# Security Area Advisory Group

Notes: https://notes.ietf.org/notes-ietf-118-saag

Meetecho (full client): https://meetings.conf.meetecho.com/ietf118/?session=31634 Meetecho (on-site): https://meetings.conf.meetecho.com/onsite118/?session=31634



## Roman Danyliw Paul Wouters **IETF 118**

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.
- records of meetings may be made public.

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)
- <u>https://www.ietf.org/privacy-policy/</u> (Privacy Policy)

### SAAG - IETF 118

## Note Well

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

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.

# 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 118 meeting tips

### **In-person participants**

- agenda
- Use Meetecho to join the mic queue

### **Remote participants**

- chairing or presenting during a session
- Use of a headset is strongly recommended

### SAAG - IETF 118

 Make sure to sign into the session using the Meetecho (usually the "Meetecho lite" client) from the Datatracker

• Keep audio and video off if not using the onsite version

Make sure your audio and video are off unless you are



# Agenda

- 1. Welcome, Administrivia, and Agenda Bashing (5 mins)
- 2. WG and AD Reports (15 mins, chairs/ADs)
- 3. Survey of "Newer Cryptography" being used in IETF work (Orie Steele, Chris Wood)
- 4. Open Mic (remaining time)

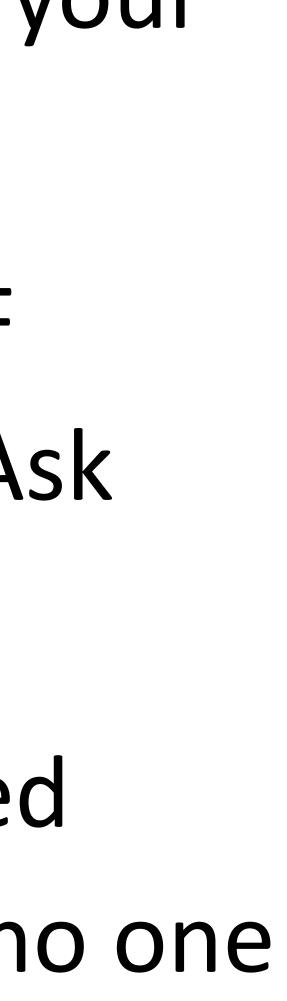




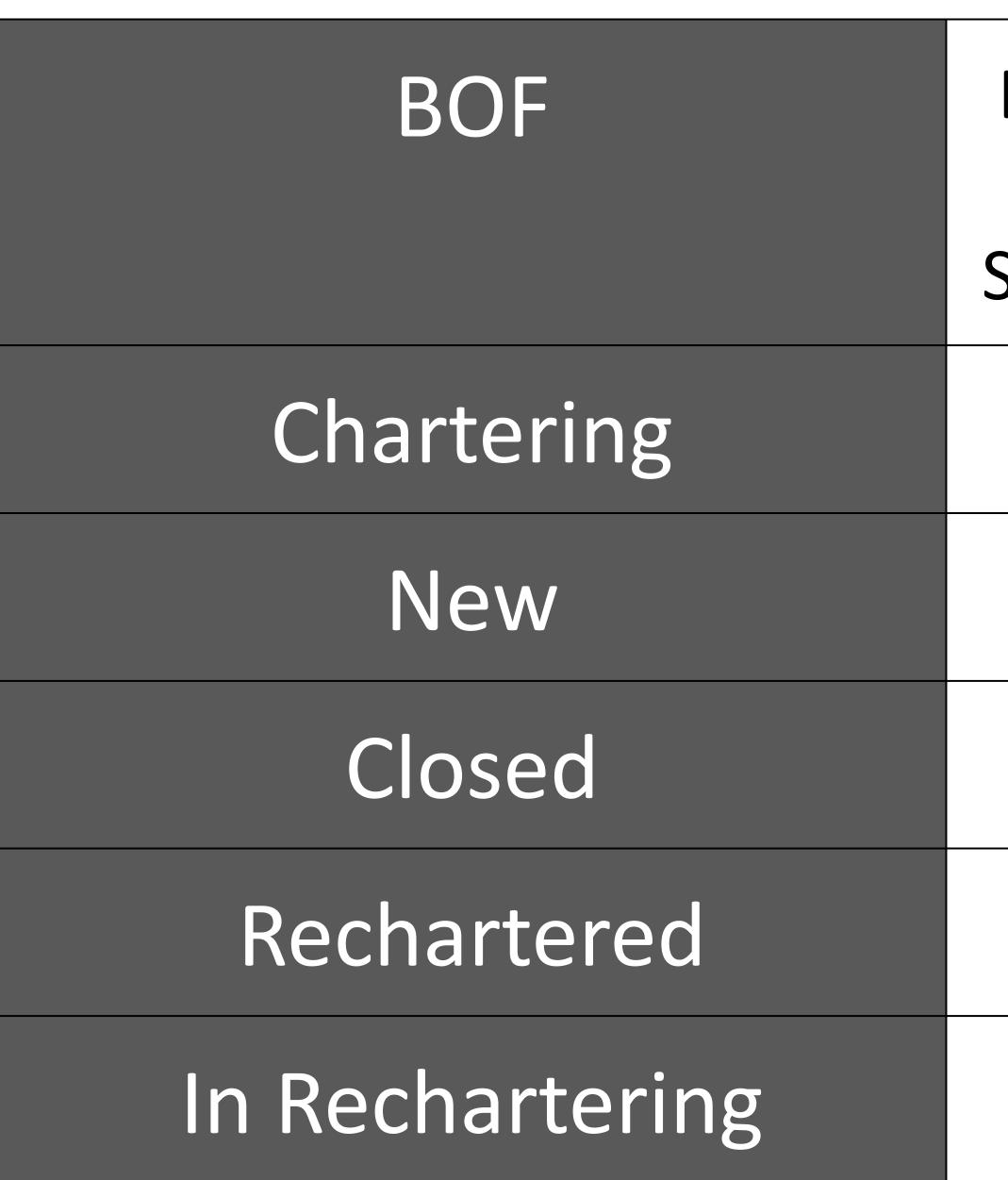
## Helping out

- If you are interested in becoming a WG chair, let your ADs know. Experience not always a plus!
- Become a document Shepherd. Learn about IETF processes while helping advancing documents! Ask your AD if shepherding is right for you!
- 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

