MSEC Group Key Management Architecture

Mark Baugher, Cisco Systems
Ran Canetti, IBM
Lakshminath Dondeti, Nortel

Overview

- Purpose: Define a common architecture
- Requirements
- Overall Design
- Group Security Association definitions
- Conclusion: Direction of MSEC key management

Purpose

- MSEC key management protocols…
  - For IPsec, transport, application security
  - For single-source, multi-source security
  - For broadcast, telephony security
- …may benefit from a common architecture
  - Offering common abstractions, terminology
  - Featuring common structures
  - Addressing common problems

Group Key Management Apps

- Multicast security
  - Command and control
  - Mbone-style conferencing
  - File transfer
- Internet entertainment
  - Media downloads
  - Media on demand
  - License distribution

Telephony? Teleconferencing?

MSEC Group Key Management supports…

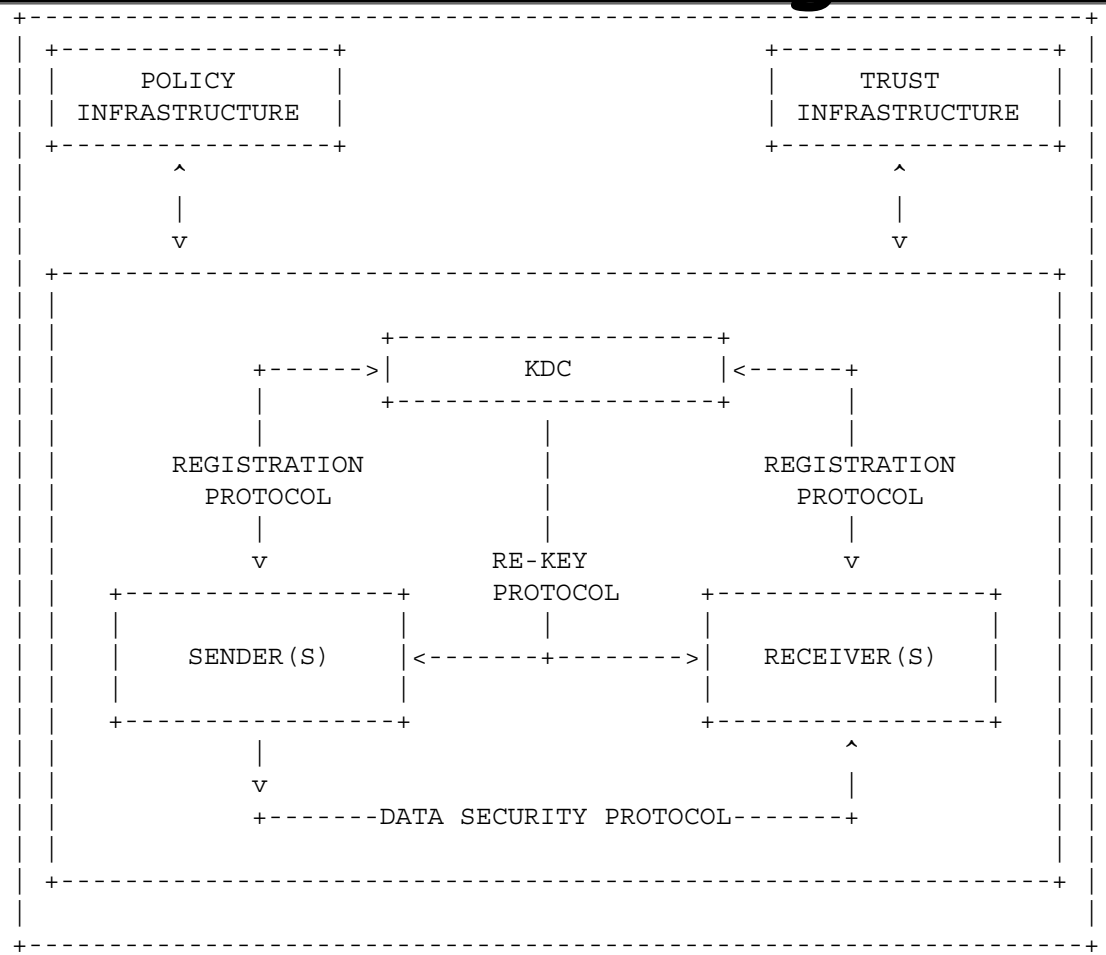
IPsec protocols (AH and ESP) when run in multicast mode.
Application security protocols such as SRTP, reliable multicast, etc.
Group and source authentication such as A/MESP.
Group membership management such as LKH.
Secure key dissemination to groups of authenticated principals

