# Group key management architecture

<draft-ietf-msec-gkmarch-02.txt>

Mark Baugher, Cisco

Ran Canetti, IBM

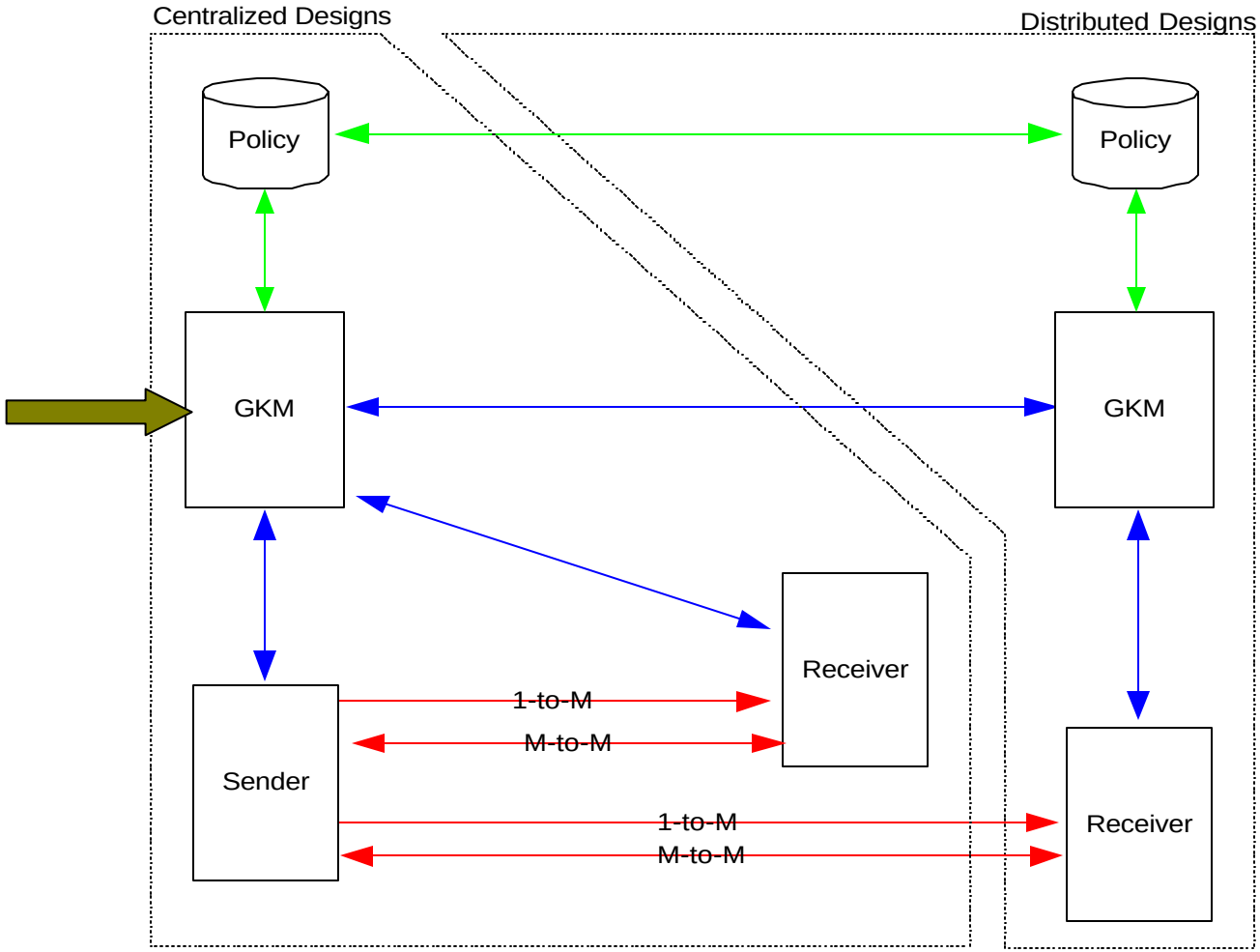
Lakshminath Dondeti, Nortel

Fredrik Lindholm, Ericsson

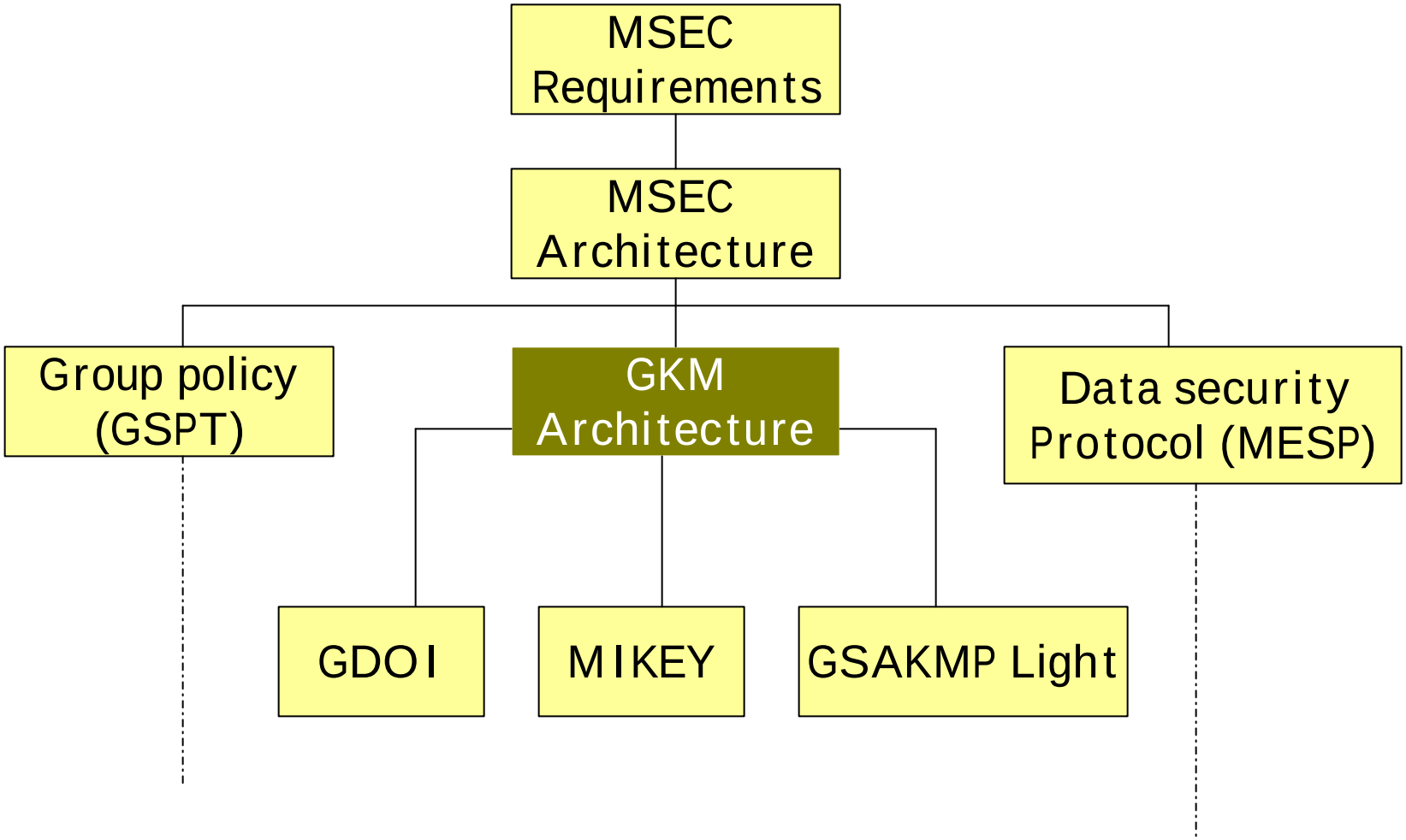
# Overview of this talk

- Introduction to GKMArch
  - Relative positioning in MSEC I-Ds
- Current revisions (01→02)
  - MIKEY
  - Additional text about deregistration
  - Rekey protocol folded into this I-D
- Conclusion