### SAAG - IETF 118



# WG Changes since IETF 117



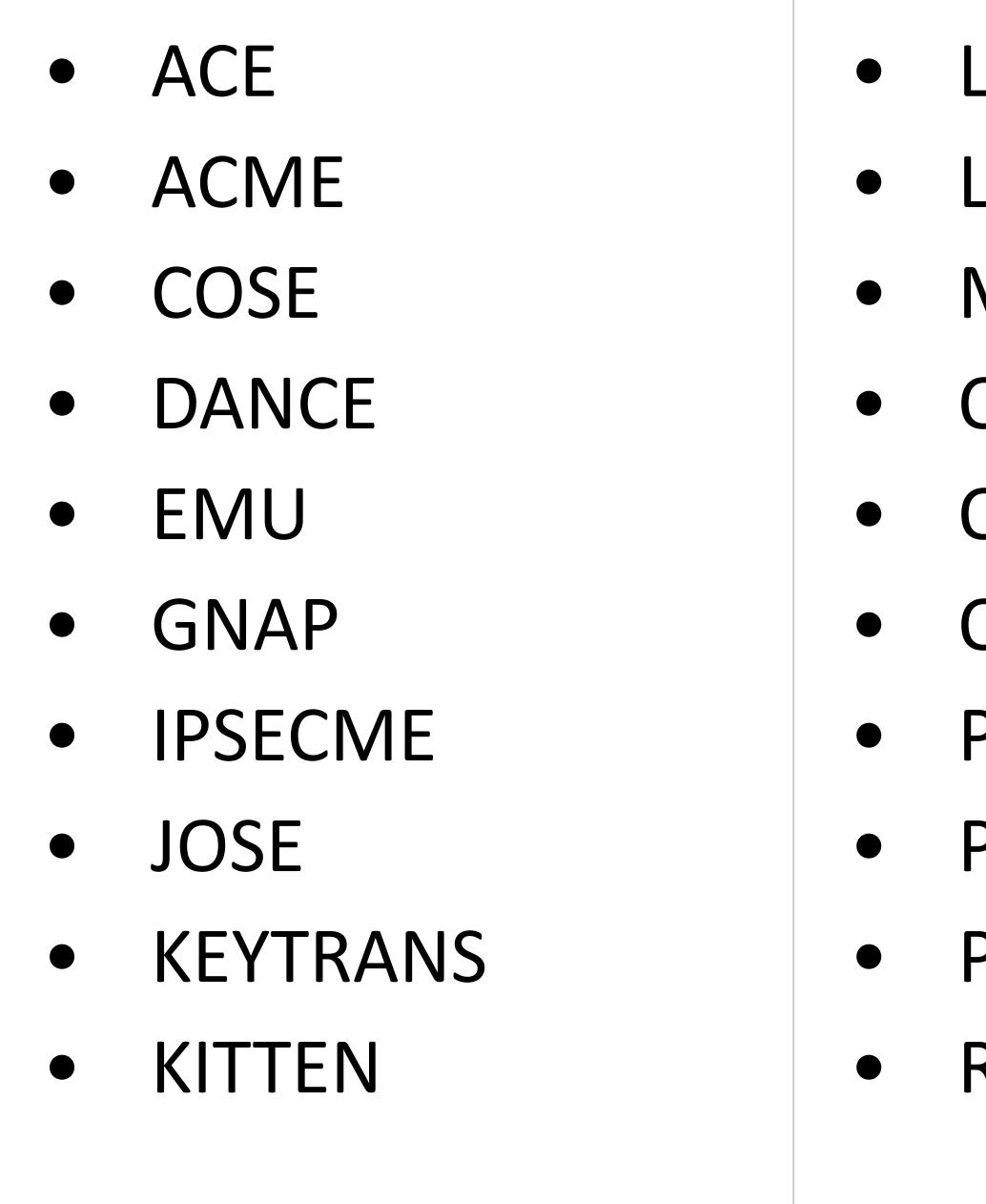
SAAG - IETF 118

- Detecting Unwanted Location Trackers (DULT)
- Secure Patterns for Internet Credentials (SPICE)

Key Transparency (KEYTRANS)

OPENPGP, MLS and LAKE

## Working Group Summaries If you have highlights to share, please sent to saag@ietf.org



to SEC when area reorgnizations occur before/at IETF 119

### SAAG - IETF 118

## \* WGs currently in ART (some with responsible SEC ADs) that officially move

LAKE	RATS
LAMPS	SATP
MLS	SCITT
OAUTH	SecDispatch
OHAI	SCIM*
OPENPGP	SUIT
PPM	TEEP
PQUIP	TIGRESS*
PRIVACYPASS	TLS
RADEXT	UTA*



