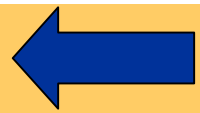
Evolving the SMuG Framework to a Group and Multicast Architecture

<draft-irtf-smug-framework-01.txt>

Thomas Hardjono (Nortel)
Ran Canetti (IBM)
Mark Baugher (Cisco)
Peter Dinsmore (NAI)

Group & Multicast Security Architecture

Goals



Requirements

The SMuG Framework

MSEC Architecture Elements

MSEC Architecture Draft

Goals

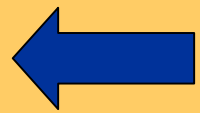
- Describe the MSEC architecture
  - Summarize requirements
  - Define the abstractions
  - Define relationship of functional elements
  - Define relationship of protocols
- Build upon SMuG Reference Framework
  - Evolve the framework of the initial specifications

The authors of the SMuG Reference Framework propose to evolve this document into the MSEC Architecture draft specification

Group & Multicast Security Architecture

Goals

Requirements



The SMuG Framework

MSEC Architecture Elements

MSEC Architecture Draft

Security Services

- Group policy definition and interfaces
- Group membership management
- Source & group authentication
- Data transforms
- Group key management

We take as a requirement that services need to support IPSec and application-layer security protocols.

Scalability and Performance

- Goal is to support large, 1:N groups
  - Scalable membership management
  - State management in GCKS
  - GCKS implosion
  - Tree bandwidth-utilization
- Support real-time packet rates
  - Real-time source-authentication needed

Transport and Network Services

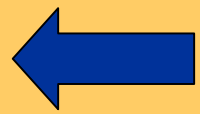
- SA definition for groups, multicast
  - SAD and SPD
  - Selectors, bundles
- IPv6 as well as IPv4
- Tunnel versus transport mode