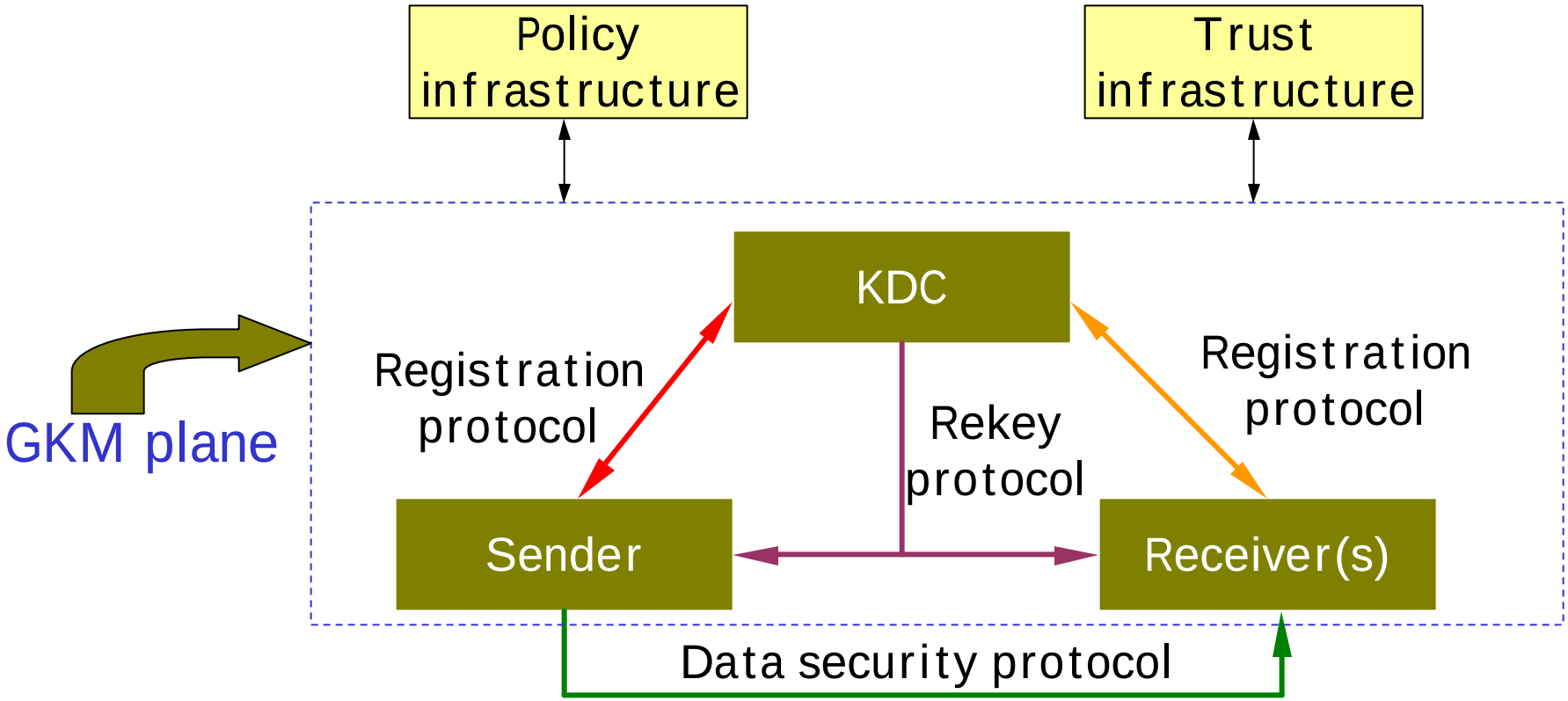
# GKM in MSEC architecture



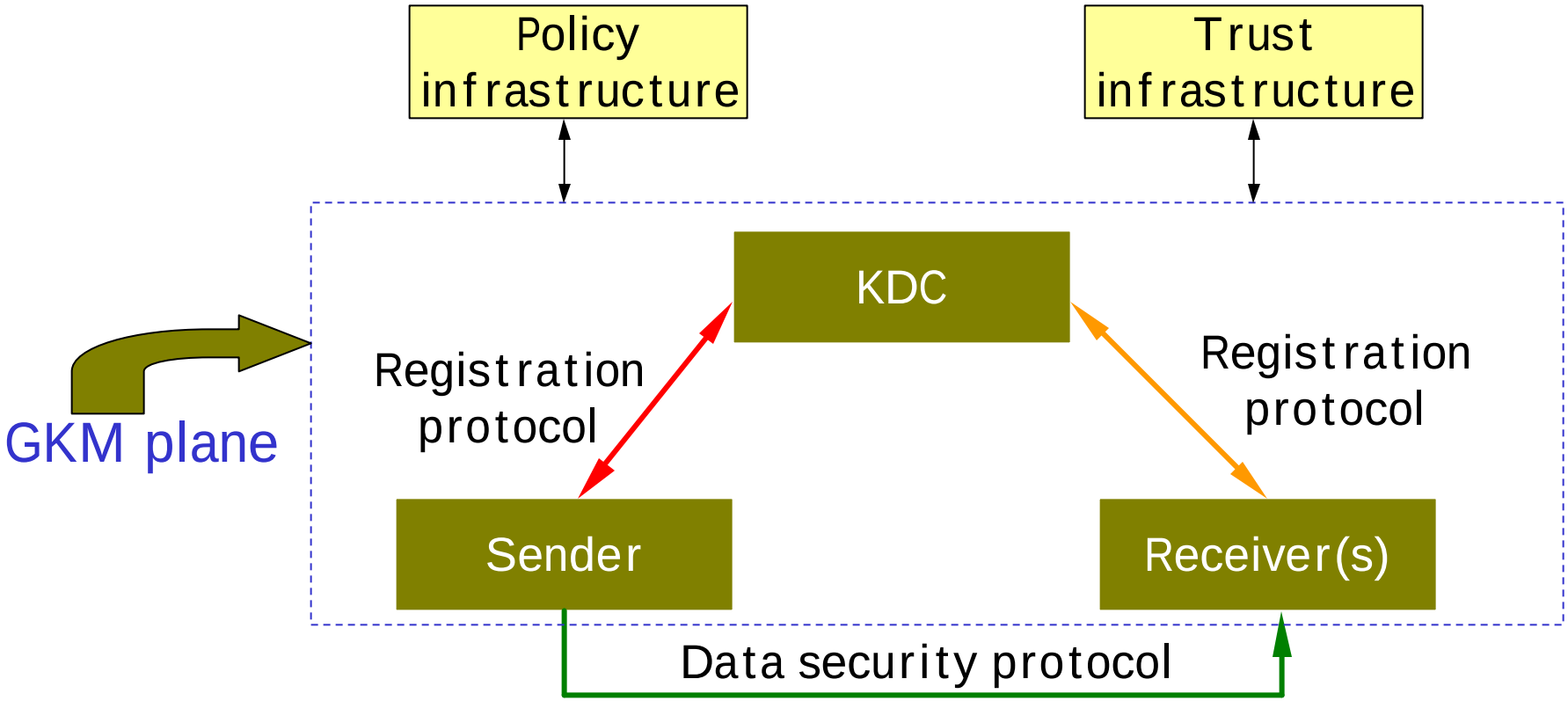
# GKMArch as part of MSEC IDs



# GKM entities and protocols



# GKM entities and protocols



# Overview of this talk

- Introduction to GKMArch
  - Relative positioning in MSEC I-Ds
- Current revisions (01→02)
  - MIKEY
  - Additional text about deregistration
  - Rekey protocol folded into this I-D
- Conclusion

# Revisions (01 → 02)

- Incorporated MIKEY requirements
  - Lightweight to run over SIP/RTSP
- Notes about de-registration protocol
- Rekey protocol requirements
  - Reliable transport
  - Feedback implosion
  - Group key management algorithms (GKMA)

# MIKEY requirements

- GKM model too complex for SIP and RTSP
- Fewer round trips to establishing SAs
- Optimize SA setup time
  - Allow SA download during call setup
  - Use session information in SIP and RTSP

# Notes on quick SA establishment

- Fewer roundtrips
  - One roundtrip, i.e., two messages
- Replay protection
  - Timestamps
    - Time synchronization requirements
  - Sequence numbers
    - Extra state
- No identity protection or PFS

# Rekey protocol requirements

- To synchronize a GSA
  - SAs might expire
    - Members may ask to be resync'ed
  - Membership changes
- Ensure timely updates to GSA
- Privacy and authentication of rekey messages
- Via multicast or multi-unicast

# Rekey protocol requirements

- Reliable transport of updates
- Avoid implosion problems
  - Feedback implosion
  - Resync request implosion
- Scalable operation
- Use Group key management algorithms (GKMA) (LKH, OFT etc.)

# Outstanding issues in rekeying

- Reliable transport of rekey messages
- Address feedback implosion
- Incorporating GKMA into rekey msgs
  - Stateful and stateless rekeying
    - Different reliability requirements
- Interoperability of GKMA
  - e.g. Different LKH implementations

# Conclusion

- Requirements of SIP and RTSP key establishment
- Deregistration protocol
- Rekey protocol issues
  - Reliability and implosion issues
  - Interoperability of GKMAs
    - Standardize LKH, OFT, Subset difference etc.