25 July 2025

IETF 123 Security Area Open Meeting (SAAG)

This session is being recorded

Internet Engineering Task Force

Production by Meetecho

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)

Note Really Well

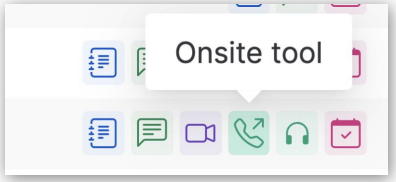
- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, please talk to the Ombudsteam, who are available if you need confidentiality to raise concerns confident about harassment or other conduct in the IETF.
- The IETF strives to create and maintain an environment in which people of many different backgrounds and identities are treated with dignity, decency, and respect. Those who participate in the IETF are expected to behave according to professional standards and demonstrate appropriate workplace behavior.
- IETF participants must not engage in harassment while at IETF meetings, virtual meetings, social events, or on mailing lists. Harassment is unwelcome hostile or intimidating behavior—in particular, speech or behavior that is aggressive or intimidates.
- If you believe you have been harassed, notice that someone else is being harassed, or have any other concerns, you are encouraged to raise your concern in confidence with one of the Ombudspersons.

This session is being recorded

IETF 123 Meeting Tips

In-person participants

- Make sure to sign into the session via Datatracker or the QR Code in this session.
- Use Meetecho (usually the “Meetecho lite”) client to:
  - join the mic queue
  - participate in shows of hands
- *Keep audio and video off if not using the onsite version.*
- *Do not use personal hotspot / mifi devices - it interferes with IETF wifi*



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.

Resources for IETF 123 Madrid

- Agenda
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information:
  https://www.ietf.org/how/meetings/preparation
- If you need technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

Agenda

- Welcome, Administrivia, and Agenda Bashing (5 mins)
- WG and AD Reports (15 mins, chairs/ADs)
- Push And Pull Based Security Event Token Delivery (15 mins)
- RFC 4086 Randomness Requirements for Security (15 mins)
- Open Mic (remaining time)

WG Changes since IETF 122

BOFs	EXPAT (attested TLS) WebBotAuth (in WIT area)
Chartering (charter is at IESG)	
New Working Groups	HPKE
Closed Working Groups	
Rechartered Working Groups	COSE, LAMPS
In Rechartering (charter at WG or IESG)	LAKE

WG Chair changes since IETF 122

WG	Departures	Additions
ACME	Tomofumi Okubo	Mike Ounsworth
HPKE		Martin Thomson, Yaroslav Rosomakho

Helping Out

- If you are interested in becoming a **WG chair**, let your ADs know.
- 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.
- Attend BoFs (virtually or in person)
- Volunteer right now for being minute taker for this meeting :)

IETF

Working Group Summaries

Send highlights and summaries to saag@ietf.org

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

IETF

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 work
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 since IETF 122

List Name	Purpose
PLANT [*]	PKI, Logs, And Tree Signatures
SETTLE (in OPS)	Secure access to TLS local resources