## **Related Non-SEC Area Activities**

### **Security Topics in Related WGs**

- ADD
- ANIMA
- DIME
- DISPATCH
- DMARC
- DPRIVE
- DRIP
- HTTPBIS
- QUIC
- NETCONF
- NTP
- OPSEC
- PERC
- SATP

• STIR

• TAPS

SAAG - IETF 118

- SFRAME

- SIDROPS

### **Security Related IRTF**

- CFRG
- PEARG
- UFMRG

### **IAB Programs**

• (proposed) WHODIS

### **External related**

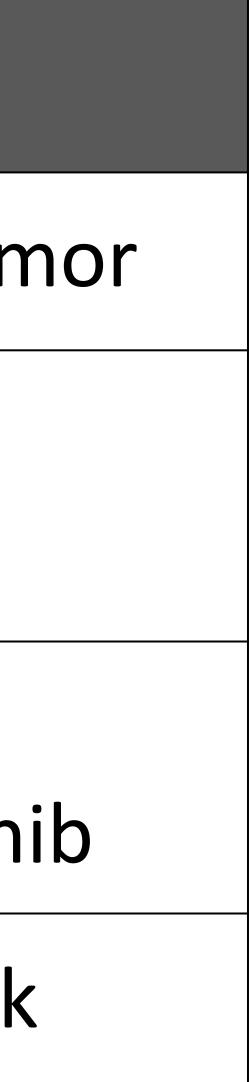
- W3C
- IEEE
- ITU
- NIST Lightweight Crypto
- NIST PQC



# WG Chair Changes

WG	Departures	Additions
SECDISPATCH	Kathleen Moriarty	Daniel Kahn Gillm
SUIT	Russ Housley David Thaler	
KEYTRANS		Orie Steele Shivan Kaul Sahi
ACE	Daniel Migault	Tim Hollebeek





