# Group key management architecture -05-

**Mark Baugher**
**Ran Canetti**
**Lakshminath Dondeti**
**Fredrik Lindholm**

**IETF-57 MSEC WG meeting**
**July 14 2003, Vienna, Austria**

# My last slide from IETF-56

- **Will be adding a comparison chart/section on GDOI, GSAKMP, and MIKEY**
  - Hope we can explain why we need three!
- **The next rev appears to be substantial**
  - Note: Only clarification, no new requirements really
- **Proposed last call March 2003 according to the new Charter** ☺
  - Informational/Standards RFC?

# GKM Architecture updates

- **Introduction is revised slightly**
- **Added a section on applicability of the IETF group key management protocols**
  - GKMA? (old Experimental RFC 2094)
  - Tunneled GSAKMP (MSEC Experimental track)
  - GDOI (Standards track RFC 3547)
  - MIKEY (MSEC Standards track)
  - GSAKMP (MSEC standards track)
  - GDOIv2 (some initial discussion on the list)

# Introduction

- **Added a paragraph on the scope of the MSEC key management architecture**
- **In the next rev, we may make the registration protocol optional ☺**
  - Some group key management algorithms (e.g., SDR) may not need the registration protocol

# Applicability

- **With a number of MSEC key management protocols, it is hard to figure out the applicability for each of them**
- **Added a new section on the topic**
  - Initial text
  - Will add more in the next rev
- **Currently on standards track protocols only**
  - GDOI, GSAKMP, MIKEY
- **Will include some comments on tGSAKMP**
  - Should we talk about GKMP?
- **Protocol authors: please read and comment**

# GDOI

- **Based on IKE**
- **Comes with the advantages and the ISAKMP baggage**
- **Rich feature set**
- **Too many round trips**
- **No support for subordinate GCKS etc.**
- **Target application areas (TBD)**
  - Group keying for IPsec and SRTP

# GSAKMP

- New protocol
- 1.5 to 2.5 RTTs
- No support for legacy protocols, NAT traversal etc.
- Supports subordinate GCKSs
- Policy token
- Target application areas (TBD)

# MIKEY

- Registration protocol only
- ½ RTT or 1 RTT in DH mode
- Belongs in MSEC because of the key download model
- Usually for multimedia call setup in low latency situations
- Uses time stamps for replay protection
- Target application space: peer-to-peer or small interactive group keying (SRTP)

# Conclusion

- **Finish the applicability section**
  - Protocols authors: please (feel free to) send text
- **Add text on the optionality of the registration protocol**
- **Plan to finish and go to WG last call in August (4-6 weeks from today)**
  - Informational RFC
- **Questions**