Security Area Advisory Group

Stephen Farrell

Sean Turner

March 14, 2013

note well summary

- The brief summary:
  - This summary is only meant to point you in the right direction, and doesn't have all the nuances; see below for the details.
  - By participating with the IETF, you agree to follow IETF processes.
  - If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.
- You understand that meetings might be recorded and broadcast.
- The details:
  - For further information, talk to a chair, ask an Area Director, or review BCP 9 (on the Internet Standards Process), BCP 25 (on the Working Group processes), BCP 78 (on the IETF Trust) , and BCP 79 (on Intellectual Property Rights in the IETF).

agenda

- WG Reports, <10 mins
- Security Related BOFs, 10 mins
- Invited Presentation
  - NIST SHA-3 Update - 15 minutes (Quynh Dang)
  - iSchedule/DKIM - 5 minutes (Cyrus Daboo)
  - SSH BCP - 15 minutes (Tatu Ylonen)
  - W3C Web Crypto API Update - 30 minutes (Ryan Sleevi)
- Open Mike

WGs

oauth

- Chairs
  - Derick Atkins
  - Hannes Tschofenig

ipsecme

- Chairs
  - Paul Hoffman
  - Yaron Sheffer

emu

- Chairs
  - Alan DeKok
  - Joe Salowey

pkix

- Chairs
  - Stephen Kent
  - Stefan Santesson

httpauth

- Chairs
  - Yoav Nir
  - Matt Lepinski

jose

- Chairs
  - Jim Schaad
  - Karen O’Donoghue

mile

- Chairs
  - Kathleen Moriarty
  - Brian Trammell

abfab

- Chairs
  - Leif Johansson
  - Klaas Wierenga

kitten

- Chairs
  - Shawn Emery
  - Josh Howlett
  - Sam Hartman

tls

- Chairs
  - Eric Rescorla
  - Joe Salowey

dane

- Chairs:
  - Ondřej Surý
  - Warren Kumari

not meeting

nea

- Chairs
  - Stephen Hanna
  - Susan Thomson

not meeting

BOFs

sacm

- Chairs
  - Dan Romascanu
  - Kathleen Moriarty

other

- Security Related WGs
  - WEBSEC
  - HTTPBIS
  - Routing: KARP & SIDR
  - PRECISE
  - WPKOPS
- Security Related RGs
  - CFRG

Invited Presentations

- NIST SHA-3 Update - 15 minutes (Quynh Dang)
- iSchedule/DKIM - 5 minutes (Cyrus Daboo)
- SSH BCP - 15 minutes (Tatu Ylonen)
- W3C Web Crypto API Update - 30 minutes (Ryan Sleevi)

OPEN MIC