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/) 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 IEFT 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)* Radius (RADEXTRA), Secure Asset Transfer (SATP)
Chartering	JOSE (was JWP BOF)
New	SCITT
Closed	
Rechartered	
In Rechartering	

*SEC has held 2 interim BoFs in the last 6-months – appears to be accelerating the start of new work

Working Group Summaries

Please sent IETF 115 summaries to saag@ietf.org

ACE

ACME

COSE

DANCE

DOTS

EMU

GNAP

I2NSF

IPsecME

LAKE

KITTEN

LAMPS

MLS

OAUTH

OHAI

OPENPGP

PPM

PrivacyPass

RATS

SCITT

SecDispatch

SUIT

TEEP

TLS

UTA

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

WG	Departures	Additions
SECDISPATCH	Mohit Sethi Richard Barnes	Rifaat Shekh-Yusef
SCITT		Jon Geater Hannes Tschofenig

* in ART, overseen by SEC

New Non-WG Mailing Lists

List Name	Purpose
none	

AD Sponsored Drafts

Draft	Sponsor	Status
draft-knodel-e2ee-definition	Paul	AD Evaluation:: Revised I-D Needed
draft-gont-numeric-ids-sec-considerations	Paul	AD Evaluation:: Revised I-D Needed
draft-leggett-spkac	Roman	NEW, from SecDispatch at IETF 115
draft-moskowitz-ipsecme-ipseckey-eddsa	Roman	AD Evaluation:: Revised I-D Needed
draft-yee-ssh-iana-requirements	Roman	Waiting for Writeup:: Revised I-D Needed

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

Errata Processing

	Total Open Errata	Since Last Meeting	
		Closed	Reported
at IETF 115	275	-1	+10
at IETF 114	266	-15	+17
at IETF 113	264	N/A	N/A

Need help from
TLS, LAMPS, OAUTH, ACME, EMU, IPSEC(ME)

Additional PQC Next Steps Side Meeting on Monday

https://github.com/rdanyliw/ietf-pqc-transition/blob/main/ietf115-pqc-next-steps-side-meeting.md

Strong support for chartering a “PQC Transition Support WG”

- Charter Text: https://github.com/rdanyliw/ietf-pqc-transition/blob/main/pqct-charter.md

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