Security Area Advisory Group

Notes: https://notes.ietf.org/notes-ietf-121-saag

Meetecho (full client): https://meetecho.ietf.org/client/?session=33522
Meetecho (on-site): https://meetings.conf.meetecho.com/onsite121/?session=33522

Deb Cooley
Paul Wouters

IETF 121 Dublin, Nov 8 2024

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 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. Next Generation Internet EU-funding Update (10 min)
4. Current Cryptography Practices at IETF (30 min, chairs)
5. Open Mic (remaining time)

WG Changes since IETF 120

BOF	
Chartering (charter at IESG)	
New WG	SSHM
Closed WG	GNAP
Rechartered	MLS, LAKE, EMU
In Rechartering (charter at WG or IESG)	LAMPS

WG Chair Changes

WG	Departures	Additions
SSHM		Stephen Farrell Job Snijders
LAKE	Stephen Farrell	?
RATS	Nancy Cam-Winget	N/A (two chairs remain)

Helping out

1. If you are interested in becoming a WG chair, let your ADs know.
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 BoFs (virtually or in person)

Working Group Summaries

Send highlights and summaries to saag@ietf.org

- ACE
- ACME
- COSE
- DANCE
- DULT
- EMU
- IPSECME
- JOSE
- KEYTRANS
- KITTEN
- LAKE
- LAMPS
- MLS
- OAUTH
- OHAI*
- OPENPGP
- PPM
- PQUIP
- PRIVACYPASS
- RADEXT
- RATS
- SCIM
- SCITT
- SecDispatch
- SPICE
- SSHM
- SUIT
- TEEP
- TLS
- UTA

Related Non-SEC Area Activities

Security Topics in Related WGs

- ADD
- ANIMA
- DISPATCH
- DMARC
- DPRIVE
- DRIP
- HTTPBIS
- MIMI
- NETCONF
- NTP
- QUIC
- SATP
- SFRAME
- SIDROPS
- STIR
- TAPS
- TICTOC
- WIMSE

Security Related IRTF

- CFRG
- PEARG
- UFMRG
- HRPC

IAB Programs

External related

- ICANN
- W3C
- IEEE
- ITU
- 3GPP
- CA/B Forum
- PKI Consortium
- NIST Lightweight Crypto
- NIST PQC

New Non-WG Mailing Lists

List Name	Purpose
pq-dnssec@ietf.org	PostQuantum DNSSEC
[tbd]	Site Privacy Policy (“privacy.txt”)

AD Sponsored Drafts

Draft	Sponsor	Status
draft-eastlake-fnv		Going to ISE
draft-tulshibagwale-saag-pushpull-delivery draft-deshpande-secevent-http-multi-push		Possibly re-open secevents

Possibly SEC related dispatch outcomes

Proposal	Suggested
ALFA 2.0 - The Abbreviated Language for Authorization (Theo Dimitrakos)	Hold a BoF
Identifying and Authenticating Home Servers: Requirements and Solution Analysis (Dan Wing)	Hold a BoF Consider IRTF
High Assurance DIDs with DNS (Jesse Carter)	Not in IETF, better fit for W3C
Update IDMEFv1 (Gilles Lehmann)	AD Sponsor, provided viability
A File Format to Aid in Consumer Privacy Enforcement, Research, and Tools (Louise Van der Peet) - privacy.txt	Create a mailing list

Errata Processing

	Total Open Errata	Since Last Meeting	
		Closed	Reported
at IETF 121	250	-23	+18
at IETF 120	257	-50	+27
at IETF 119	279	-33	+17
at IETF 118	295	-16	+15
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

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/deb.cooley
- 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

