Security Area Advisory Group

Notes: https://notes.ietf.org/notes-ietf-113-saag

Meetecho: https://meetings.conf.meetecho.com/ietf113/?group=saag&short=&item=1

Benjamin Kaduk
Roman Danyliw
Paul Wouters

IETF 113 -- Session III
Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
Living the IETF Code of Conduct

Reminder of the key points of the Code of Conduct [RFC7154]:

1. IETF participants extend respect and courtesy to their colleagues at all times
2. IETF participants have impersonal discussion
3. IETF participants devise solutions for the global Internet that meet the needs of diverse technical and operational environments
Agenda

1. Welcome, Administrivia, and Agenda Bashing (5 mins)

2. WG Reports (10 mins, chairs)

3. AD Report (15 mins, ADs)

4. Introduction to IPsec (30min, Paul Wouters)

5. Open Mic (remaining time)
Working Group Summaries
ACE

Chairs

- Daniel Migault
- Loganaden Velvindron

Report

https://mailarchive.ietf.org/arch/msg/saag/vPGAKfwSPpmIINQSF1-2kbSR6Q6M/
ACME

Chairs

- Deb Cooley
- Yoav Nir

Report

https://mailarchive.ietf.org/arch/msg/saag/czhalltgD0LBGjZcyzItm2Aimb4/
COSE

Chairs
- Matthew Miller
- Ivaylo Petrov
- Mike Jones

Report
  xxx
EMU

Chairs
• Joe Salowey
• Mohit Sethi

Report

https://mailarchive.ietf.org/arch/msg/saag/jptt5gA8AyJfUchaG58TSPlxWoY/
LAKE

Chairs

• Stephen Farrell
• Mališa Vučinić

Report

https://mailarchive.ietf.org/arch/msg/saag/SjLXrrFVHLxZIXJHJAk0pH8J6dM/
MLS

Chairs
- Nick Sullivan
- Sean Turner

Report
https://mailarchive.ietf.org/arch/msg/saag/agjP1ll0GUO6ymE3LAMiVQRUnJE/
OAUTH

Chairs

- Hannes Tschofenig
- Rifaat Shekh-Yusef

Report

XXX
OHAI

Chairs

- Richard Barnes
- Shivan Sahib

Report

xxx
OPENPGP

Chairs

- Daniel Gillmor
- Stephen Farrell

Report

https://mailarchive.ietf.org/arch/msg/saag/pT7fYNYh56vNlwphd5Tjv-JlpaA/
PrivacyPass

Chairs
- Benjamin Schwartz
- Joseph Salowey

Report

xxx
RATS

Chairs

- Nancy Cam-Winget
- Ned Smith
- Kathleen Moriarty

Report

xxx
SecDispatch

Chairs

• Richard Barnes
• Kathleen Moriarty
• Mohit Sethi

Report

https://mailarchive.ietf.org/arch/msg/saag/Z2wJCj385VvcLK6wi8H1om_Woe8/
SUIT

Chairs

- Russ Housley
- Dave Thaler
- David Waltermire

Report

https://mailarchive.ietf.org/arch/msg/saag/s6dyxppjYpWzvv8sDyAyJbeyEUY/
TEEP

Chairs

- Nancy Cam-Winget
- Tirumaleswar Reddy

Report

https://mailarchive.ietf.org/arch/msg/saag/MOmpLxwrr21UyPkJTvt9I1Hci5g/
TLS

Chairs

- Joe Salowey
- Sean Turner
- Chris Wood

Report

xxx
WGs meeting later in the week

- DANCE
- GNAP
- I2NSF
- IPSECME – https://mailarchive.ietf.org/arch/msg/saag/C5o0oXz2d22yww0fmV334RCZQow/
- LAMPS
- PPM
WG's not meeting at IETF 113

- KITTEN
- SACM
- SECEVENT
Related Non-SEC Area Activities

Security Topics in Related WGs
- ADD
- ANIMA
- DIME
- DISPATCH
- DMARC
- DPRIVE
- DRIP
- HTTPBIS
- QUIC
- NETCONF
- NTP
- OPSEC
- PERC
- RADext
- SCIM
- SFRAME
- SIDROPS
- STIR
- UTA
- TAPS

BoFs
- SECRET

Security Related IRTF
- CFRG
- PEARG

IAB Programs
- model-t

External related
- W3C
- IEEE
- ITU
- NIST Lightweight Crypto
- NIST PQC
# AD Sponsored Drafts

<table>
<thead>
<tr>
<th>Draft</th>
<th>Sponsor</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>draft-foudil-securitytxt</td>
<td>Paul</td>
<td>RFC Ed Queue</td>
</tr>
<tr>
<td>draft-gont-numeric-ids-sec-considerations</td>
<td>Paul</td>
<td>IESG::Waiting for Writeup</td>
</tr>
<tr>
<td>draft-housley-ers-asn1-modules</td>
<td>Roman</td>
<td>RFC9169</td>
</tr>
<tr>
<td>draft-eastlake-rfc6931bis-xmlsec-uris</td>
<td>Roman</td>
<td>RFC Ed Queue</td>
</tr>
<tr>
<td>draft-yee-ssh-iana-requirements</td>
<td>TBD</td>
<td>Dispatched to ADs at IETF113</td>
</tr>
</tbody>
</table>
SEC Area Pointers