AD sponsored drafts

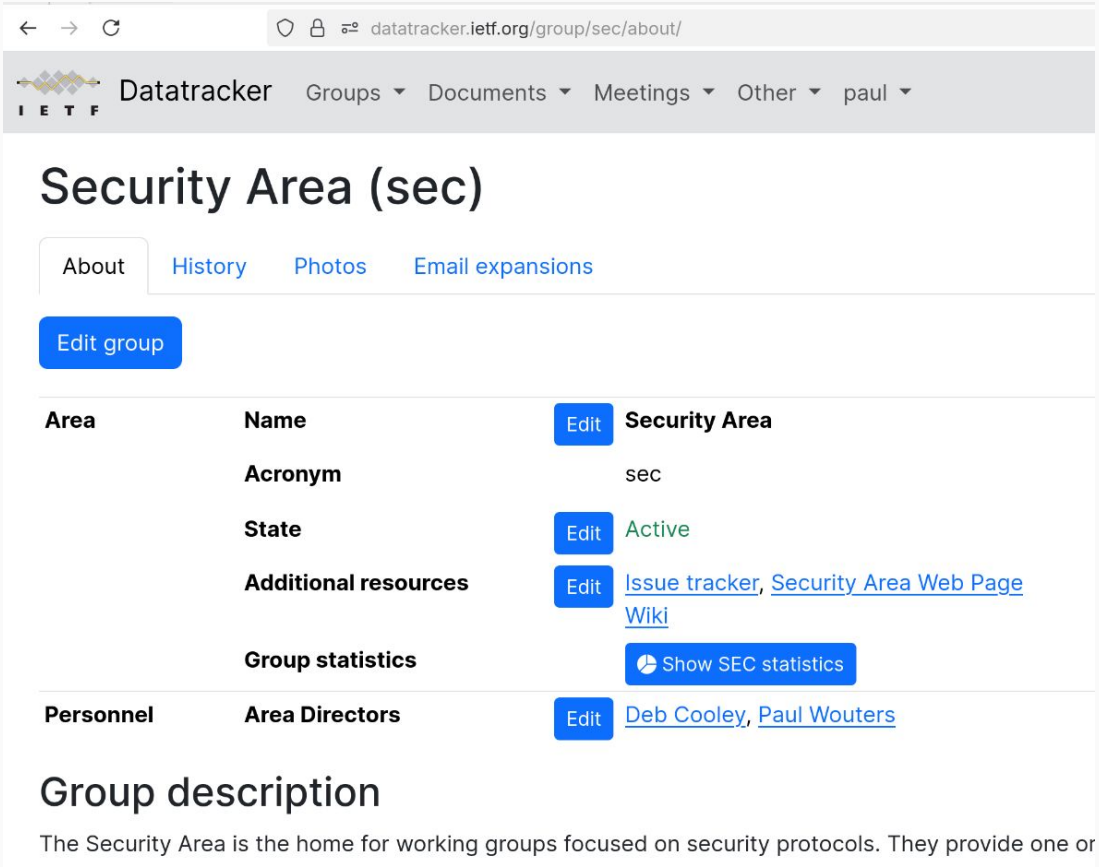
Draft	Sponsoring AD	Status
draft-tulshibagwale-saag-pushpull-delivery	Deb	work in progress

Security related DISPATCH outcomes of IETF 122

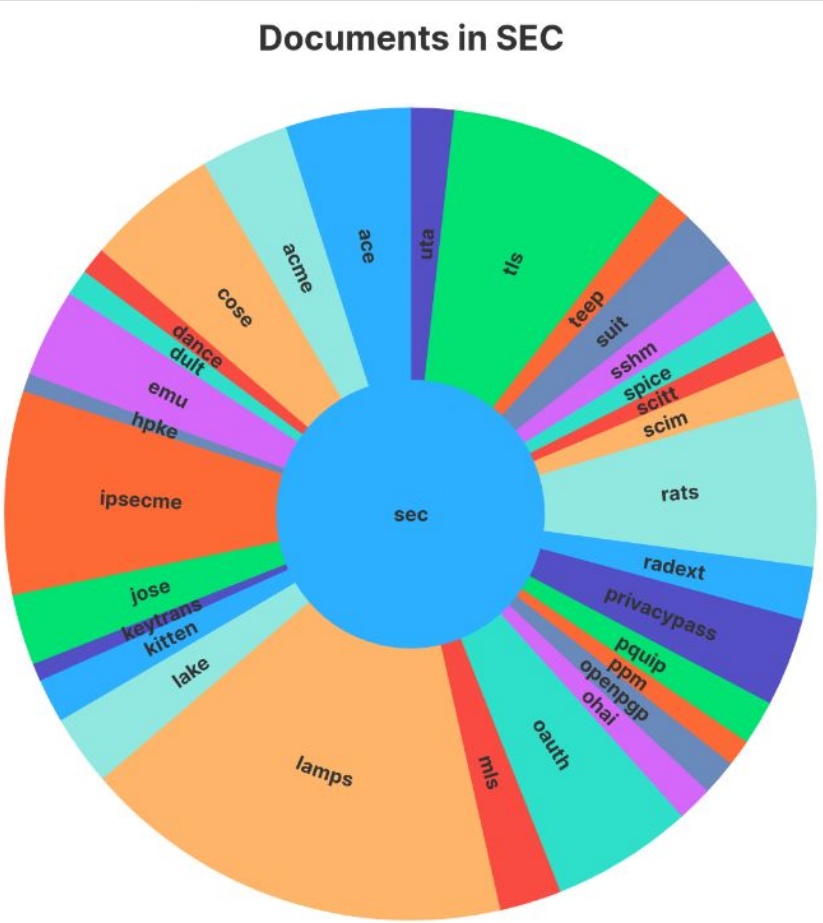
Draft	Outcome
Merkle Tree Certificates draft-davidben-tls-merkle-tree-certs	Mailing list (plant@ietf.org [*]), maybe BoF?
PSI based on ECDH draft-wang-ppm-ecdh-psi	unclear / offline discussion
Unobtrusive End-to-End Email Signatures draft-gallagher-email-unobtrusive-signatures	MAILMAINT or a side meeting
JSContact/EARL Peer-to-Peer Security Scheme	CALEXT WG for the JSContact and JOSE or a BoF for the crypto part

