Multicast Security BOF (MSEC)

MSEC BOF Agenda

- Part 1: Tuesday 14:15 - 15:15
  - Session chair: Thomas Hardjono
- Break

- Part 2: Tuesday 17:00 - 18:00
  - Session Chair: Ran Canetti
- Break

MSEC BOF

- Welcome
- Background
- Agenda
  - 2 Parts, with break in between
- BOF guidelines:
  - Assumed to have read the drafts
  - Questions at the end of each Part
  - Longer discussion at the end of Part 2

Background

- Why the BOF/WG:
  - to bring mature work-items from IRTF to IETF
    - Building Blocks and Protocol Instantiations
- IRTF Secure Multicast Group (SMuG):
  - SMuG formed in July-1998 (Chicago IETF)
  - "Research" the problem of Multicast Security
  - Broader Group Security (not just IP Multicast)
- Solutions increasingly needed:
  - Content-protection in content networks
    - ties-in with Digital Rights Management
  - Other protocols that have group behaviors

Background (continued)

- Specific items for MSEC:
  - Data transforms
    - A/MESP
  - Source authentication
    - TESLA
  - Group Security Association (GSA) management
    - Group DOI and GSAKMP
  - Group Key Determination algorithms
    - LKH and OFT
- Future:
  - MSEC and SMuG in parallel
    - Comparisons: RMRG/RMT, AAA/AAAarch

MSEC BOF Agenda

- Part1:
  - Agenda bashing — 10 min — Thomas Hardjono
  - Charter presentation — 10 min — Ran Canetti
  - Taxonomy of Issues — 10 min — Ran Canetti
  - SMuG Framework — 10 min — Mark Baugher
  - Data transforms — 10 min — Ran Canetti
  - TESLA — 10 min — Adrian Perrig
  - Questions
- Part 2:
  - GKM Building Block — 10 min — Thomas Hardjono
  - GSAKMP — 10 min — Hugh Harney
  - Group DOI for ISAKMP — 10 min — Brian Weis
  - Security analysis of GDOI — 10 min — Cathy Meadows
  - Group policy — 10 min — Patrick McDaniel
  - Discussion & Questions

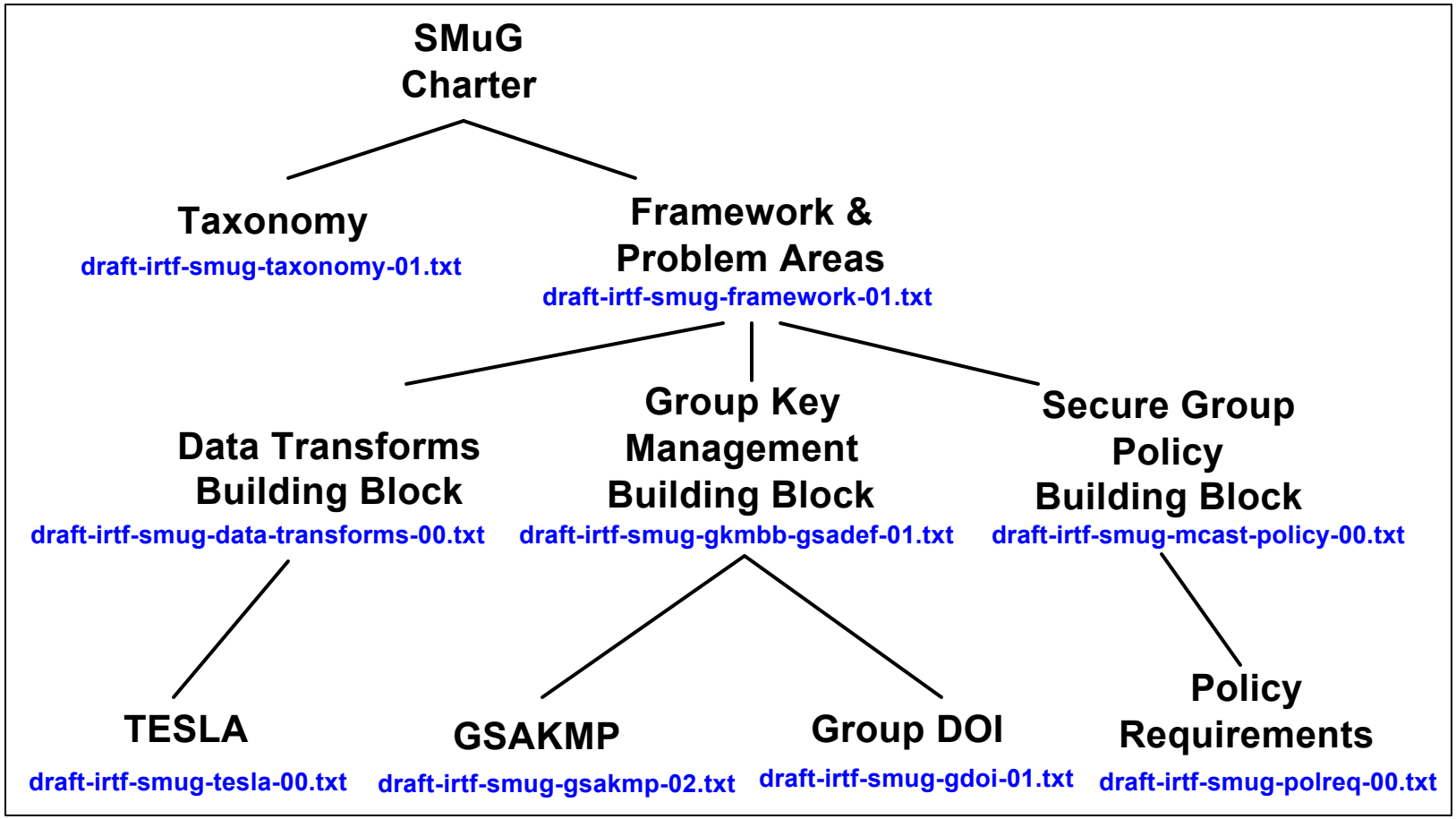
MSEC Agenda - Part 1

- Time: 14:15 - 15:15
- Agenda bashing — Thomas Hardjono
- Charter presentation — Ran Canetti
- Taxonomy of Issues — Ran Canetti
- SMuG Framework — Mark Baugher
- Data transforms — Ran Canetti
- TESLA — Adrian Perrig
- Questions
- Break

MSEC Agenda - Part 2

- Time: 17:00 - 18:00
- GKM Building Block — Thomas Hardjono
- GSAKMP — Hugh Harney
- Group DOI for ISAKMP — Brian Weis
- Security analysis of GDOI — Cathy Meadows
- Group policy — Patrick McDaniel
- Discussion & Questions
- Close

Drafts Roadmap



End of Agenda Bashing