Common SEC AD DISCUSS items
- https://trac.ietf.org/trac/sec/wiki/TypicalSECAreaIssues

Where is my document that is with AD/IESG?
- https://datatracker.ietf.org/doc/ad/roman.danyliw
- https://datatracker.ietf.org/doc/ad/paul.wouters

SEC Area Summary
- https://trac.ietf.org/trac/sec/wiki
<table>
<thead>
<tr>
<th>Category</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post-BOF</td>
<td>SECRET*</td>
</tr>
<tr>
<td>New</td>
<td>PPM</td>
</tr>
<tr>
<td>Closed</td>
<td>CURDLE</td>
</tr>
<tr>
<td>Rechartered</td>
<td></td>
</tr>
<tr>
<td>In Rechartering</td>
<td>RATS</td>
</tr>
</tbody>
</table>

* in ART, overseen by SEC
## WG Chair Changes

<table>
<thead>
<tr>
<th>WG</th>
<th>Departures</th>
<th>Additions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DANCE</td>
<td>- Paul Wouters</td>
<td>+ Joey Salazar</td>
</tr>
<tr>
<td>KITTEN</td>
<td>- Robbie Harwood</td>
<td></td>
</tr>
<tr>
<td>PPM</td>
<td></td>
<td>+ Benjamin Schwartz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ Samuel Weiler</td>
</tr>
<tr>
<td>SCIM*</td>
<td></td>
<td>+ Aaron Parecki</td>
</tr>
</tbody>
</table>

* in ART, overseen by SEC
# New Responsible ADs by WG

<table>
<thead>
<tr>
<th>Paul</th>
<th>Roman</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACE</td>
<td>ACME</td>
</tr>
<tr>
<td>COSE</td>
<td>GNAP</td>
</tr>
<tr>
<td>DANCE</td>
<td>I2NSF</td>
</tr>
<tr>
<td>DOTS</td>
<td>IPSECME</td>
</tr>
<tr>
<td>EMU</td>
<td>LAMPS</td>
</tr>
<tr>
<td>KITTEN</td>
<td>OAUTH</td>
</tr>
<tr>
<td>LAKE</td>
<td>OPENPGP</td>
</tr>
<tr>
<td>MLS</td>
<td>PPM</td>
</tr>
<tr>
<td>PRIVACYPASS</td>
<td>RATS</td>
</tr>
<tr>
<td>RADEXT</td>
<td>SACM</td>
</tr>
<tr>
<td>TEEP</td>
<td>SECEVENT</td>
</tr>
<tr>
<td>TLS</td>
<td>SUIT</td>
</tr>
<tr>
<td></td>
<td>SCIM</td>
</tr>
</tbody>
</table>
# New Non-WG Mailing List

<table>
<thead>
<tr>
<th>WG</th>
<th>Departures</th>
</tr>
</thead>
<tbody>
<tr>
<td>scitt@ietf</td>
<td>Supply Chain Integrity, Transparency, and Trust (SCITT).</td>
</tr>
<tr>
<td></td>
<td>See IETF 113 SecDispatch result</td>
</tr>
</tbody>
</table>
Help on Errata Processing

264 Reported Errata for SEC Work


![Errata Count by Open WG](chart.png)

153 Reported Errata (58% of Total)
Thanks to the
In-Person WG Delegates

ACE, DANCE, SECDISPATCH -- Paul Wouters
I2NSF -- Rifaat Shekh-Yusef
LAMPS -- Alexey Melnikov
MLS -- Stephen Farrell
OHAI — Francesca Palombini
PPM -- Joe Salowey
SUIT -- Nancy Cam-Winget
Thanks to the SECDIR Reviewers since IETF 112

- Alexey Melnikov
- Barry Leiba
- Benjamin Schwartz
- Carl Wallace
- Catherine Meadows
- Charlie Kaufman
- Chris Lonvick
- Christian Huitema
- Christopher Wood
- Dan Harkins
- Daniel Migault
- David Mandelberg
- Derrell Piper
- Donald Eastlake
- Hilarie Orman
- Joseph Salowey
- Kyle Rose
- Linda Dunbar
- Magnus Nystrom
- Melinda Shore
- Paul Wouters
- Phillip Hallam-Baker
- Radia Perlman
- Rich Salz
- Rifaat Shekh-Yusef
- Robert Sparks
- Russ Housley
- Russ Mundy
- Samuel Weiler
- Scott Kelly
- Sean Turner
- Shawn Emery
- Stefan Santesson
- Tero Kivinen
- Tirumaleswar Reddy
- Valery Smyslov
- Vincent Roca
- Watson Ladd
- Yaron Sheffer
- Yoav Nir

Thank you to Tero Kivinen for managing the reviews!
Outgoing SEC AD Thank You

Ben Kaduk
Introduction to IPsec
Open Mic