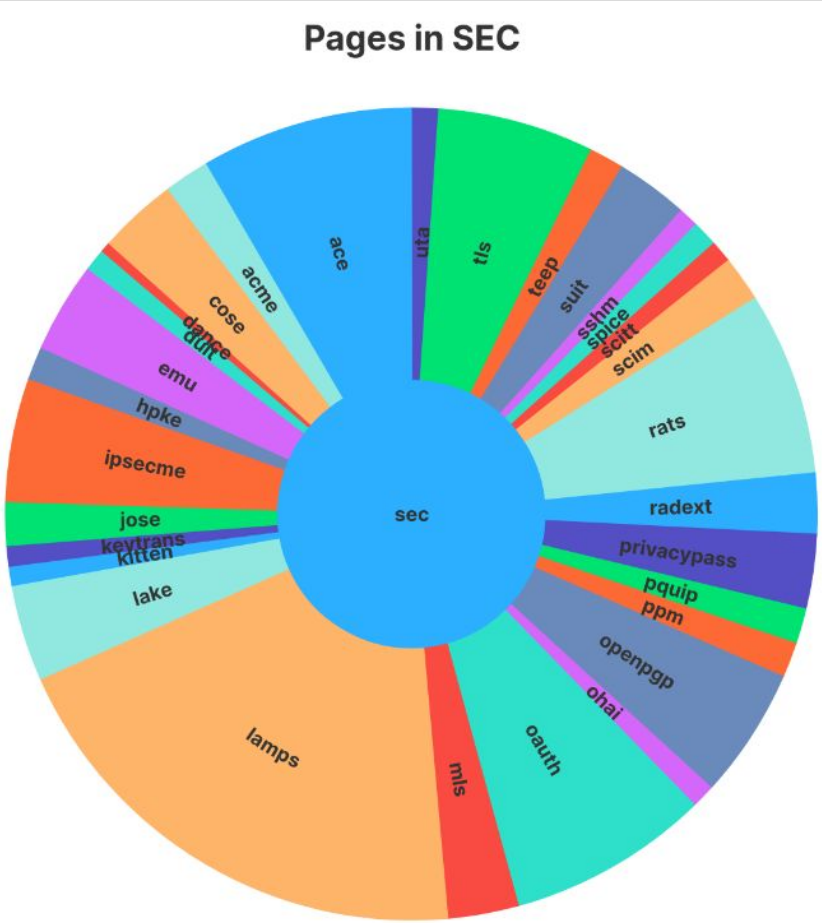
IETF

New datatracker WG page statistics



New datatracker WG page statistics (285 documents with 9554 pages)





Errata processing

	Total Open SEC Errata (non-editorial)	**Since last meeting**	
		Closed	**Reported**
IETF 123	**218** (of a total of 599)	21	34
IETF 122	205	n/a	n/a
IETF 121	250	23	18
IETF 120	257	50	27
IETF 119	279	33	17
IETF 118	295	16	15
IETF 117	296	0	8
IETF 116	288	3	16

