

# RMT Working Group Status

*Brian Adamson/ Lorenzo Vicisano*

74<sup>th</sup> IETF

27 March 2009

# Agenda

1. Agenda Bashing  
*5 min - All*
2. WG Progress  
*20 min - WG Chairs & Document Editors*
3. "TESLA for ALC/NORM"  
- draft-ietf-msec-tesla-for-alc-norm-07  
*5 min - Vincent Roca*
4. "Simple Authentication for ALC/NORM"  
- draft-ietf-rmt-simple-auth-for-alc-norm-01  
*5 min - Vincent Roca*
5. "FCAST Update"- draft-roca-rmt-newfcast-04  
*5 min – Vincent Roca / Brian Adamson*
6. "LCT Update"- draft-ietf-rmt-bb-lct-revised-08  
*5 min – Mark Watson*
7. Open Discussion, Related Work & Announcements  
*25 min - All*

# RMT RFCs Published

- RFC 5401 - “Multicast Negative-Acknowledgment (NACK) Building Blocks”, November 2008
- RFC 5445 – “Basic Forward Error Correction (FEC) Schemes”, March 2009
  - This clears the way for “Reed-Solomon FEC” document to be published.
  - Errata already submitted against RFC 5445: RFC Editor XML comment appears in published document text.

# RMT Documents Submitted for Publication

- draft-ietf-rmt-pi-norm-revised
  - *AD review completed (thanks Magnus!)*
- draft-ietf-rmt-bb-lct-revised-08
  - *In AD evaluation*
- draft-ietf-rmt-pi-alc-revised-06
- draft-ietf-rmt-flute-revised-06
- draft-ietf-rmt-sec-discussion-03
  - *needs AD attention?*

# Updated RMT Documents

- [draft-ietf-rmt-simple-auth-for-alc-norm-01](#)
- [draft-roca-rmt-newfcast-04](#)
- [draft-ietf-rmt-bb-lct-revised-08](#)

# TESLA for ALC / NORM

*-Vincent Roca*

- MSEC WG document of high RMT interest
- draft-ietf-msec-tesla-for-alc-norm-07
  - Completed WG last call
  - Ready for Publication

# Simple Authentication for ALC/NORM

*- Vincent Roca*

- Updated draft:
  - draft-ietf-rmt-simple-auth-for-alc-norm-01
  - Added description of Elliptic Curve Cryptography (ECC) support
- Comments received:
  - Some minor editorial comments
  - Would like to see references to support the pros/cons table on Page 6.

# FCAST Update

- *Brian Adamson / Vincent Roca*

- Updated draft
  - draft-roca-rmt-newfcast-04
  - Added “checksum” FCAST compound object header
    - 16-bit one-complement checksum (UDP, TCP)
  - Overall editorial enhancements
- Outstanding Issues
  - Some details with respect to Transport Object Identifier (TOI) assignment compatible with NORM.
  - Should this be an RMT WG document?



IETF #74, 22-27 March 2009  
RMT working group

draft-ietf-rmt-lct-revised-08

Mark Watson

# draft-ietf-rmt-bb-lct-revised-08

- Address AD and other miscellaneous comments
- Update references
- Substantially revise security considerations
  - Focus on requirements that must be met by PIs
  - Avoid duplication of solution material from ALC