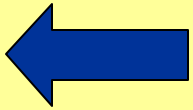
Secure IP Multicast: Problem Areas, Framework, and Building Blocks

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

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

Problem Areas, Framework and Building Blocks

Introduction 

Reference Framework

Building Blocks

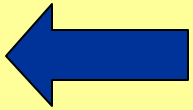
Status of Our Work

Introduction

- RFC 2014 Offers Guidelines for IRTF WGs
  - Investigate topics important to future
  - Present work in appropriate venues
  - Identify potential technologies for standards
- SMuG Framework devised to focus work
  - Summarize research & requirements results
  - Identify areas and technologies for standards

Problem Areas, Framework and Building Blocks

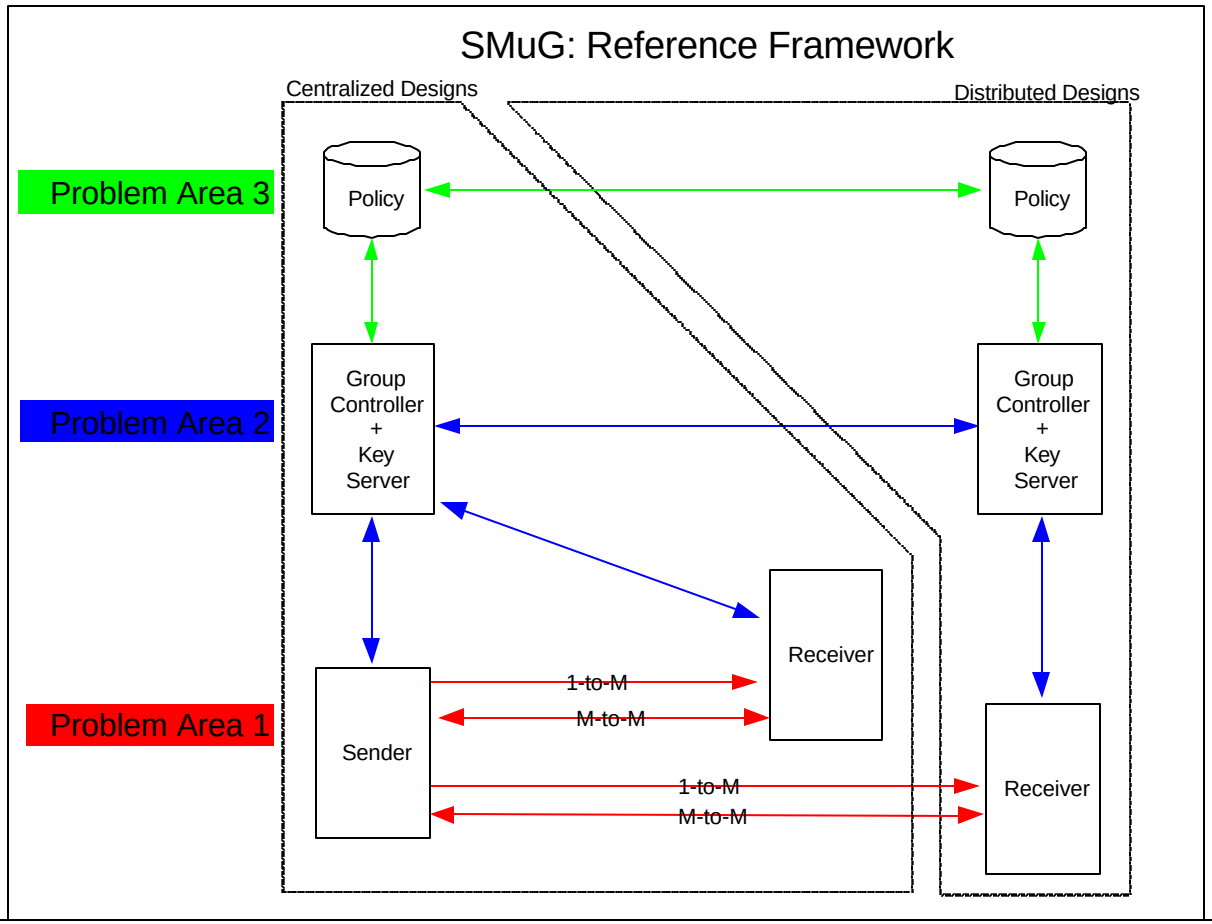
Introduction

Reference Framework 

Building Blocks

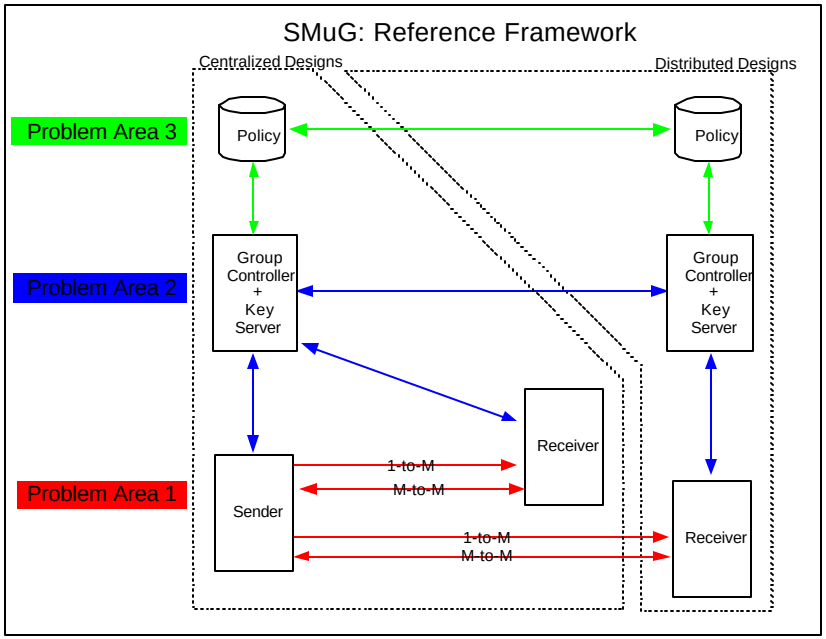
Status of Our Work

SMuG Reference Framework