IETF

Security 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/

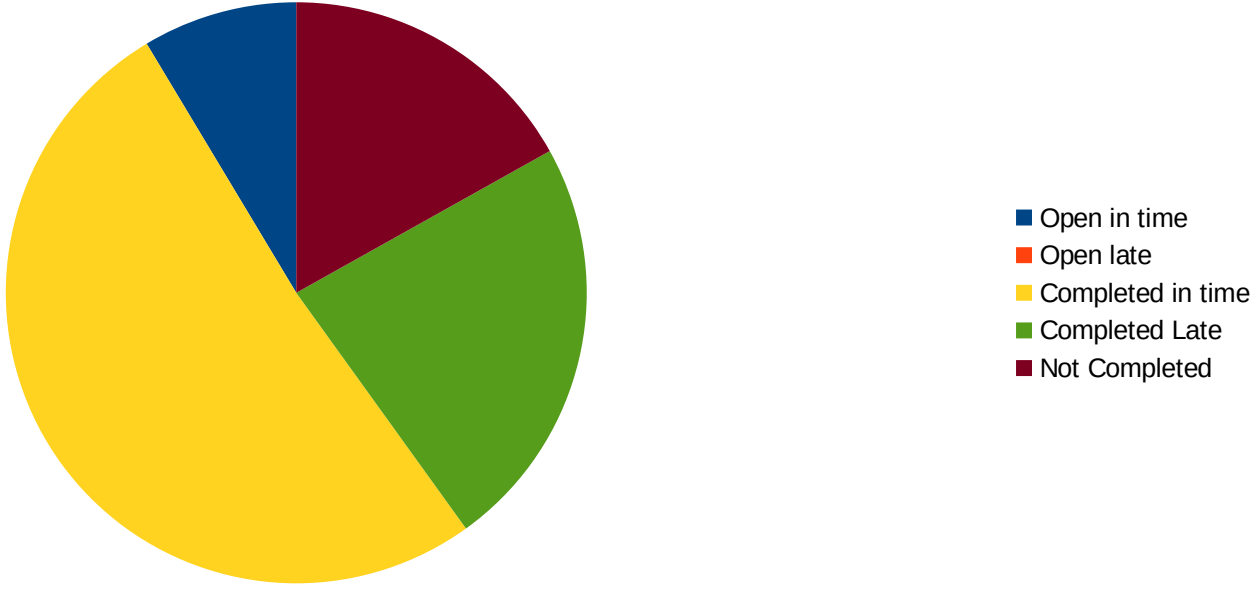
IETF

Thanks to all SECDIR reviews !

- The Security Directorate attempts to (security) review all drafts
- Thanks to Tero Kivinen for managing the SECDIR Directorate
  - https://datatracker.ietf.org/group/secdir/about/
- SecDir meets on Tuesday of each IETF during lunch time
  - Free Lunch provided!
- Membership is SEC area Working Group chairs and willing alumni