Group & Multicast Security Architecture

Goals

Requirements

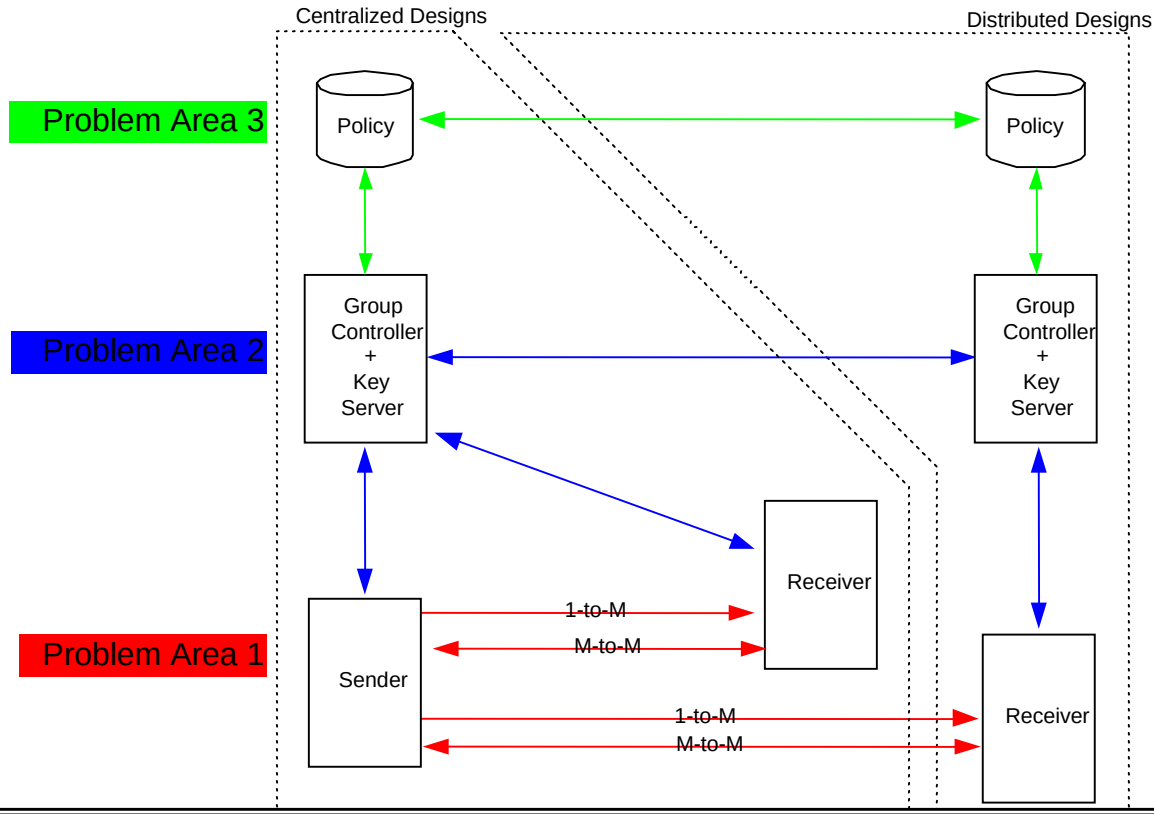
The SMuG Framework



MSEC Architecture Elements

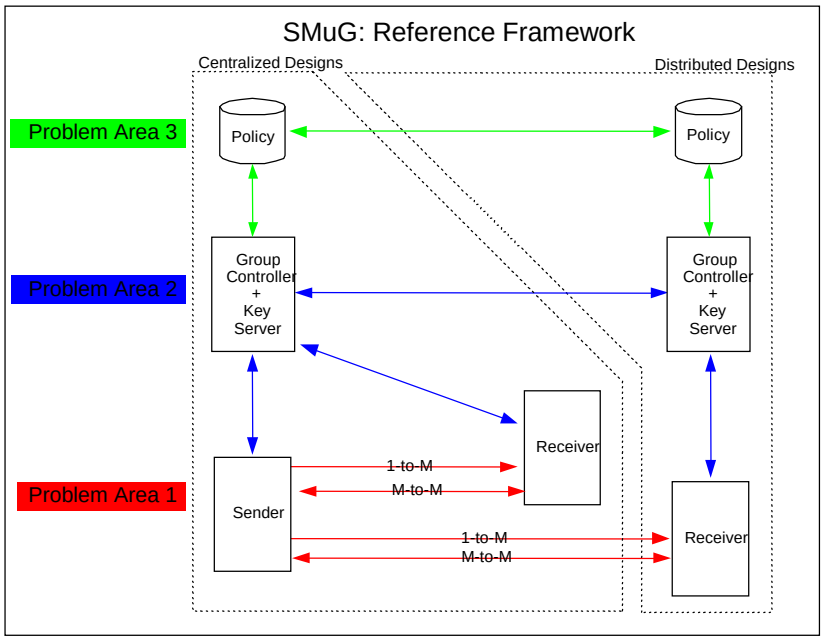
MSEC Architecture Draft

SMuG Reference Framework



The framework oriented the work of SMuG. Each box is a functional entity and each line is an interfaced to be realized by a protocol .

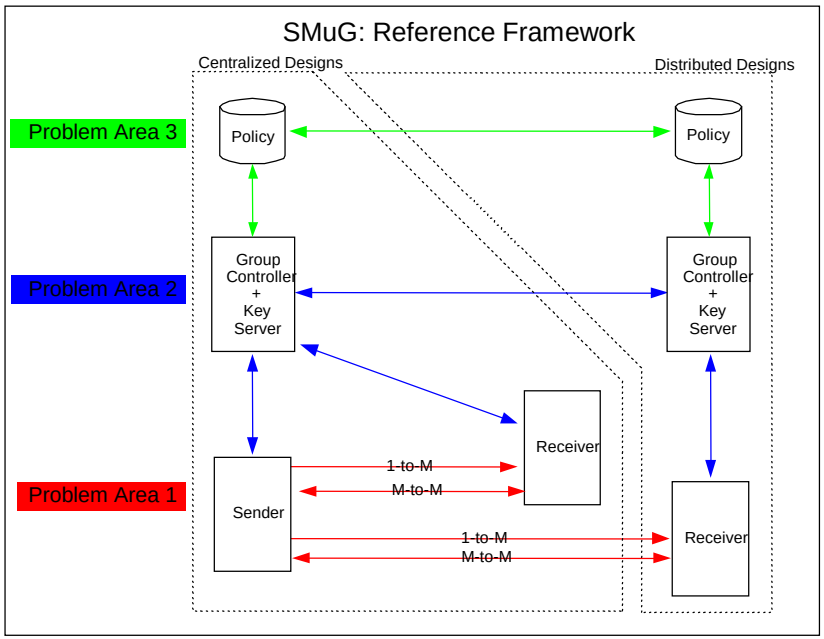
3 Entity Types, Interfaces



- Policy repository
- Group Controller-Key Server
- Sender/Receiver

Group Controller authorizes access to keys and groups; the key server acts on behalf of the Group Controller. We merged these functions.

