GSAKMP

Group Secure Association Key Management Protocol

Presented by

Hugh Harney

hh@sparta
410-381-9400 x203

draft-irtf-smug-gsakmp-oo.txt
draft-irtf-smug-polreq-oo.txt
ftp://ftp.sparta.com/pub/columbia/gsakmp/gsakmp-0.5.tar.gz

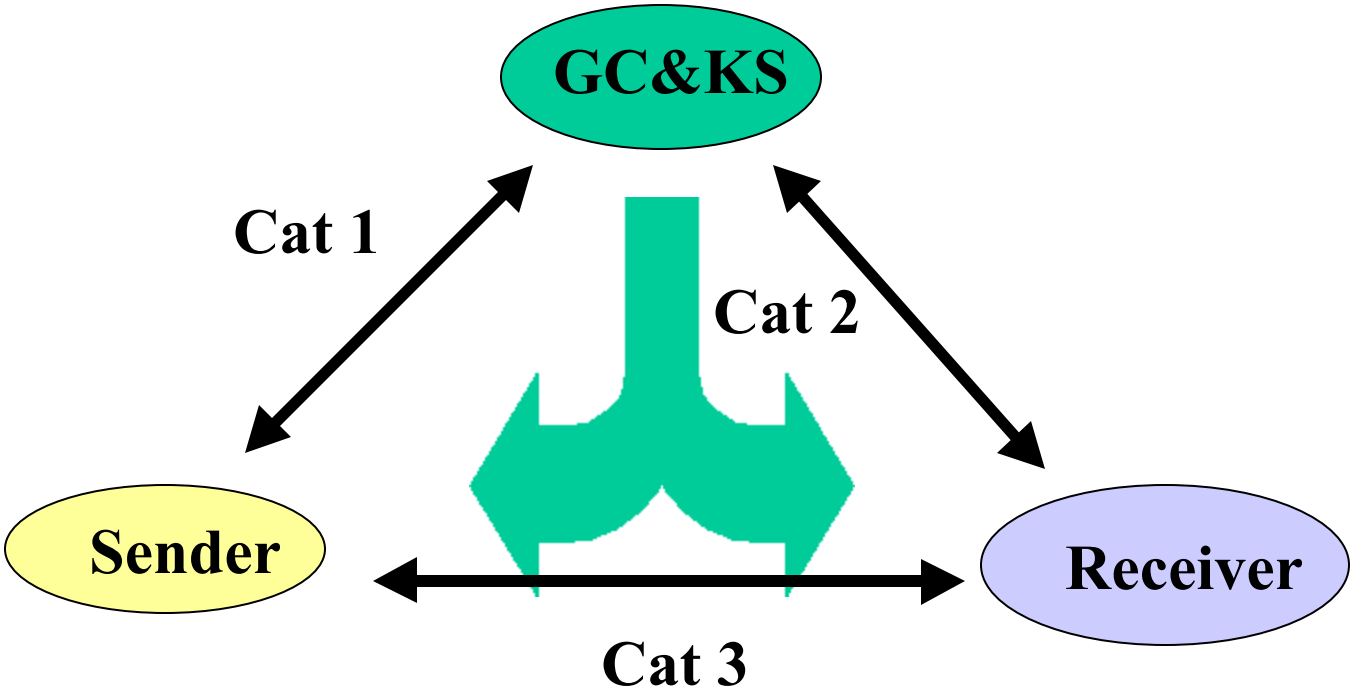
GSAKMP Goals

- **Secure group key management**
  - Secure key download in many architectures
  - Management of group keys - Traffic and Membership management
- **Coherent policy**
  - Balanced security mechanisms for group
  - Common cooperatively enforced policy
- **Flexible architectures**
  - Layered over peer SA protocols
  - Behind VPNs
- **Scalability**
  - Multiple key servers
  - Multiple authorized managers
- **Management of group membership**
  - Group membership management
  - Group policy management