Each box depicts a functional unit and each arrow an interface, which may be realized by a protocol operating over an internetwork.

3 Types of Entities, Interfaces



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

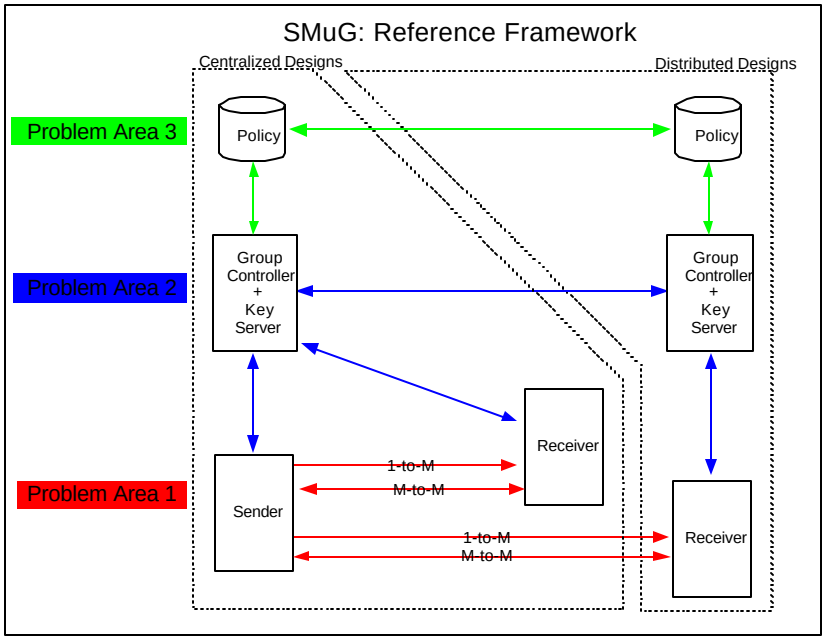
Group Controller authorizes access to keys and groups; the key server acts on behalf of the Group Controller. We merged these functions.

Problem Areas

- Protecting 1:N and M:N data distribution
  - Authentication, integrity, access control
  - Solution is needed for IP multicast applications
- Managing group keys
  - Efficiently keying various size groups
  - Managing membership in groups of various sizes
- Defining and maintaining group policy
  - Authorization, access control, crypto policy definition and mechanisms

The 3 Problem Areas summarize and simplify much work done in the area of functional and performance requirements.

