Security Area Advisory Group

Notes: https://notes.ietf.org/notes-ietf-119-saag

Meetecho (full client): https://meetings.conf.meettecho.com/ietf119/?session=32098
Meetecho (on-site): https://meetings.conf.meettecho.com/onsite119/?session=32098

Deb Cooley
Paul Wouters

IETF 119
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)
● https://www.ietf.org/privacy-policy/ (Privacy Policy)
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 discussions
3. IETF participants devise solutions for the global Internet that meet the needs of diverse technical and operational environments
IETF 119 meeting tips

In-person participants
● Make sure to sign into the session using the Meetecho (usually the “Meetecho lite” client) from the Datatracker agenda
● Use Meetecho to join the mic queue
● *Keep audio and video off if not using the onsite version*

Remote participants
● Make sure your audio and video are off unless you are chairing or presenting during a session
● Use of a headset is strongly recommended
Agenda

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

2. WG and AD Reports (15 mins, chairs/ADs)

3. PQ practise across the IETF (20 mins, Eric Rescorla)

4. Open Mic (remaining time)
Roman Danyliw ‘leaving’ Security

Roman Danyliw left the Security Area to become IETF Chair

Roman was the Responsible SEC AD for:

- 22 WGs
- 14 BoFs
- 76 RFCs + 26 in RFC-Editor Queue
- Balloted DISCUSS on 192 drafts
- Closed down 6 WGs

(our secret plan to get a 3rd SEC AD worked!)
New Security Area Director: Deb Cooley

Deb selected by NomCom to replace Roman (1 year term)
New Working Group distribution

Paul Wouters:

- ACE, COSE, DANCE, EMU, Kitten, LAKE, MLS, OpenPGP, PQuip, PrivacyPass, RADEXT, SATP, SPICE (BoF), TLS, TEEP, UTA

Deb Cooley:

- ACME, DULT, GNAP, IPsecME, JOSE, KEYTRANS, LAMPS, OAUTH, PPM, RATS, SCIM, SCITT, SUIT

OHAI moves to Francesca @ ART
# WG Changes since IETF 118

<table>
<thead>
<tr>
<th>BOF</th>
<th>Secure Patterns for Internet Credentials (SPICE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chartering (charter at IESG)</td>
<td>-</td>
</tr>
<tr>
<td>New WG</td>
<td>Detecting Unwanted Location Trackers (DULT)</td>
</tr>
<tr>
<td>Closed WG</td>
<td>TIGRESS</td>
</tr>
<tr>
<td>Rechartered</td>
<td>-</td>
</tr>
<tr>
<td>In Rechartering (charter at WG or IESG)</td>
<td>OPENPGP, MLS and LAKE</td>
</tr>
</tbody>
</table>
## WG Chair Changes

<table>
<thead>
<tr>
<th>WG</th>
<th>Departures</th>
<th>Additions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACME</td>
<td>Deb Cooley</td>
<td>Tomofumi Okubo</td>
</tr>
<tr>
<td>DULT</td>
<td></td>
<td>Erica Olsen, Sean Turner</td>
</tr>
<tr>
<td>KEYTRANS</td>
<td>Orie Steele</td>
<td>Prachi Jain</td>
</tr>
<tr>
<td>SCITT</td>
<td>Hannes Tschofenig</td>
<td>Chris Inacio</td>
</tr>
<tr>
<td>SUIT</td>
<td>David Thaler</td>
<td>Akira Tsukamoto</td>
</tr>
<tr>
<td>TLS</td>
<td>Christopher Wood</td>
<td>Deirdre Connolly</td>
</tr>
<tr>
<td>UTA</td>
<td>Orie Steele</td>
<td>Alan deKok</td>
</tr>
</tbody>
</table>
Helping out

1. If you are interested in becoming a WG chair, let your ADs know. Experience not always a plus!
2. Become a document Shepherd. Learn about IETF processes while helping advancing documents! Ask your AD if shepherding is right for you!
3. Errata processing - help your WG resolve reported erratas. We also have errata in closed WGs that no one is looking at.
4. Attend (virtual and in person) BoFs
## Working Group Summaries

Send highlights and summaries to saag@ietf.org

<table>
<thead>
<tr>
<th>ACE</th>
<th>ACME</th>
<th>COSE</th>
<th>DANCE</th>
<th>DULT</th>
<th>EMU</th>
<th>GNAP</th>
<th>IPSECME</th>
<th>JOSE</th>
<th>KEYTRANS</th>
</tr>
</thead>
<tbody>
<tr>
<td>KITTEN</td>
<td>LAKE</td>
<td>LAMPS</td>
<td>MLS</td>
<td>OAUTH</td>
<td>OPENPGP</td>
<td>PPM</td>
<td>PQUIP</td>
<td>PRIVACYPASS</td>
<td>RADEXT</td>
</tr>
<tr>
<td>RATS</td>
<td>SATP</td>
<td>SCITT</td>
<td>SCIM</td>
<td>SecDispatch</td>
<td>SUIT</td>
<td>TEEP</td>
<td>TLS</td>
<td>UTA</td>
<td></td>
</tr>
</tbody>
</table>

* (OHAI moved to WIT)
Related Non-SEC Area Activities

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

Security Related IRTF
- CFRG
- PEARG
- UFMRG

IAB Programs

External related
- W3C
- IEEE
- ITU
- NIST Lightweight Crypto
- NIST PQC
# New Non-WG Mailing Lists

