Security Area Advisory Group

Notes: https://notes.ietf.org/notes-ietf-117-saag

Meetecho: https://meetings.conf.meetecho.com/ietf117/?session=30595

Roman Danyliw

Paul Wouters

IETF 117

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 discussions
3. IETF participants devise solutions for the global Internet that meet the needs of diverse technical and operational environments

IETF 117 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. Implementation Report: Let's Encrypt and ACME (Richard Barnes) (15 min)

4. Wholistic Human-Oriented Discussions on Identity Systems (WHODIS) IAB Program (Cullen Jennings, Rifaat Shekh-Yusef, Dick Hardt) (15 min)

5. Open Mic (remaining time)

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

WG Changes since IETF 116

BOF	Detecting Unwanted Location Trackers (DULT)
Chartering	Key Transparency (KEYTRANS)
New	–
Closed	I2NSF and SECEVENT
Rechartered	LAKE
In Rechartering	–

Working Group Summaries

Please sent IETF 117 summaries to saag@ietf.org

- ACE
- ACME
- COSE
- DANCE
- DOTS
- EMU
- GNAP
- I2NSF
- IPsecME
- JOSE
- LAKE
- KITTEN
- LAMPS
- MLS
- OAUTH
- OHAI
- OPENPGP
- PPM
- PQUIP
- PrivacyPass
- RADEXT
- RATS
- SATP
- SCITT
- SecDispatch
- SCIM
- SUIT
- TEEP
- TIGRESS
- 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
- SFRAME
- SIDROPS
- STIR
- TAPS

Security Related IRTF

- CFRG
- PEARG

IAB Programs

- (proposed) WHODIS
- UFMRG

External related

- W3C
- IEEE
- ITU
- NIST Lightweight Crypto
- NIST PQC

WG Chair Changes

WG	Departures	Additions
SECDISPATCH	Kathleen Moriarty	

New Non-WG Mailing Lists

List Name	Purpose
wimse@ietf	"Workload Identity in Multi-Service Environment (WIMSE)" – Discussion of workload identity in complex multi-service environments

AD Sponsored Drafts

Draft	Sponsor	Status
draft-gont-numeric-ids-sec-considerations	Paul	RFC 9416
draft-gutmann-testkeys	Paul	IESG Review
draft-leggett-spkac	Roman	Awaiting AD review
draft-yee-ssh-iana-requirements	Roman	Approved-announcement to be sent::AD Followup

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 117	296	0	+8
at IETF 116	288	-3	+16
at IETF 115	275	-1	+10
at IETF 114	266	-15	+17
at IETF 113	264	N/A	N/A

Need help from

TLS (61), LAMPS (30), OAUTH (28), ACME (16), and EMU (10)

SEC Area Pointers

Security Area

- https://wiki.ietf.org/en/group/sec

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/roman.danyliw
- https://datatracker.ietf.org/doc/ad/paul.wouters

What is on the next IESG telechat?

- https://datatracker.ietf.org/iesg/agenda/documents/

Thanks to the SECDIR Reviewers

since IETF 116

- Alexey Melnikov
- Barry Leiba
- Benjamin Kaduk
- Benjamin M. Schwartz
- Carl Wallace
- Catherine Meadows
- Charlie Kaufman
- Chris M. Lonvick
- Christian Huitema
- Dan Harkins
- Daniel Migault
- David Mandelberg
- Deb Cooley
- Derrell Piper
- Donald E. Eastlake 3rd
- Hilarie Orman
- Ivaylo Petrov
- Joey Salazar
- Joseph A. Salowey
- Kathleen Moriarty
- Klaas Wierenga
- Kyle Rose
- Linda Dunbar
- Mališa Vučinić
- Melinda Shore
- Mike Ounsworth
- Mohit Sethi
- Nancy Cam-Winget
- Ned Smith
- Paul Wouters
- Peter E. Yee
- Radia Perlman
- Rich Salz
- Rifaat Shekh-Yusef
- Robert Sparks
- Russ Housley
- Russ Mundy
- Samuel Weiler
- Scott G. Kelly
- Sean Turner
- Shawn M Emery
- Shivan Kaul Sahib
- Stephen Farrell
- Steve Hanna
- Tero Kivinen
- Tirumaleswar Reddy.K
- Valery Smyslov
- Watson Ladd
- Wes Hardaker
- Yaron Sheffer
- Yoav Nir

Thank you to Tero Kivinen for managing the reviews!

Implementation Report: Let's Encrypt and ACME

(Proposed) Wholistic Human-Oriented Discussions on Identity Systems (WHODIS) IAB Program

Open Mic