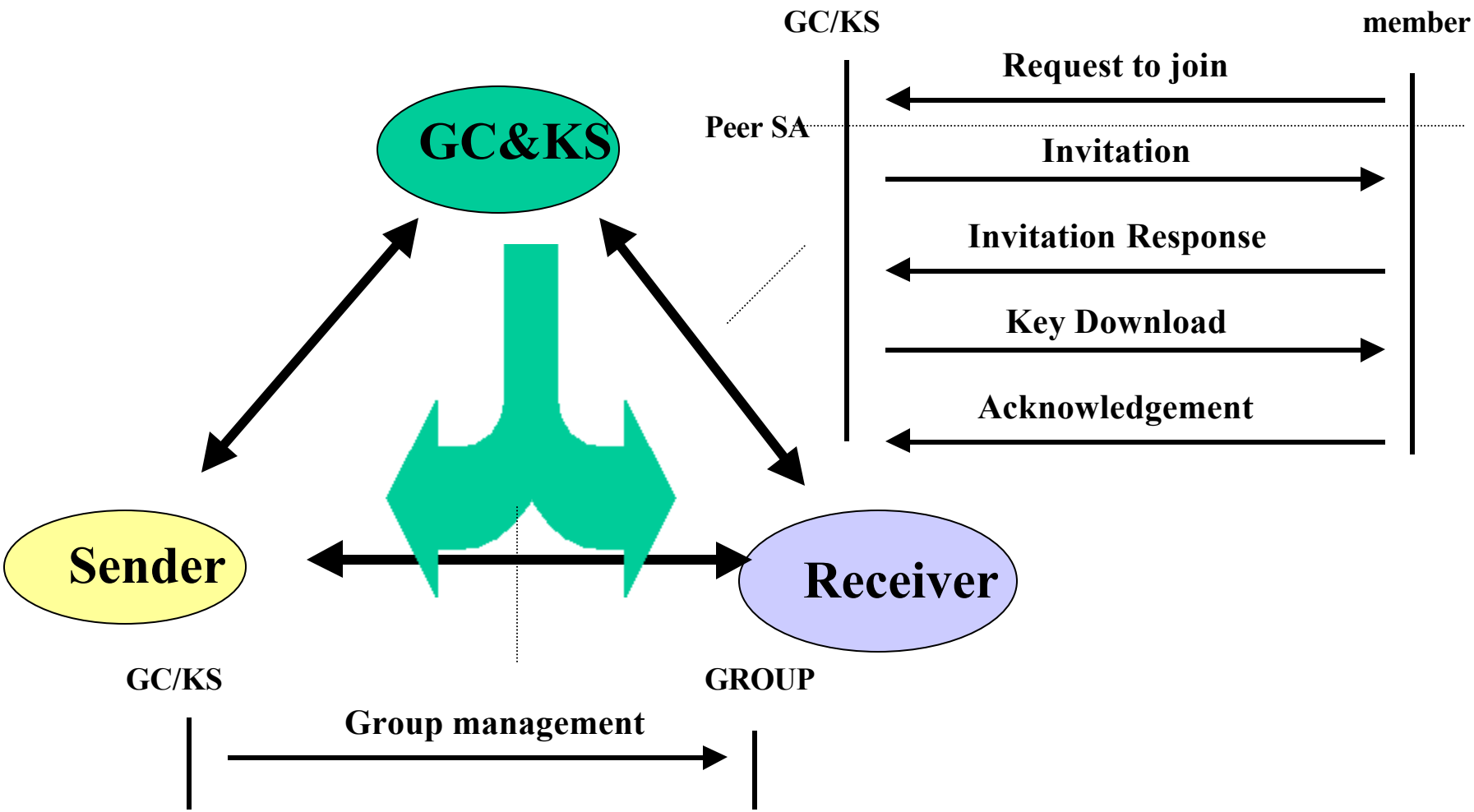
GSAKMP Functions

- **Establishment**
  - **Clearly defined group policy**
  - **Group wide enforcement of that policy**
  - **Distribution of group keys**
    - **Traffic**
    - **Group management**
- **Management**
  - **Group membership management**
  - **Flexible group policy**

Group Key Management Architecture



GSAKMP


GC/KS
member
Request to join
Peer SA
GC&KS
Invitation
Invitation Response
Key Download
Acknowledgement
Sender
Receiver
GC/KS
GROUP
Group management

Summary

- GSAKMP provides a complete solution
  - draft-irtf-smug-gsakmp-oo.txt
- Group policy is the key to group key management
  - draft-irtf-smug-polreq-oo.txt
- Free proof of concept code is available
  - ftp://ftp.sparta.com/pub/columbia/gsakmp/gsakmp-0.5.tar.gz