<table>
<thead>
<tr>
<th>List Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SKEX</td>
<td>symmetric keys as secure key exchange</td>
</tr>
<tr>
<td>id-align</td>
<td>aligning identity terminology and bringing awareness of identity standards work.</td>
</tr>
</tbody>
</table>
## AD Sponsored Drafts

<table>
<thead>
<tr>
<th>Draft</th>
<th>Sponsor</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>draft-gutmann-testkeys</td>
<td>Paul</td>
<td>RFC 9500</td>
</tr>
<tr>
<td>draft-josefsson-ntruprime-ssh</td>
<td>Roman</td>
<td>Negative review from Crypto Panel</td>
</tr>
<tr>
<td>draft-pismenny-tls-dtls-plaintext-sequence-number</td>
<td>&lt;tbd&gt;</td>
<td>&lt;tbd&gt;</td>
</tr>
<tr>
<td>draft-eastlake-fnv-20</td>
<td>&lt;tbd&gt;</td>
<td>&lt;tbd&gt;</td>
</tr>
</tbody>
</table>
# Errata Processing

<table>
<thead>
<tr>
<th></th>
<th>Total Open Errata</th>
<th>Since Last Meeting</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Closed</td>
<td>Reported</td>
</tr>
<tr>
<td>at IETF 119</td>
<td>279</td>
<td>-33</td>
<td>+17</td>
</tr>
<tr>
<td>at IETF 118</td>
<td>295</td>
<td>-16</td>
<td>+15</td>
</tr>
<tr>
<td>at IETF 117</td>
<td>296</td>
<td>0</td>
<td>+8</td>
</tr>
<tr>
<td>at IETF 116</td>
<td>288</td>
<td>-3</td>
<td>+16</td>
</tr>
<tr>
<td>at IETF 115</td>
<td>275</td>
<td>-1</td>
<td>+10</td>
</tr>
<tr>
<td>at IETF 114</td>
<td>266</td>
<td>-15</td>
<td>+17</td>
</tr>
<tr>
<td>at IETF 113</td>
<td>264</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
SEC Area Pointers

Security Area

Common SEC AD DISCUSS items
- https://wiki.ietf.org/group/sec/typicalSECareaissues

Where is my document that is with AD?
- https://datatracker.ietf.org/doc/ad/deb.cooley [*]
- https://datatracker.ietf.org/doc/ad/paul.wouters
- https://datatracker.ietf.org/doc/ad/roman.danyliw [**]

What is on the next IESG telechat?
- https://datatracker.ietf.org/iesg/agenda/documents/
Thanks to the SECDIR Reviewers

78 SecDir reviewers in the pool:
https://datatracker.ietf.org/group/secdir/about/

SecDir meets for a free BYO lunch on Tuesday of IETF

Thank you to Tero Kivinen for managing the reviews!
180 SecDir reviews since IETF 118

<table>
<thead>
<tr>
<th>Team</th>
<th>Serious Issues</th>
<th>Has Issues</th>
<th>Has Nits</th>
<th>Not Ready</th>
<th>Ready</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecDir</td>
<td>3</td>
<td>37</td>
<td>53</td>
<td>5</td>
<td>82</td>
</tr>
<tr>
<td>%</td>
<td>2%</td>
<td>21%</td>
<td>29%</td>
<td>3%</td>
<td>46%</td>
</tr>
</tbody>
</table>

- **Serious Issues**: 3
- **Has Issues**: 37
- **Has Nits**: 53
- **Not Ready**: 5
- **Ready**: 82

**Percentage Distribution**

- Serious Issues: 2%
- Has Issues: 21%
- Has Nits: 29%
- Not Ready: 3%
- Ready: 46%
### SecDir IETF-119 Completion Stats

<table>
<thead>
<tr>
<th>Team</th>
<th>Open in time</th>
<th>Open late in time</th>
<th>Completed in time</th>
<th>Completed Late</th>
<th>Not Completed</th>
<th>Avg. Compl. days</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecDir</td>
<td>23</td>
<td>0</td>
<td>110</td>
<td>70</td>
<td>45</td>
<td>16.7</td>
</tr>
<tr>
<td>%</td>
<td>9%</td>
<td>0%</td>
<td>44%</td>
<td>28%</td>
<td>18%</td>
<td></td>
</tr>
</tbody>
</table>

![Pie chart](chart.png)

- **Open in Time**
- **Open Late**
- **Completed in time**
- **Completed late**
- **Not Completed**
PQ practise across the IETF

Eric Rescorla
Pure PQ key establishment?

- NIST-standardized PQ key establishment (ML-KEM) coming soon
  - How do we deploy them?
- Broad interest in standardizing hybrid PQ/Traditional algorithms
  - E.g., X25519 + ML-KEM-768
  - TLS, SSH, LAMPS
- Some interest in standardizing PQ algorithms alone
  - LAMPS, CNSA 2.0
  - TLS just decided not to do this
Should we have a consistent practice across IETF?

- I assume this would be either
  - Standardize both PQ/T hybrid + pure PQ
  - Standardize PQ/T hybrid only and wait on pure PQ

- Mostly you can register code points without a standard
- This is about what IETF recommends
Open Mic