Group key management architecture

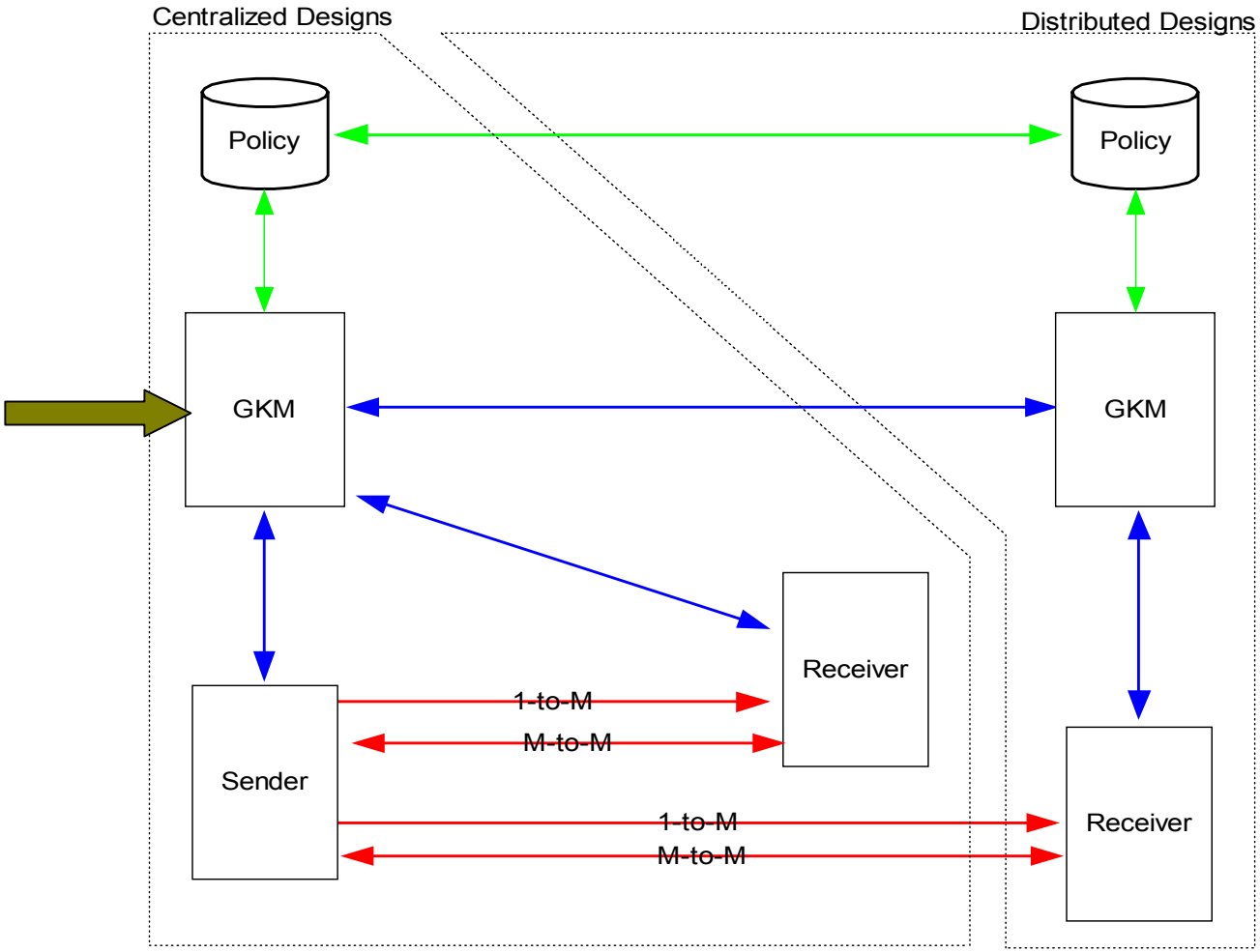
<draft-ietf-msec-gkmarch-01.txt>

Mark Baugher, Cisco
Ran Canetti, IBM
Lakshminath Dondeti, Nortel
Fredrik Lindholm, Ericsson