GKM Requirements (revised)

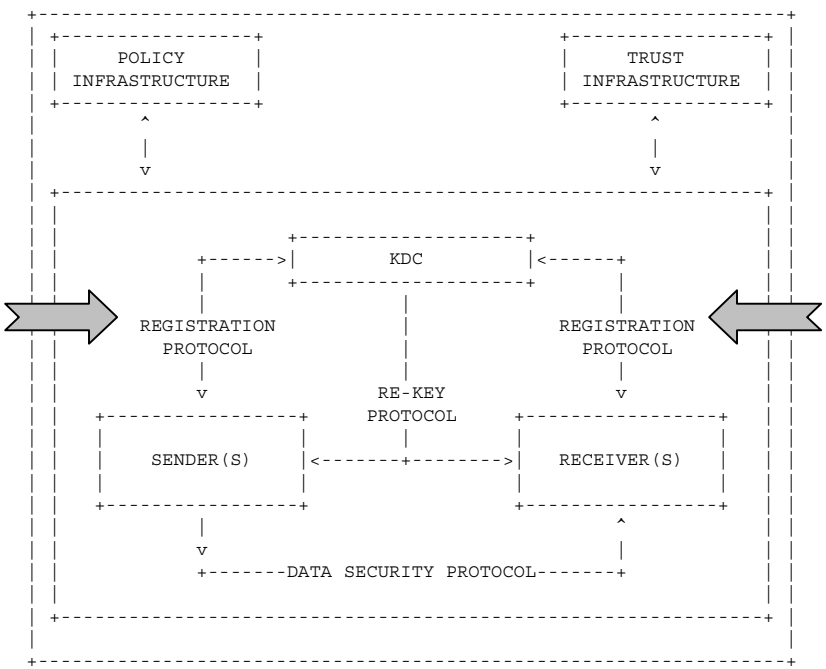
1. Establish SAs, with renewable keys, among group members
2. Refresh SAs securely against attack
3. Support forward and backward access control to group keys
4. Don't require unicast exchange for re-key
5. Don't require multicast
6. Support single-source multicast groups of arbitrarily large size
7. Support small, interactive groups with many senders (stretch)
8. Support IPsec, transport and/or application security protocols
9. Replaceable keys, algorithms, protocols, policy and trust

We recommend that MSEC take a modular by allowing separable "Registration" and "Re-key" protocols that may operate together or independently.