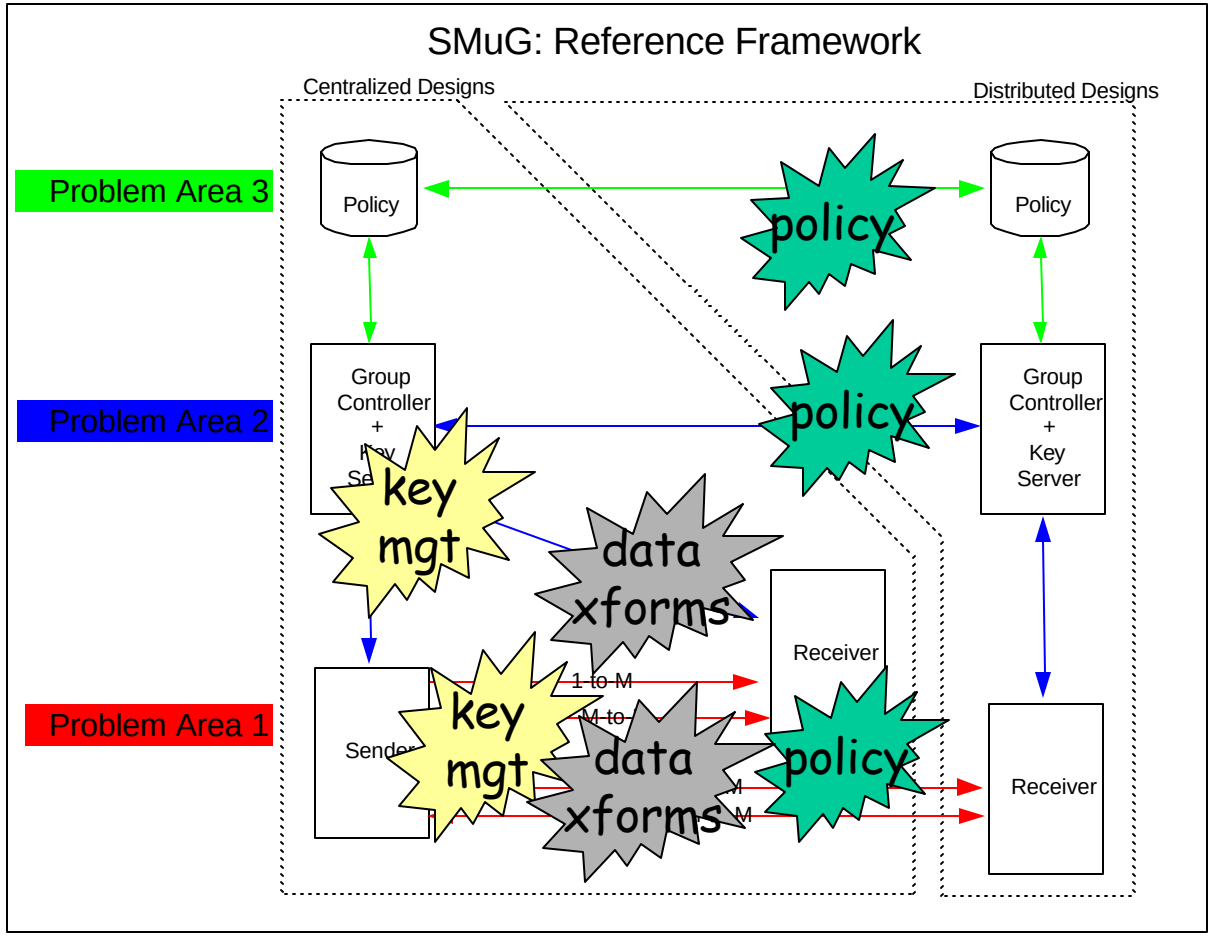
Centralized and Distributed Designs



- Centralized Designs: **single policy domain.**
- Distributed Designs: **spans administrative domains.**

The SMuG work to-date has focused on centralized rather than distributed designs.

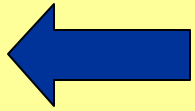
Functions Span Entities and Interfaces



Problem Areas, Framework and Building Blocks

Introduction

Reference Framework

Building Blocks 

Status of Our Work

Building-Blocks Approach

- Decomposes problem into sub-problems
  - We have 6 relatively independent functional "blocks"
  - Developed some protocol and algorithmic blocks as well
- Advantages of building-blocks approach
  - Reuse
  - Timely delivery of useful solutions
  - Robust support for different environments
  - (hopefully) simplicity
- Risks of building-blocks approach
  - Added work to integrate independent blocks
  - Reduced performance caused by too much modularization
  - Complexity of too many blocks with too many interfaces

4 SMuG Building Blocks

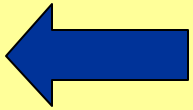
Data Transforms	Source, Group authentication, integrity, and data encryption for internetwork and application-layer multicast
Membership management	Group announcement, member registration, deregistration
Key distribution	Maintaining keys among group members in a scalable manner
Policy definition	Extensions to Internet policy infrastructure needed for groups

Problem Areas, Framework and Building Blocks

Introduction

Reference Framework

Building Blocks

Status of Our Work 

SMuG Building-Block Output