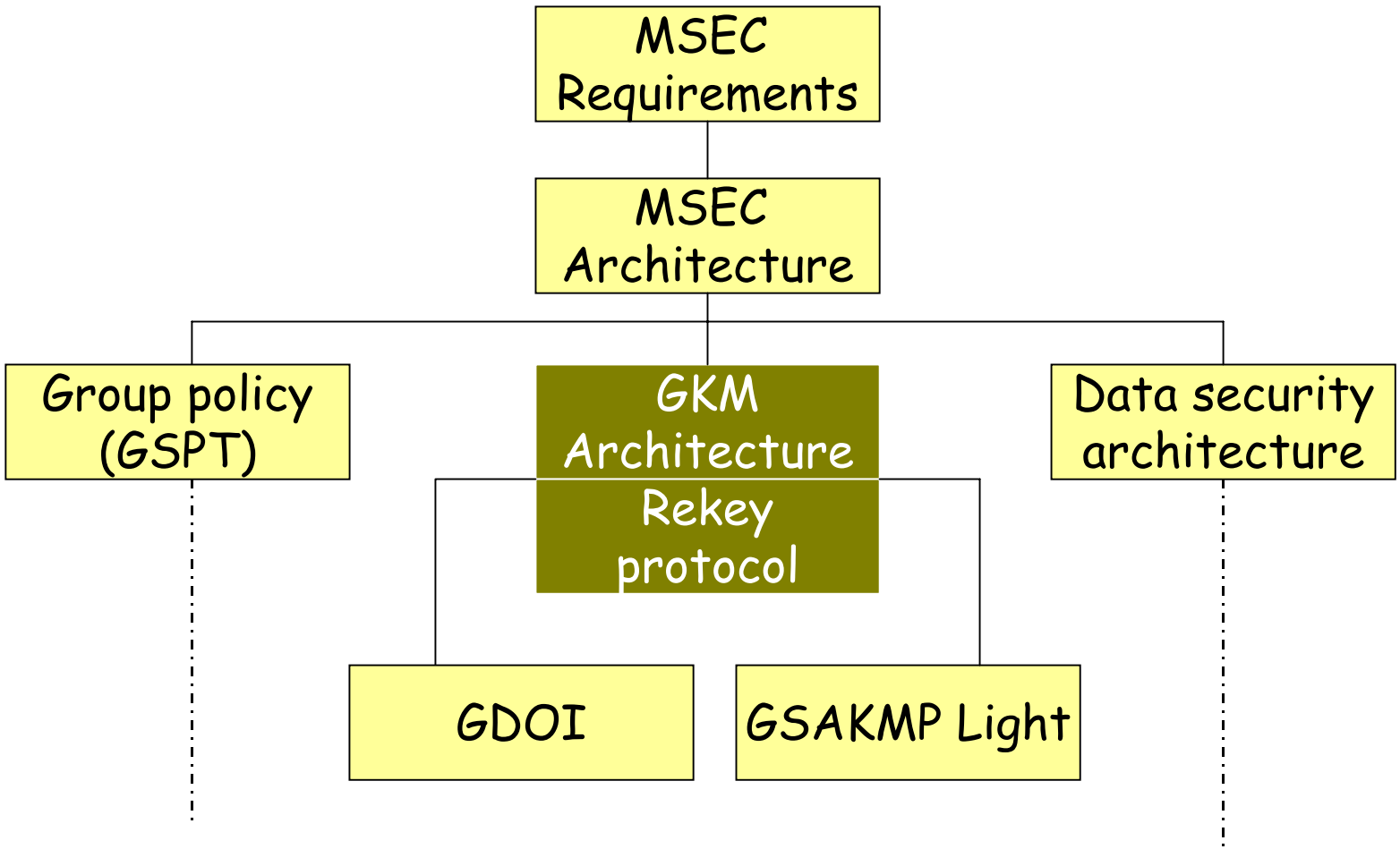
Overview of this talk

- Introduction to GKMArch
  - Relative positioning in MSEC Ids
  - GKM protocols and SAs
- Current revisions (00→01)
- Outstanding issues
  - MIKEY
  - Rekey protocol
- Conclusion

GKM in MSEC architecture



GKMArch as part of MSEC IDs



Purpose of GKMArch

- Download SAs to members, securely
  - Data security SA, mainly
  - Rekey SA, to facilitate efficient updates to SAs
- Update SAs via unicast or multicast
- Manage membership
  - Joins and leaves
  - Support optional PFC and/or PBC in doing so
- Download and/or update KM/SA policy to members

GKMArch requirements

- Allow reuse of existing protocols for data transmission
  - e.g. IPsec AH or ESP, AMESP, SRTP
- Support diverse authentication, authorization and trust mechanisms
- Support large single sender groups
- Support small multi-sender groups