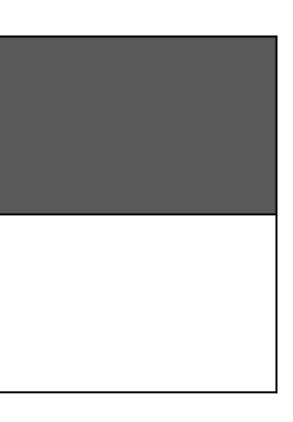
## New Non-WG Mailing Lists

### List Name





Purpose



# AD Sponsored Drafts

### Draft

### draft-gutmann-testkeys

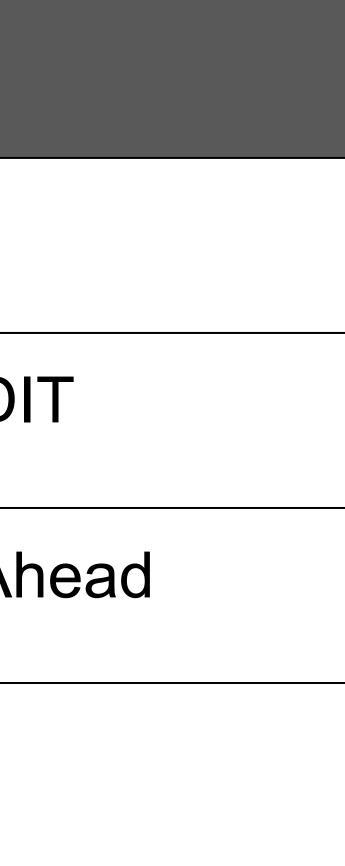
draft-yee-ssh-iana-requirements

draft-josefsson-ntruprime-ssh

draft-pismenny-tls-dtls-plaintext-sequ number



	Sponsor	Status
	Paul	RFC Ed Queue
	Roman	RFC Ed Queue : ED
	Roman	Waiting for AD Go-Al
uence-	<tbd></tbd>	<tbd></tbd>

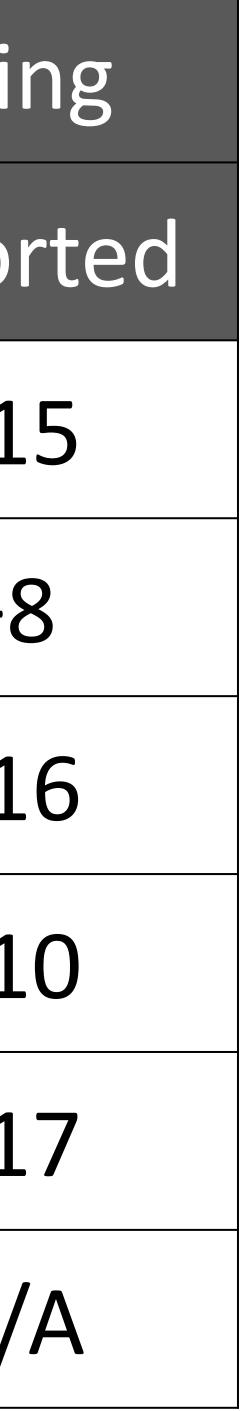


## Errata Processing

	Total Open Errata	Since Last Meeti	
		Closed	Repo
at IETF 118	295	-16	+1
at IETF 117	296	0	+8
at IETF 116	288	-3	+1
at IETF 115	275	-1	+1
at IETF 114	266	-15	+1
at IETF 113	264	N/A	N/



### Need help from: TLS, LAMPS, OAUTH, ACME, and EMU



## SEC Area Pointers

## Security Area

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

## **Common SEC AD DISCUSS items**

https://wiki.ietf.org/group/sec/typicalSECareaissues 

- 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/ 

### SAAG - IETF 118

Where is my document that is with AD?

### Thanks to the SECDIR Reviewers since IETF 117

٠	Alexey Melnikov	•	١v
•	Barry Leiba		K
•	Brian Weis		Li
•	Carl Wallace		$\mathbb{N}$
•	Chris M. Lonvick		$\mathbb{N}$
٠	Dan Harkins	•	$\mathbb{N}$
٠	Daniel Migault		$\mathbb{N}$
•	David Mandelberg		Ν
•	Deb Cooley		P
•	Derrell Piper		R
•	Donald E. Eastlake 3rd		R
•	Hilarie Orman		R