MSEC Group Key Management Reference Diagram



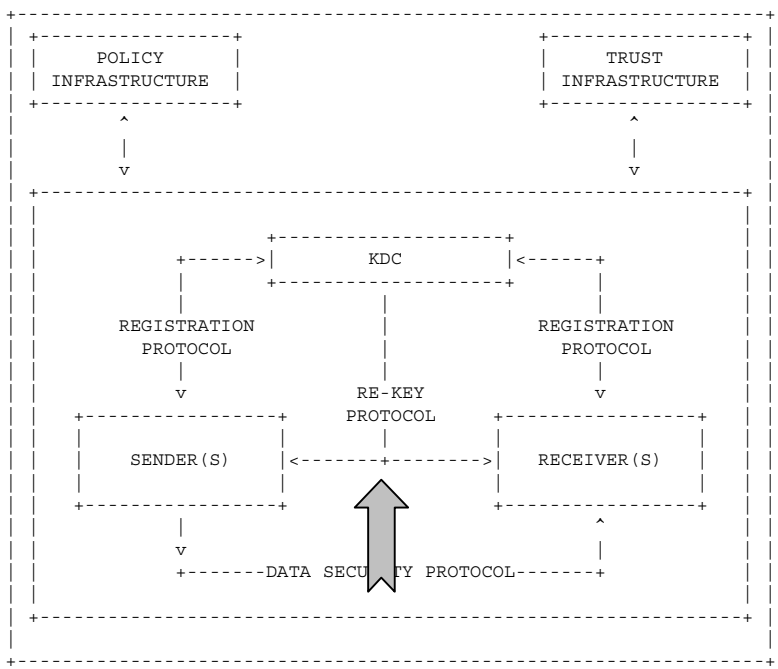
Registration Protocol



- Point-to-point authenticated key exchange
- May use IKE Phase 1 with custom Phase 2
- May run on TLS, SSL, IPsec
- Downloads
  - Re-key SA (KEK)
  - Data Security SA (TEK)

The goal of these protocols is to affect Security Association (SA) state.

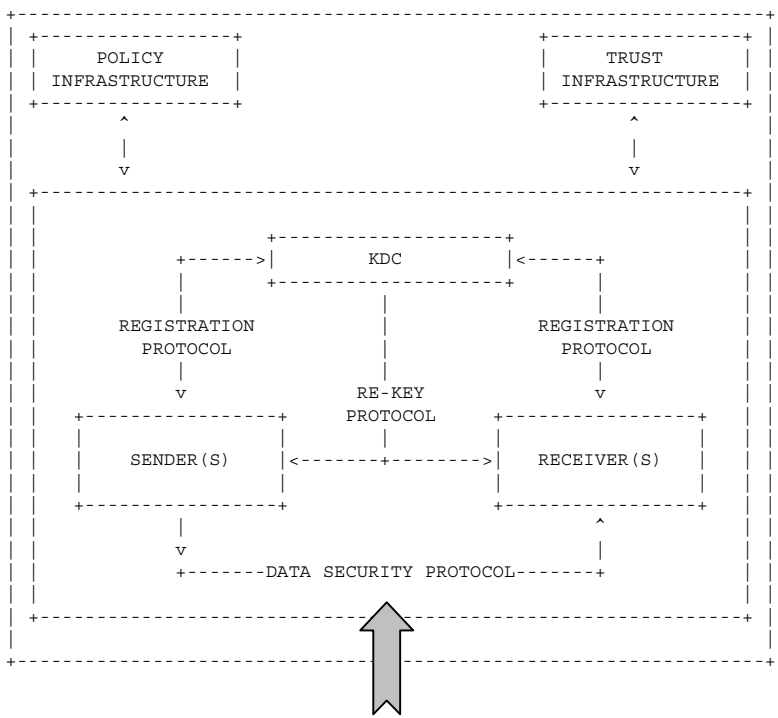
Re-key Protocol



- Downloads
  - Data security SA
  - refreshed Re-key SA
- Unicast or multicast
- Supports group membership mgt
- Separable from Registration Protocol