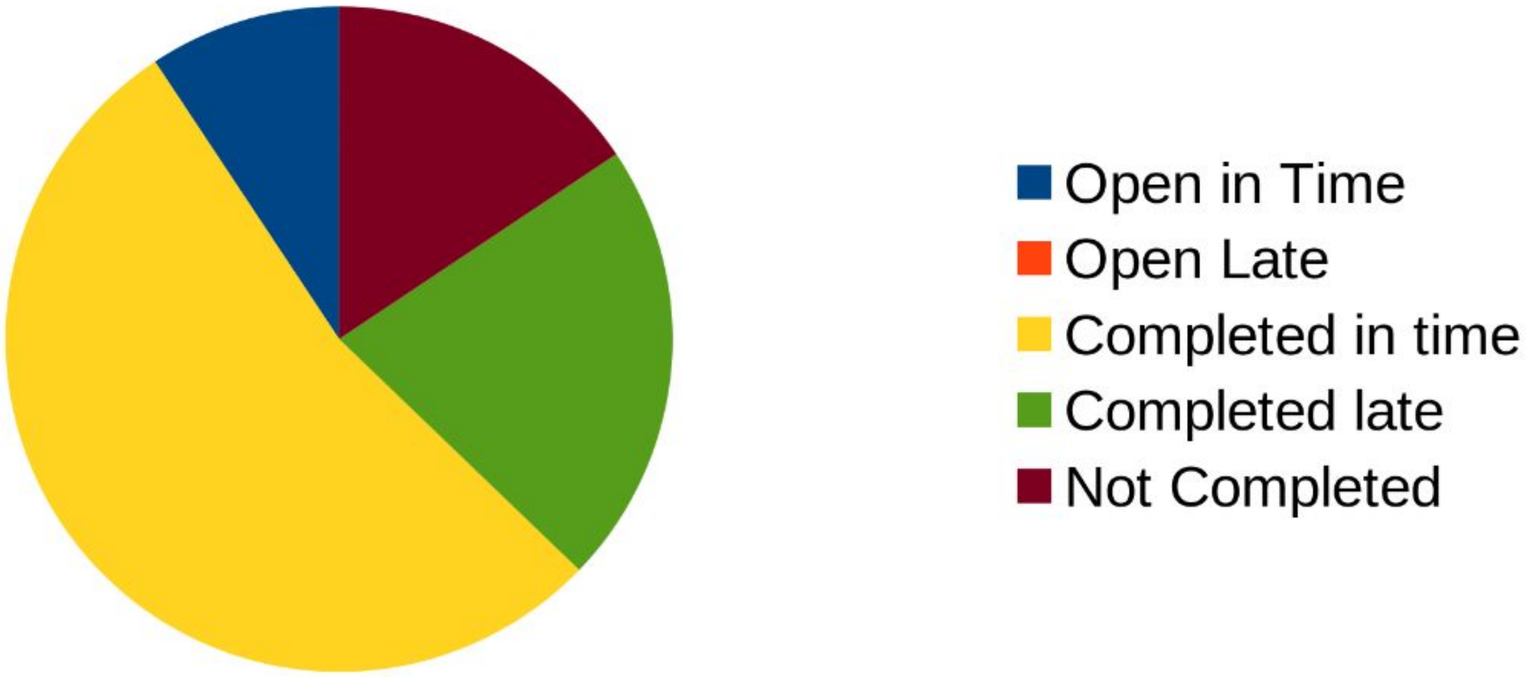
78 - 14 = 64 SecDir reviewers in the pool:
https://datatracker.ietf.org/group/secdir/about/

SecDir meets on Tuesday of IETF

Thank you to Tero Kivinen for managing the reviews!