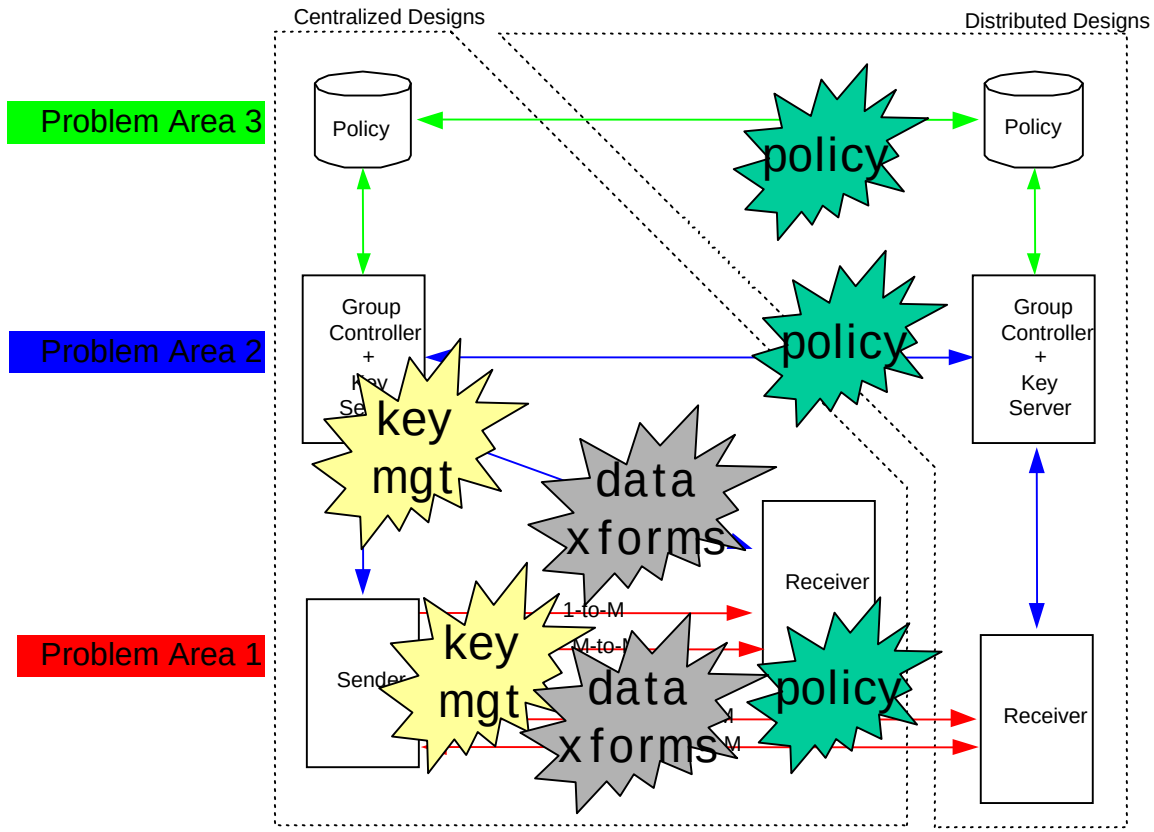
Centralized and Distributed Designs



- Centralized Designs: **single policy domain**
- Distributed Designs: **span administrative domains**

We propose to focus on centralized designs and leave distributed designs to SMuG for ongoing work.