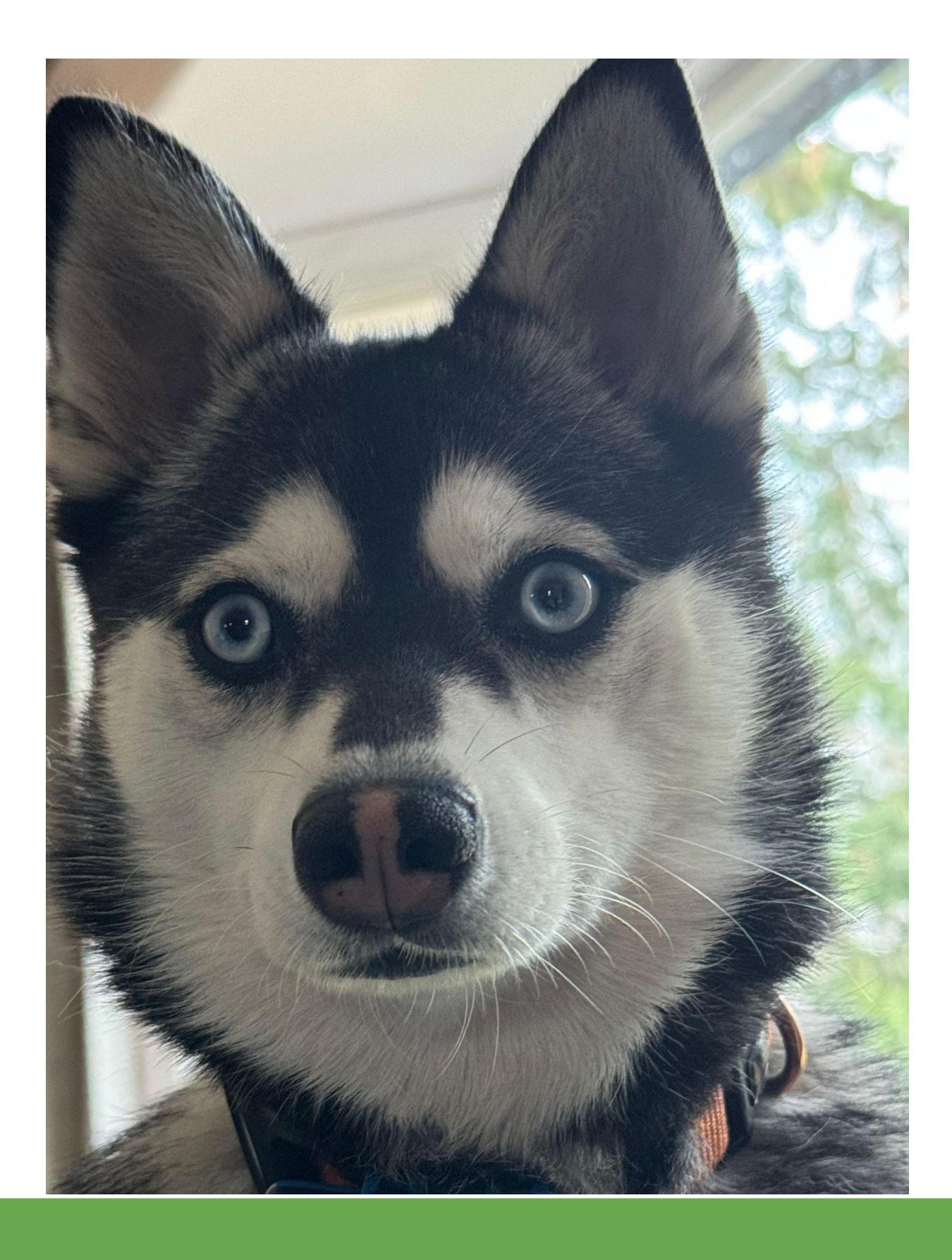
### Thank you to Tero Kivinen for managing the reviews!

### SAAG - IETF 118

- vaylo Petrov
- Kyle Rose
- inda Dunbar
- Magnus Nystrom
- Mališa Vučinić
- Melinda Shore
- Mike Ounsworth
- Jed Smith
- Peter E. Yee
- Radia Perlman
- Rich Salz
- Rifaat Shekh-Yusef

- **Robert Sparks**
- **Russ Housley**
- Sean Turner
- Shawn M Emery
- Shivan Kaul Sahib
- Stephen Farrell
- Tero Kivinen
- Valery Smyslov
- Vincent Roca
- Watson Ladd
- Yaron Sheffer
- Yoav Nir

# Open Mic



### SAAG - IETF 118