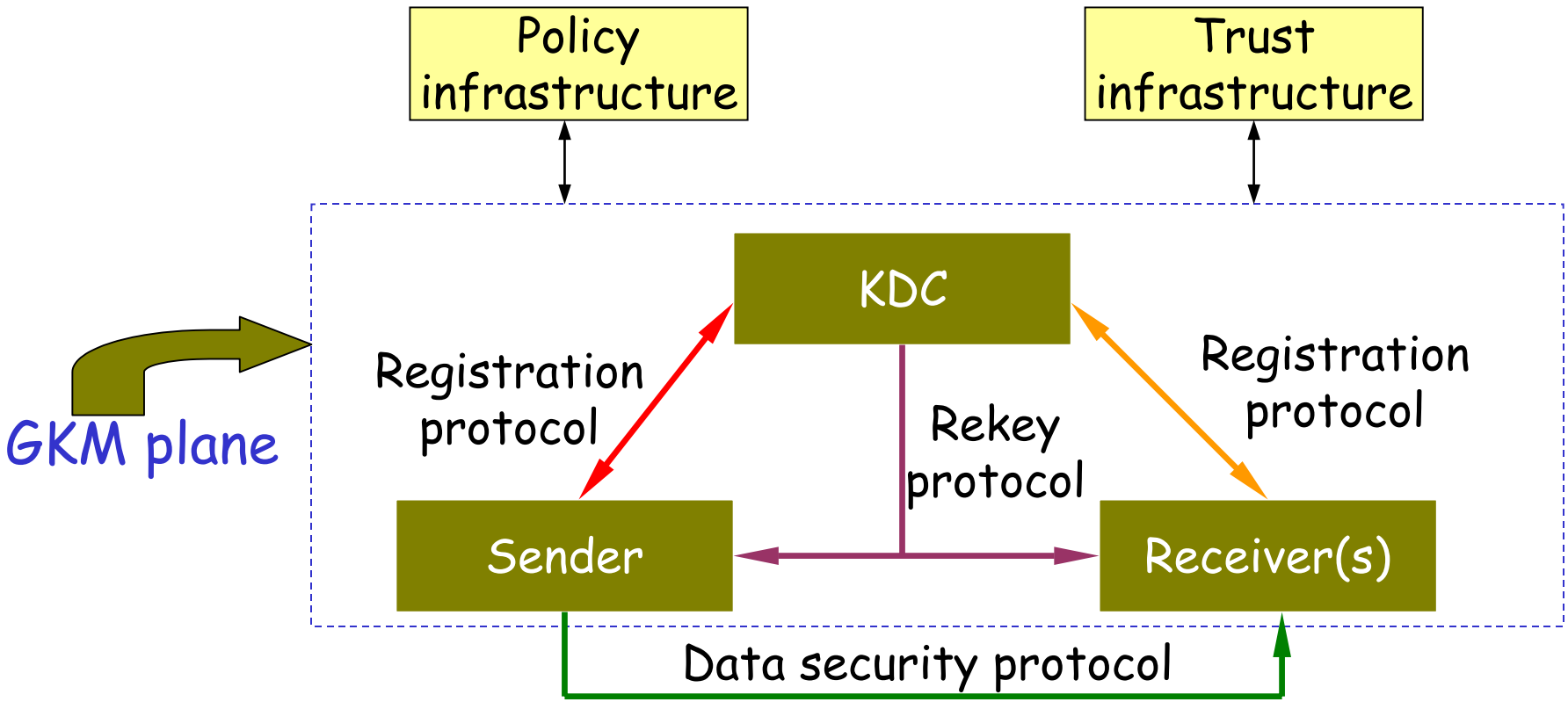
SAs in GKMArch

- GSA comprised of three SAs
  - Registration SA
    - Established via one-one bidirectional secure channels
      - e.g. IKE phase1, TLS, IPsec
  - Rekey SA (optional)
    - Initialized during registration
    - Initialized/updated during rekey (uni-directional)
  - Data security SA
    - Initialized during registration
    - Initialized/updated during rekey (uni-directional)