Functions Span Interfaces, Entities

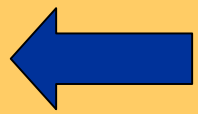


Group & Multicast Security Architecture

Goals

Requirements

The SMuG Framework

MSEC Architecture Elements 

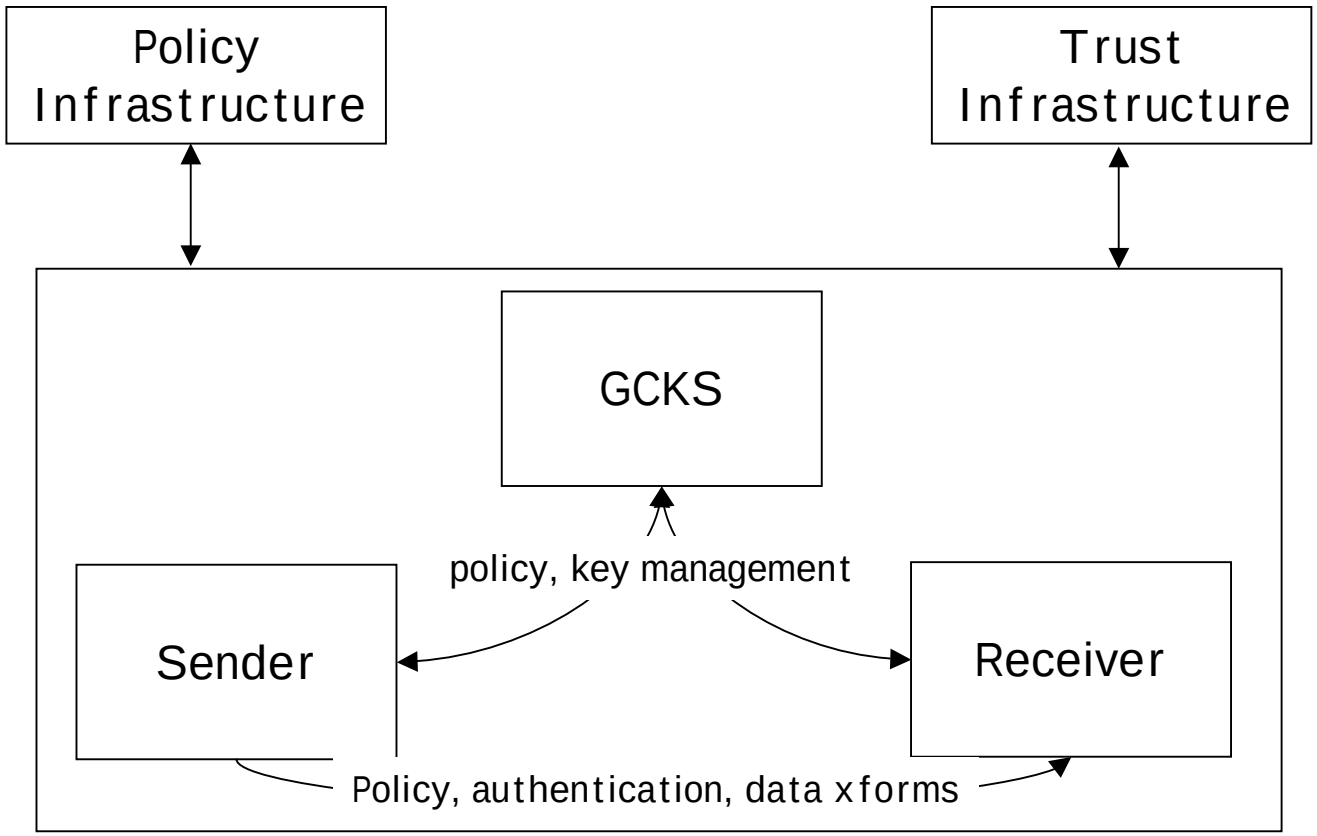
MSEC Architecture Draft

Whither the Reference Framework?

- We should adapt the Framework
  - Don't need to talk about problem areas
  - Should defer distributed designs
- The functional entities, interfaces remain
  - GCKS to Policy Server
  - GCKS to Sender/Receiver
  - Sender to Receiver

We propose to develop a document that uses elements from SMuG Framework and approaches our problem as RFC 2401 approached IPSec.

MSEC Block Diagram



Group & Multicast Security Architecture

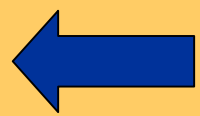
Goals

Requirements

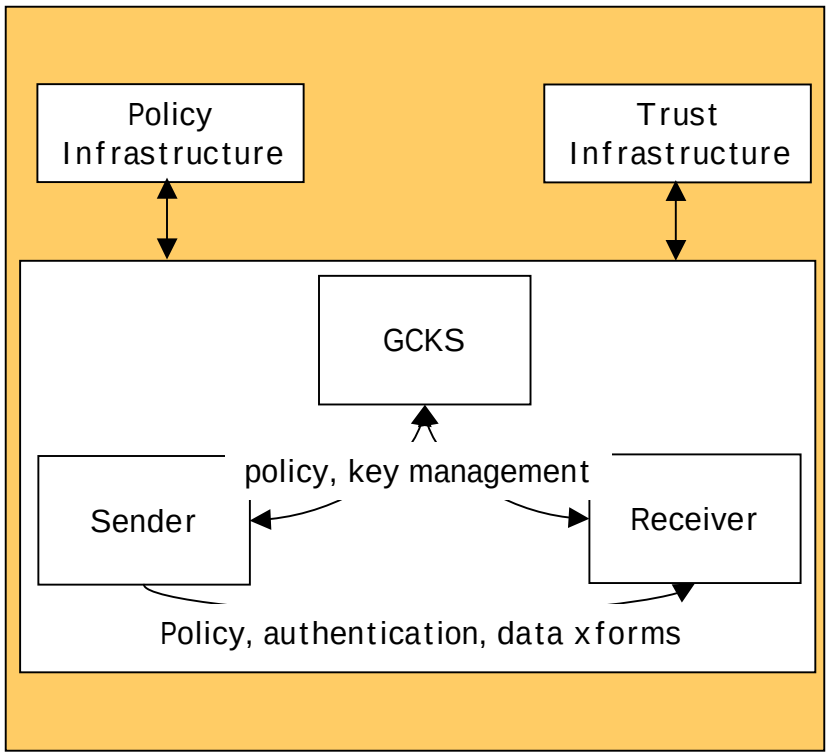
The SMuG Framework

MSEC Architecture Elements

MSEC Architecture Draft



MSEC Architecture Draft



- Propose to begin draft
- Review requirements
  - Security services
  - Performance, scalability
  - Transport & network
- Describe architecture
  - Abstractions
  - Interfaces