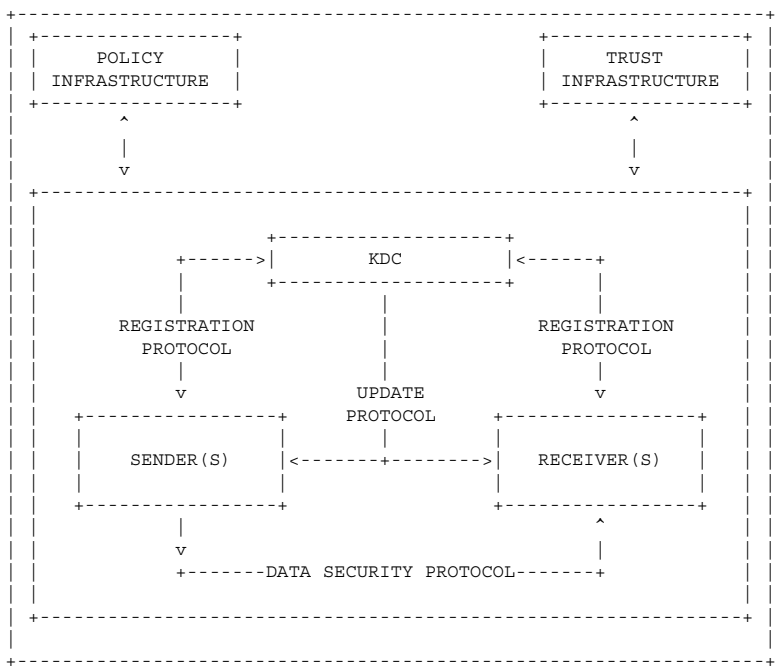
Implosion, partition, and message loss are issues to be addressed

Data Security Protocol



- Support for IPsec, SRTP, A/MESP, RMT protocols, …
  - Outside of group key management
  - Serviced by group key management
  - Goal of group key management

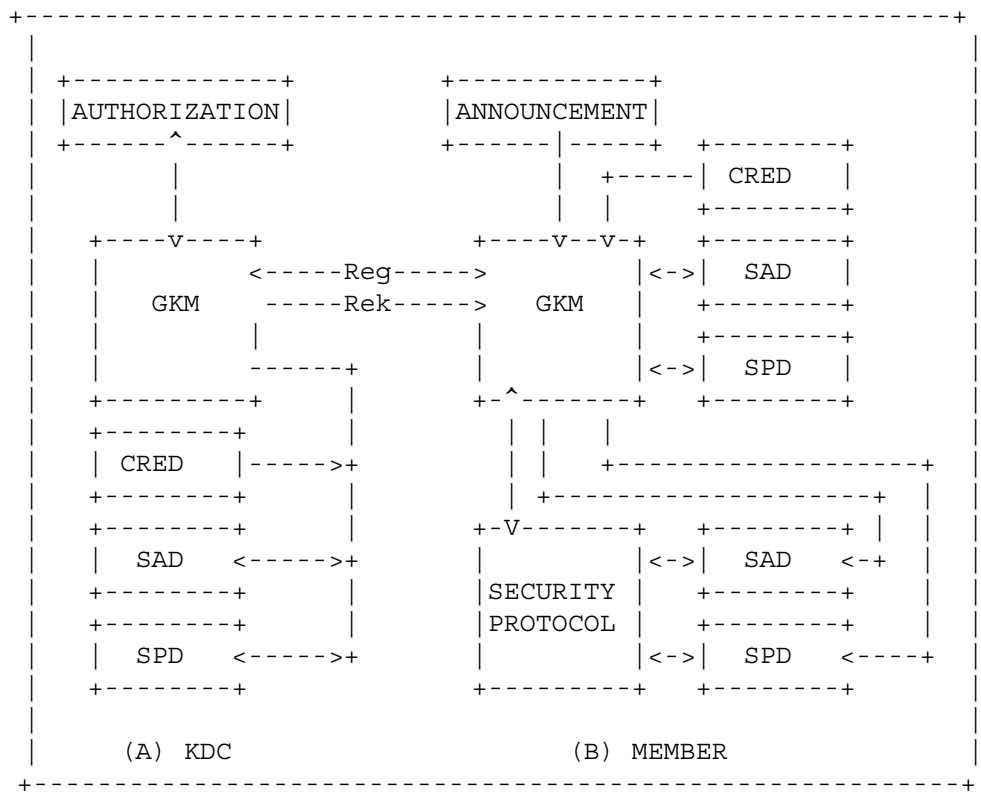
Group Security Association (GSA)



- SA is key + metadata
- GSA composes
  - Registration SA
  - Re-key SA
  - Data Security SA
- Each are independent

