 - Member deletes local copies of key
 - De-Registration
 - New optional exchange

Departure

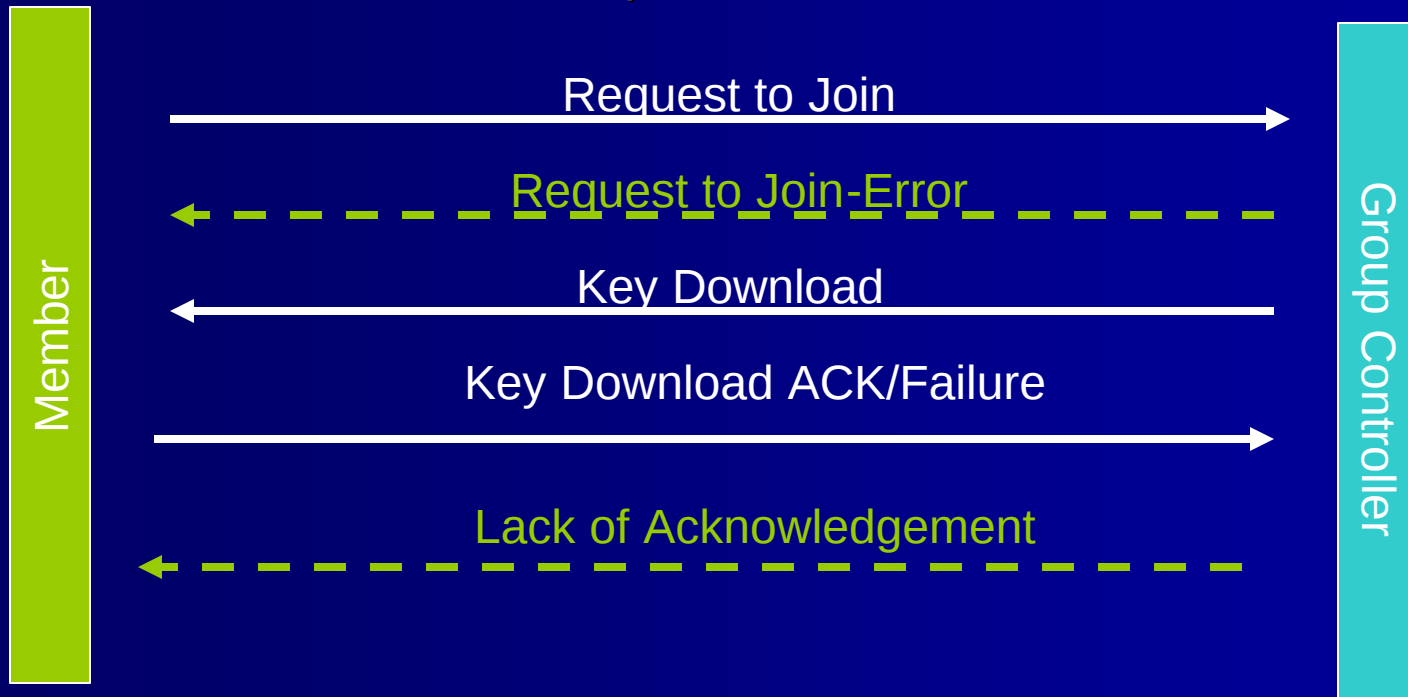
De-Registration



Optional Error Messages

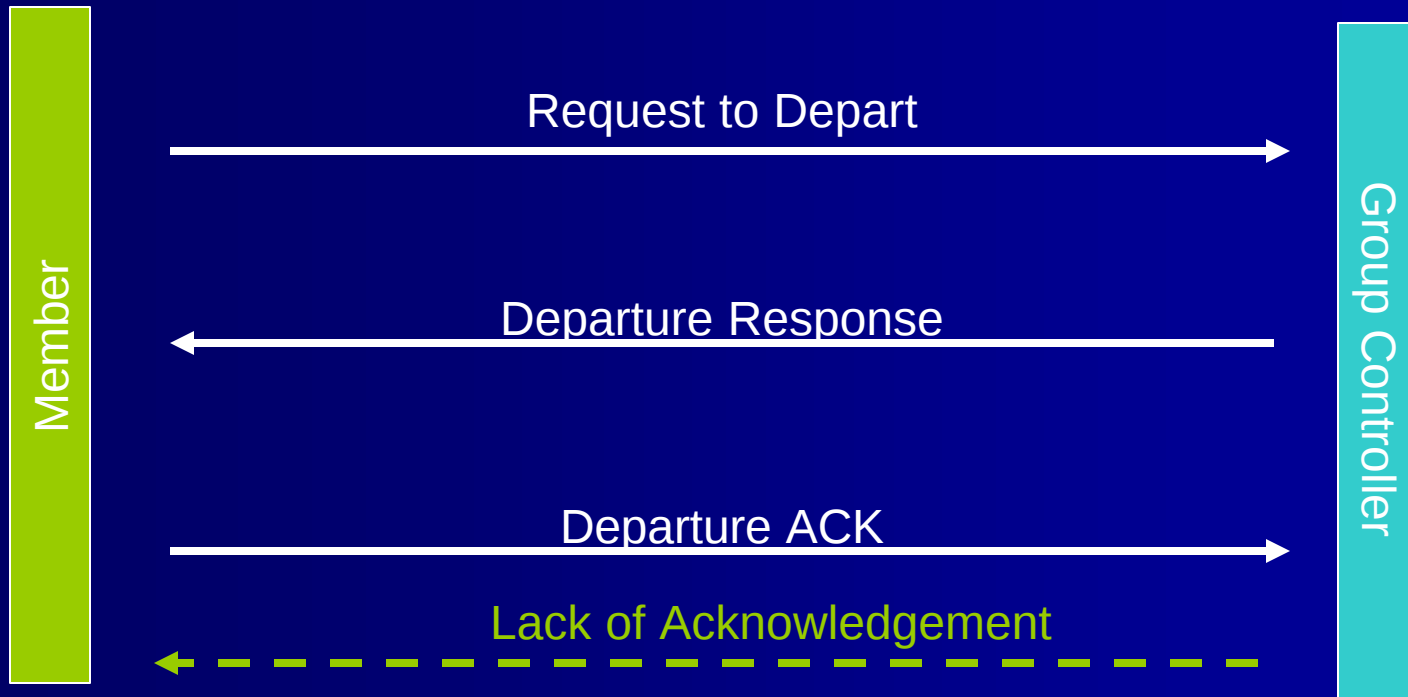
Group Establishment

Group Establishment



Optional Error Messages

Departure



“Generic” MSEC Token

PolicyToken -- {TBD}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

```
Token ::= SEQUENCE {  
    tokenInfo      TokenID,  
    registration   Registration,  
    rekey          Rekey,  
    data           SEQUENCE OF DataSA  
}
```