Security Area Advisory Group

Notes: https://notes.ietf.org/notes-ietf-115-saag

Meetecho: https://meetings.conf.meetecho.com/ietf115/?group=saag&short=&item=1

Roman Danyliw

Paul Wouters

IETF 115
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/](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/](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 discussion
3. IETF participants devise solutions for the global Internet that meet the needs of diverse technical and operational environments
IETF 115 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
● Wear masks unless actively speaking at the presenter microphone

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. Implementation report from EDUROAM's adoption of EAP/RADIUS (Margaret Cullen)

4. Role of formal verification in the standards process (ADs)

5. HTTP Message Signatures (draft-ietf-httpbis-message-signatures) (Justin Richer)

6. Open Mic (remaining time)
Helping out

1. If you are interested in becoming a 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 harvesting - help your WG resolve reported erratas. It’s fun and it’s free! We also have errata in closed WGs that no one is looking at (discuss where?)

4. Attend (virtual and in person) BoFs
## WG Changes since IETF 114

| BOF                          | JSON Web Proofs (JWP)*  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Radius (RADEXTRA),</td>
</tr>
<tr>
<td></td>
<td>Secure Asset Transfer (SATP)</td>
</tr>
<tr>
<td>Chartering</td>
<td>JOSE (was JWP BOF)</td>
</tr>
<tr>
<td>New</td>
<td>SCITT</td>
</tr>
<tr>
<td>Closed</td>
<td></td>
</tr>
<tr>
<td>Rechartered</td>
<td></td>
</tr>
<tr>
<td>In Rechartering</td>
<td></td>
</tr>
</tbody>
</table>

*SEC has held 2 interim BoFs in the last 6-months – appears to be accelerating the start of new work*
<table>
<thead>
<tr>
<th>ACE</th>
<th>LAMPS</th>
<th>TEEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACME</td>
<td>MLS</td>
<td>TLS</td>
</tr>
<tr>
<td>COSE</td>
<td>OAUTH</td>
<td>UTA</td>
</tr>
<tr>
<td>DANCE</td>
<td>OHAI</td>
<td></td>
</tr>
<tr>
<td>DOTS</td>
<td>OPENPGP</td>
<td></td>
</tr>
<tr>
<td>EMU</td>
<td>PPM</td>
<td></td>
</tr>
<tr>
<td>GNAP</td>
<td>PrivacyPass</td>
<td></td>
</tr>
<tr>
<td>I2NSF</td>
<td>RATS</td>
<td></td>
</tr>
<tr>
<td>IPsecME</td>
<td>SCITT</td>
<td></td>
</tr>
<tr>
<td>LAKE</td>
<td>SecDispatch</td>
<td></td>
</tr>
<tr>
<td>KITTEN</td>
<td>SUIT</td>
<td></td>
</tr>
</tbody>
</table>
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

Security Related IRTF
- CFRG
- PEARG

IAB Programs
- model-t

External related
- W3C
- IEEE
- ITU
- NIST Lightweight Crypto
- NIST PQC
## WG Chair Changes

<table>
<thead>
<tr>
<th>WG</th>
<th>Departures</th>
<th>Additions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECDISPATCH</td>
<td>Mohit Sethi Richard Barnes</td>
<td>Rifaat Shekh-Yusef</td>
</tr>
<tr>
<td>SCITT</td>
<td></td>
<td>Jon Geater Hannes Tschofenig</td>
</tr>
</tbody>
</table>

* in ART, overseen by SEC
# New Non-WG Mailing Lists

<table>
<thead>
<tr>
<th>List Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td></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-knodel-e2ee-definition</td>
<td>Paul</td>
<td>AD Evaluation:: Revised I-D Needed</td>
</tr>
<tr>
<td>draft-gont-numeric-ids-sec-considerations</td>
<td>Paul</td>
<td>AD Evaluation:: Revised I-D Needed</td>
</tr>
<tr>
<td>draft-leggett-spkac</td>
<td>Roman</td>
<td>NEW, from SecDispatch at IETF 115</td>
</tr>
<tr>
<td>draft-moskowitz-ipsecme-ipseckey-eddsa</td>
<td>Roman</td>
<td>AD Evaluation:: Revised I-D Needed</td>
</tr>
<tr>
<td>draft-yee-ssh-iana-requirements</td>
<td>Roman</td>
<td>Waiting for Writeup:: Revised I-D Needed</td>
</tr>
</tbody>
</table>

Per SecDispatch results at IETF 114, still exploring next step for draft-eastlake-fnv
# Errata Processing

<table>
<thead>
<tr>
<th></th>
<th>Total Open Errata</th>
<th>Since Last Meeting</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Closed</td>
<td>Reported</td>
<td></td>
</tr>
<tr>
<td>at IETF 115</td>
<td>275</td>
<td>-1</td>
<td>+10</td>
<td></td>
</tr>
<tr>
<td>at IETF 114</td>
<td>266</td>
<td>-15</td>
<td>+17</td>
<td></td>
</tr>
<tr>
<td>at IETF 113</td>
<td>264</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

Need help from TLS, LAMPS, OAUTH, ACME, EMU, IPSEC(ME)
Additional PQC Next Steps Side Meeting on Monday


Strong support for chartering a “PQC Transition Support WG”

Identified technologies which need PQC agility but are without a WG
- SSH, Kerberos and XML Signature

Now is NOT the right time to consider a “PQC Directorate”
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

NomCom: Give feedback to SEC AD candidates

- https://datatracker.ietf.org/nomcom/2022/nominate/

SEC Area Summary

- https://trac.ietf.org/trac/sec/wiki
Thanks to the SECDIR Reviewers

- Adam W. Montville
- Alexey Melnikov
- Barry Leiba
- Brian Weis
- Carl Wallace
- Catherine Meadows
- Charlie Kaufman
- Chris M. Lonvick
- Christian Huitema
- Dan Harkins
- Daniel Migault
- Dave Thaler
- David Mandelberg
- Deb Cooley
- Derrell Piper
- Dick Hardt
- Donald E. Eastlake 3rd
- Hilarie Orman
- Ivaylo Petrov
- Joey Salazar
- Joseph A. Salowey
- Kathleen Moriarty
- Klaas Wierenga
- Kyle Rose
- Leif Johansson
- Linda Dunbar
- Magnus Nystrom
- Mališa Vučinić
- Melinda Shore
- Mohit Sethi
- Nancy Cam-Winget
- Ned Smith
- Phillip Hallam-Baker
- Rich Salz
- Rifaat Shekh-Yusef
- Russ Housley
- Russ Mundy
- Sean Turner
- Shawn M Emery
- Shivan Kaul Sahib
- Stefan Santesson
- Stefan Santesson
- Stephen Farrell
- Steve Hanna
- Tero Kivinen
- Tirumaleswar Reddy.K
- Valery Smyslov
- Vincent Roca
- Watson Ladd
- Wes Hardaker
- Yoav Nir

Thank you to Tero Kivinen for managing the reviews!
Implementation report from EDUROAM's adoption of EAP/RADIUS
Formal verification in the standards process

Past success was WG-driven or on the initiative of external parties taking in interest in an IETF protocol
- https://trac.ietf.org/trac/sec/wiki/FormalVerification

Is something more deliberate needed?
- For what type of work?
- As a MAY? SHOULD? MUST? Do these change per type of work?
- When (in the lifecycle of the document)?
- Who can help us?
HTTP Message Signatures (draft-ietf-httpbis-message-signatures)
Open Mic