Registration SA protects Re-key SA and/or Data Security Protocol SA; Re-key SA protects Data Security Protocol

MSEC Group Key Management Host Implementation



GSA Interfaces

- Pro's, Con's of separating protocols
  - Pro's: can use only Registration protocol; allows Re-key SA setup thru various means
  - Con's: we need interfaces to support the separation, mixing, and matching of protocols; how many documents?
- The interface is the G-SAD
  - Through contents of the Re-key SA
  - Suggested contents of the Data-security SA

The Registration Protocol establishes Re-key SA and/or Data SAs; the Re-key protocol refreshes the Re-key SA and establishes the Data SAs.

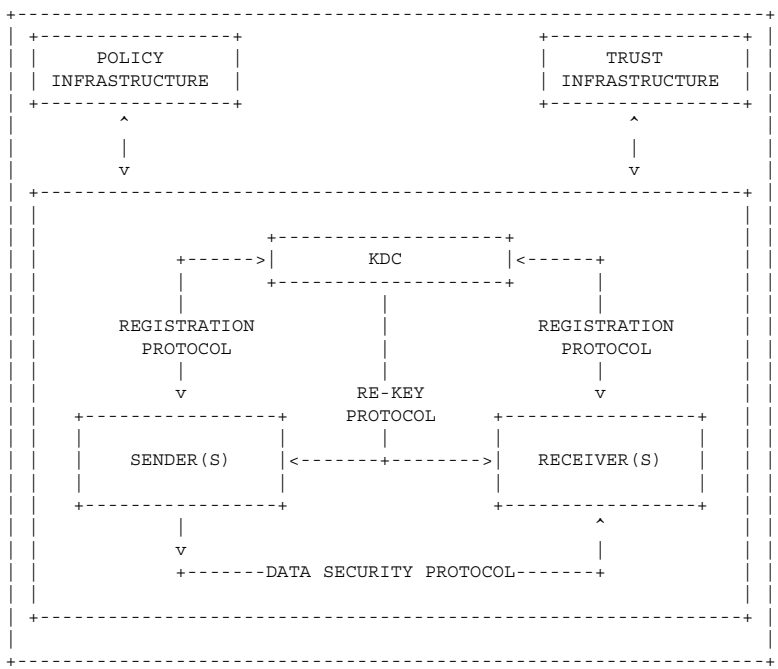
Re-key SA

- Policy (crypto, group mgt., addresses)
- Group Identity
- KEK(s) (issue of multiple groups)
- Authentication/Integrity keys
- Replay protection (sequence number)
- SPI

Data Security SA

- Group identity
- Source identity
- TEK
- Authentication/Integrity
- Replay Protection
- SPI

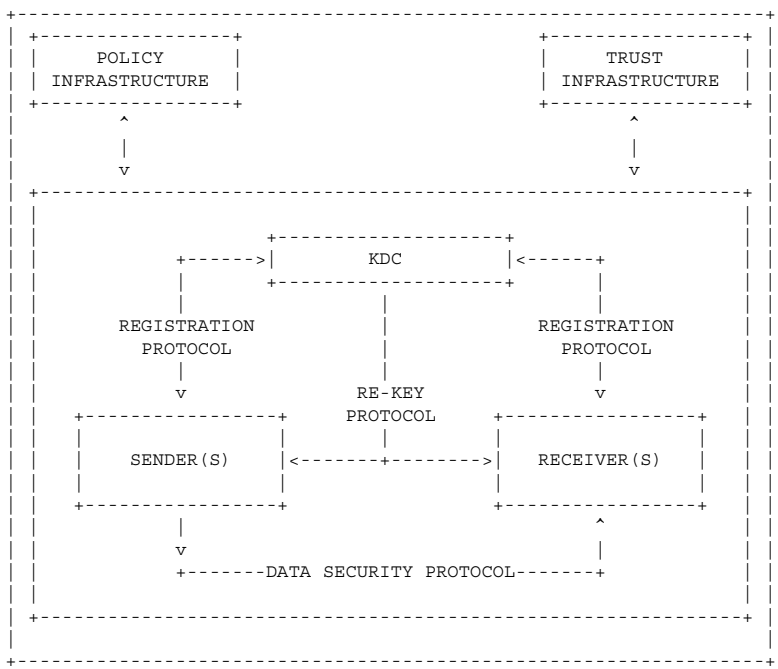
Group Policy



- Crypto policy describes SAs
- Must also describe GSA (next slide)
- Group ownership relationships
- Membership management
- Various membership policies