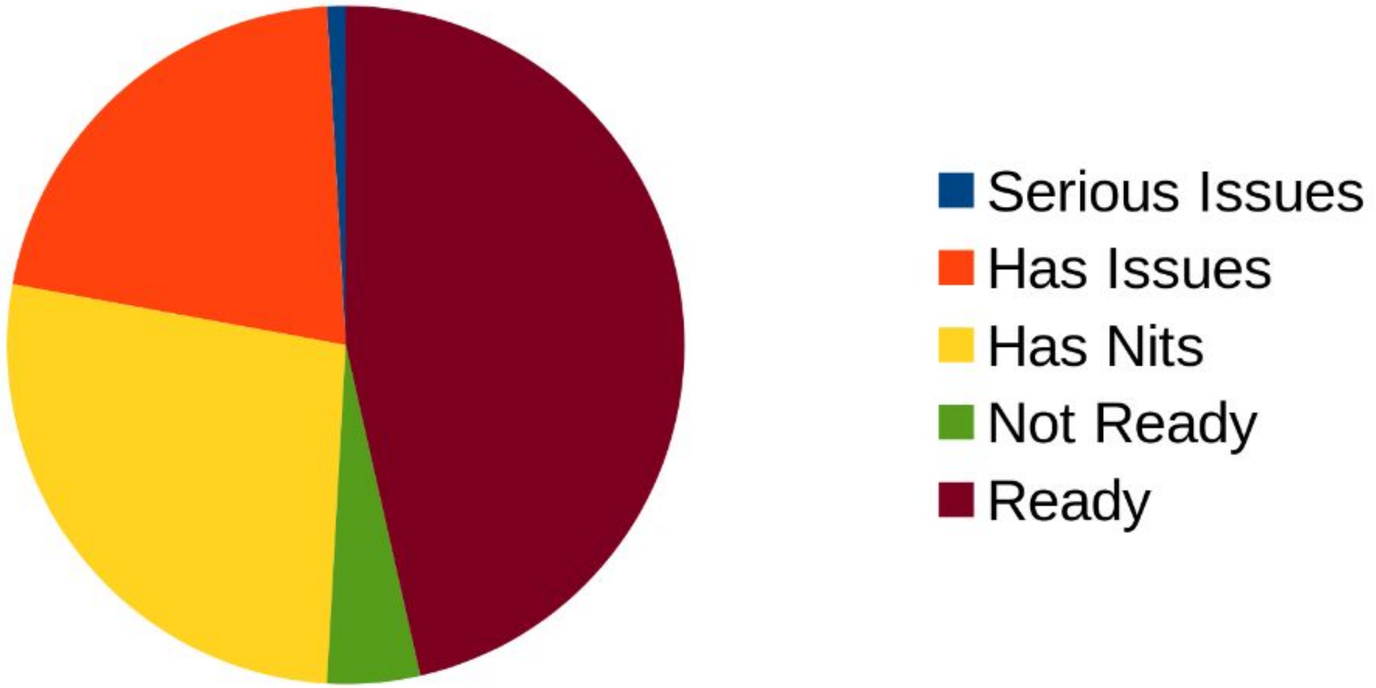
226 SecDir reviews since IETF 120

Team	Open in time	Open late	Completed in time	Completed Late	Not Completed	Avg. Compl. days
SecDir	28	0	161	65	47	11.4
%	9%	0%	53%	22%	16%	



SecDir IETF-121 Outcomes

Team	Serious Issues	Has Issues	Has Nits	Not Ready	Ready
SecDir	2	48	61	10	105
%	1%	21%	27%	4%	46%



Next Generation Internet EU-funding Update (10 min)

Stephen Farrell

draft-pwouters-crypto-current-practices-00

Current practices for new cryptography at the IETF

Abstract

This document describes the current practices for handling new cryptography within the IETF. Some of these practices are informal and depend on individuals in certain relevant roles, such as Working Group Chairs, the Security Area Directors and the Independent Stream Editor. This document is intended to increase consistency and transparency in how the IETF handles new cryptography, such as new algorithms, ciphers and new primitives or combiners, by providing a reference for the cryptographic practices within the IETF. This document does not describe any new policies and does not prohibit exceptions in the described current practices.

Overview of document

A little history

- Not always consistent, decisions made in different contexts

IETF interacts with the wider Cryptographic Community

- Academia, Conferences, Competitions, etc
- CFRG at IRTF, Crypto Panel, Some crypto-heavy WG

Code Points vs RFCs

- Allow Code Points wherever possible - very low bar
  - Experimental or Informational RFCs
- Limit issuing RFCs wherever possible - high bar
  - Due to different interpretation of “RFC” outside the IETF
  - Categorize which kind of drafts should get RFC

Recommended Y / Mandatory-to-Implement

- Require Standards Track RFC

TODO

‘fancy crypto’

- How to handle new crypto constructs, primitives ?
- How to evaluate, eg outside the IETF ?

Any missing topics or issues ?

Please discuss on the list

- Find any mismatch between community and ADs
- Textual improvements

SAAG: Open MIC

See you in Bangkok !