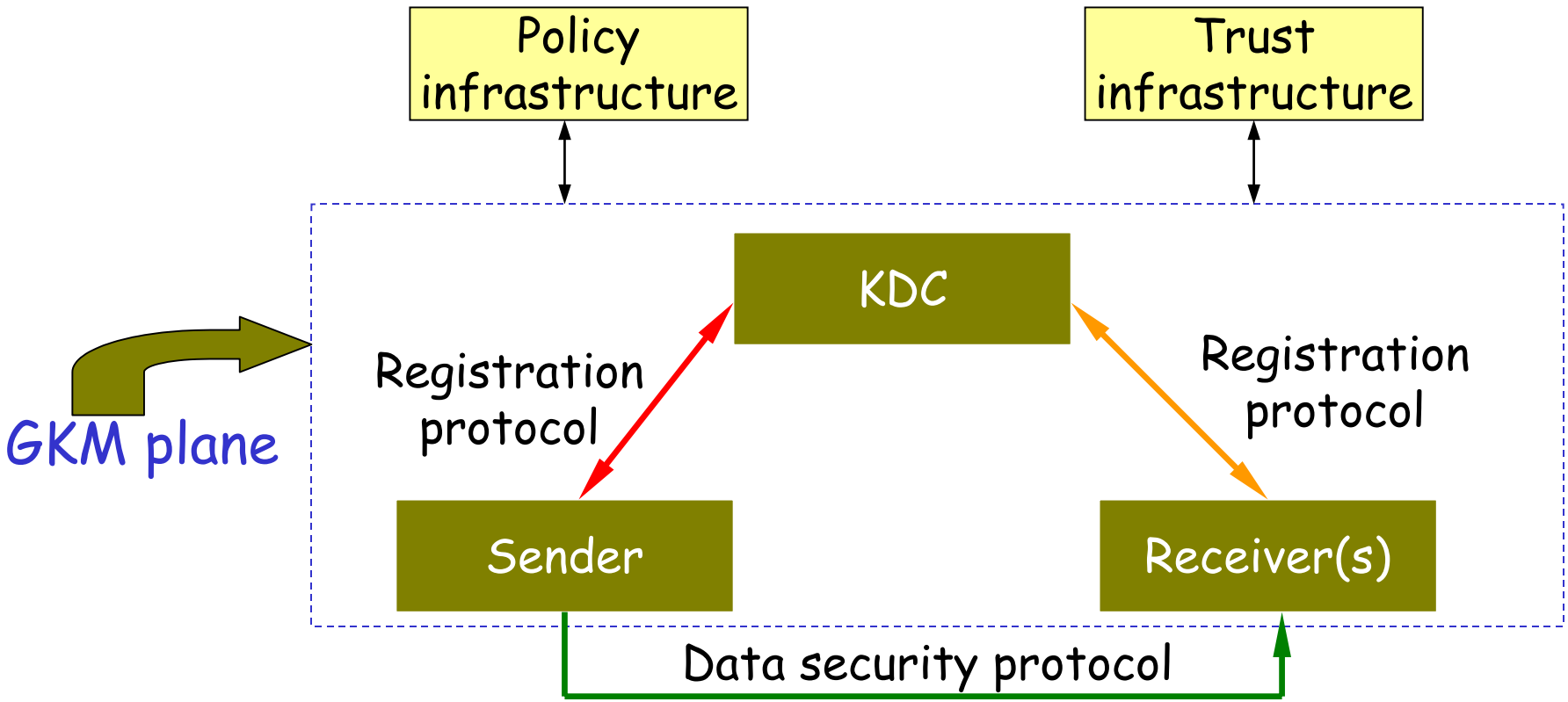
Protocols in GKMArch

- Registration protocol
  - Protected by registration SA
- Rekey protocol (optional)
  - Protected by rekey SA
- Data security protocol (external to GKM)
  - Protected by data security SA

GKM entities and protocols



GKM entities and protocols



Scalability of GKMArch

- Registration could be done off-line
- Delegation of registration "service"
- Loose coupling of registration and rekey protocols
- Rekey protocol with key revocation algms
  - LKH, OFT, OFC, SDR (subset diff), STR
  - Multicast of rekey messages
- Delegation of rekey service

Overview of this talk

- Introduction to GKMArch
  - Relative positioning in MSEC Ids
  - GKM protocols and SAs
- Current revisions (00→01)
- Outstanding issues
  - MIKEY
  - Rekey protocol
- Conclusion

Revisions (00 → 01)

- Addressed issues raised in mailing list
  - Have not heard any complaints!
    - Did we do such a good job of that? ☺
- Notes about de-registration protocol
  - De-registration is not supported!
- KDC → GCKS
  - (what were we thinking?)
- SHOULD, MUST etc in IETF sense

Overview of this talk

- Introduction to GKMArch
  - Relative positioning in MSEC Ids
  - GKM protocols and SAs
- Current revisions (00→01)
- Outstanding issues
  - MIKEY
  - Rekey protocol
- Conclusion

Outstanding issues

- Fold MIKEY requirements into GKMArch I-D
  - Small interactive group security reqs.
- Rekey protocol description back in GKMArch
  - Yet to be resolved!
  - Looking for WG consensus
  - Details in another presentation

Conclusion

- A scalable architecture for GKM
  - Supports large single sender groups and
  - Small interactive multi-sender groups
- Scalability by
  - Delegation
  - Multicast of GSA updates
- Incorporate MIKEY reqs in –02-
- Discussion on rekey protocol to follow