Membership question: Should I send to, belong to, this group?

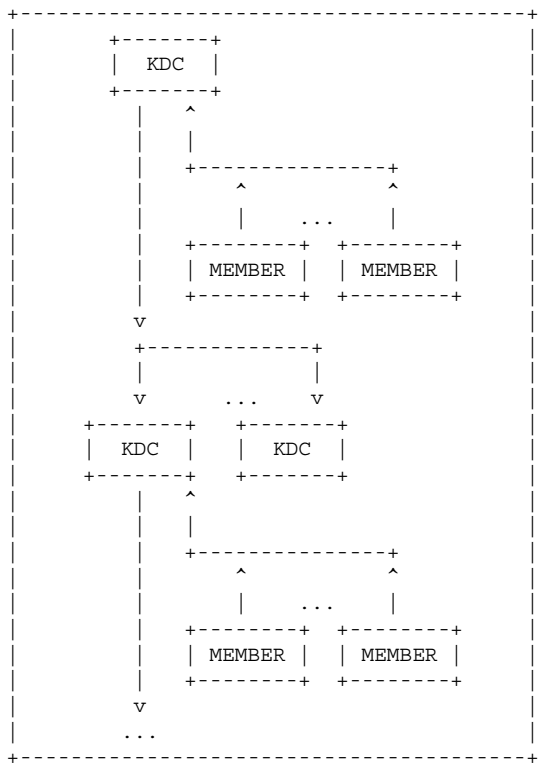
Trust Infrastructure



- One of more
  - X.509
  - Pre-shared key
  - SPKI
  - Kerberos ticket
  - PGP

Key management for IP networks should support diversity in authorization, authentication and trust

Group Key Management Infrastructure



- KDC function can be delegated
- Permits load balancing
- Enables large-scale operation

Summary

- Architecture has 3 loosely-coupled "protocols"
  - Packaged together or separately?
- Interface is thru the G-SAD
  - Interface to Re-key SA most important
- Work has begun on Re-key
- De-Registration discussed on the list

Issues

- "Distributed GKM" red herring
  - List discussion leads us to remove this
- Positioning of GSAKMP, GDOI
  - WG rationale needed for each
- External Policy infrastructure
  - Group Policy I-D should help resolve this
- Change "KDC" to "GCKS"

Backup

GKM Requirements

1. The group members must receive "security associations" including encryption keys, authentication/integrity keys, metadata describing the keys (also called "policy") and attributes such as an index for referencing the security association.
2. Keys will have a predetermined lifetime and will be periodically refreshed.
3. Key material must be delivered securely to members of the group so that they are secret and authenticated to group members during the key lifetime and refreshed securely at the end ofthe key lifetime.
4. The key-management protocol must be secure against man-in-the-middle, connection-hijacking, and reflection/replay attacks; it must use best-known practices to thwart denial-of-service attacks.
5. It must be possible to add and remove group members so that members who are added may optionally be denied access to the key material used before they joined the group, and that members who are removed lose access to the key material following their departure.
6. It must be possible to provide re-key for the group without requiring unicast exchange between a key distribution center (KDC)and individual members, which would overwhelm a KDC when the group is large.
7. The key management protocol must be suitable for IPsec security protocols, AH and ESP, and/or application-layer security protocols such as AMESP and SRTP.
8. The key management protocol should allow keys and algorithms to be renewed and the trust infrastructure and authentication systems to be replaced.