Security Area Advisory Group

Stephen Farrell

Sean Turner

July 28, 2011

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

  - the IETF plenary session,
  - any IETF working group or portion thereof,
  - the IESG or any member thereof on behalf of the IESG,
  - the IAB or any member thereof on behalf of the IAB,
  - any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices,
  - the RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

- WG Reports
- BOF Reports
- Invited Presentation
  - NIST SHA-3 Update (Tim Polk)
  - Issues in Identifier Comparison for Security Purposes (Dave Thaler)
  - KMP for IEEE 802.15 (Robert Moskowitz)
- Open Mike

ltans

(Long Term Archive and Notary Service)

- Final work item published: RFC 6283
- Closed

pkix

- Stephen Kent
- Stefan Santesson

emu

- Alan DeKok
- Joe Salowey
- http://www.ietf.org/mail-archive/web/saag/current/msg03422.html

oauth

- Barry Leiba
- Hannes Tschofenig
- Blaine Cook
- http://www.ietf.org/mail-archive/web/saag/current/msg03421.html

nea

- Stephen Hanna
- Susan Thomson
- http://www.ietf.org/mail-archive/web/saag/current/msg03423.html

krb-wg

- Jeff Hutzelman
- Larry Zhu
- Sam Hartman

hokey

- Tina Tsou
- Glen Zorn
- (meeting Thursday 1520-1720)

tls

- Eric Rescorla
- Joe Salowey
- (meeting Thursday 1520-1720)

kitten

- Shawn Emery
- Tom Yu
- Alexey Melnikov
- (meeting Thursday 1740-1940)

abfab

- Leif Johansson
- Klaas Wierenga
- (meets Friday 0900-1130)

dane

- Ondrej Sury
- Warren Kumari
- (meets Friday 1300-1515)

dkim

- Barry Leiba
- (not meeting this week)
- http://www.ietf.org/mail-archive/web/
  saag/current/msg03412.html

msec

- Vincent Roca
- Brian Weis
- (not meeting this week)

ipsecme

- Paul Hoffman
- Yaron Sheffer
- (not meeting this week)
- http://www.ietf.org/mail-archive/web/saag/current/msg03415.html

isms

- Jürgen Schönwälder
- Russ Mundy
- (not meeting this week)

Other WGs and BOFs

- BOF
  - Web Object Encryption and Signature (WOES)
  - Common Interface to Cryptographic Modules (CICM)
- Security Related WGs
  - KARP
  - SIDR
  - WEBSEC
- Side Meetings
  - PLASMA

Invited Presentations

- NIST SHA-3 Update (Tim Polk)
- Issues in Identifier Comparison for Security Purposes (Dave Thaler)
- KMP for IEEE 802.15 (Robert Moskowitz)

Open Mike

- Concerns?
- Issues?
- Soap Box?