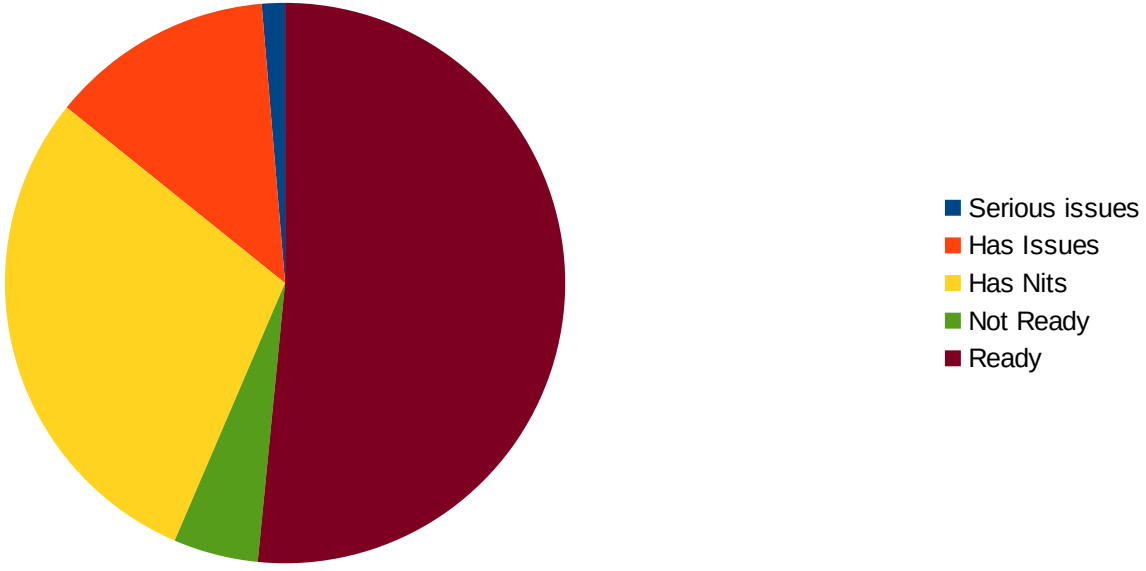
Completed reviews 2024-07 - 2025-07

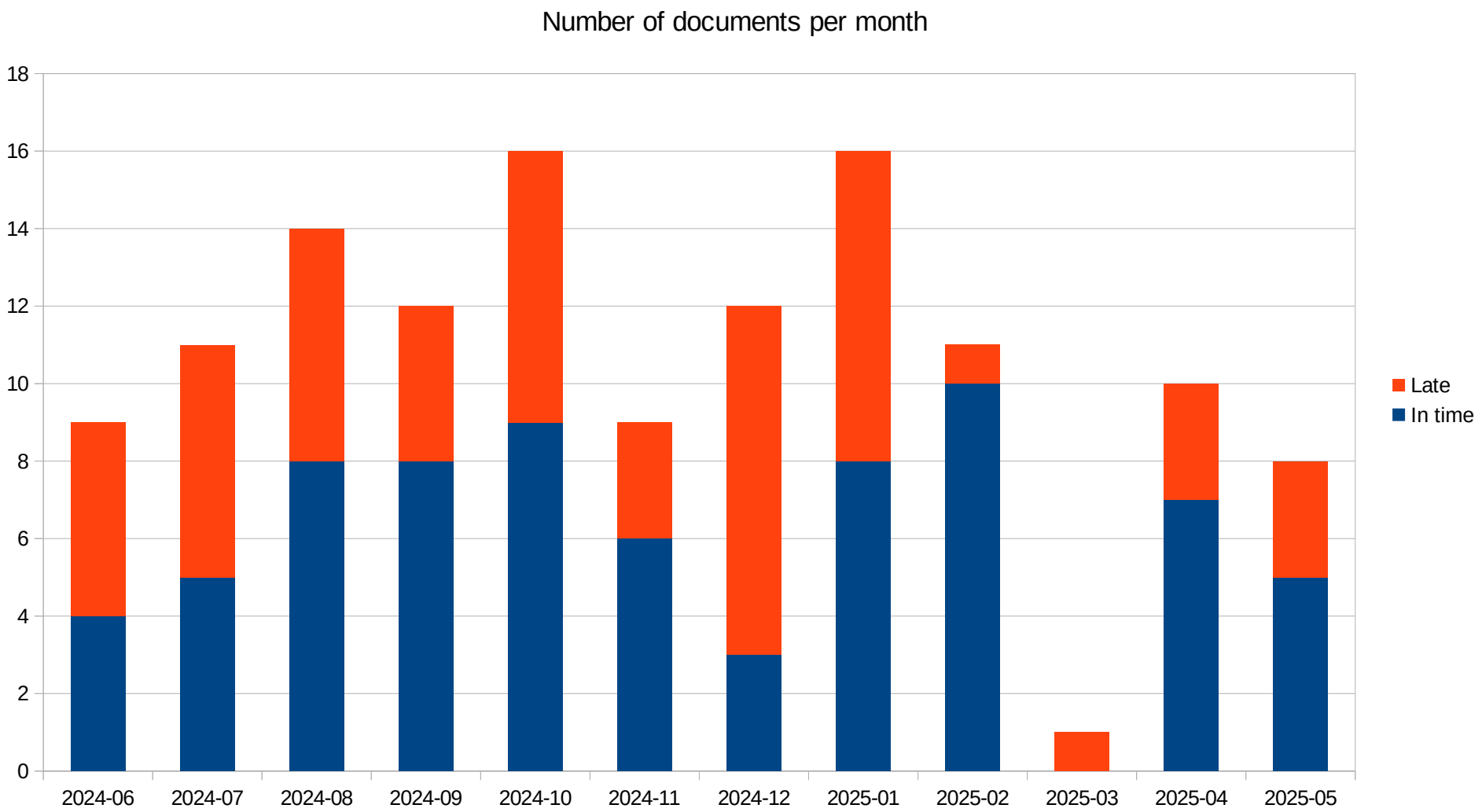
Team	Open in time	Open late	Completed in time	Completed Late	Not Completed	Avg. Compl. days
SecDir	26	0	155	70	51	11.5
%	9%	0%	51%	23%	17%	



Results of reviews 2024-07 - 2025-07

Team	Serious Issues	Has Issues	Has Nits	Not Ready	Ready
SecDir	3	29	66	11	116
%	1%	13%	29%	5%	52%




Number of documents per month
18
16
14
12
10
8
6
4
2
0
2024-06
2024-07
2024-08
2024-09
2024-10
2024-11
2024-12
2025-01
2025-02
2025-03
2025-04
2025-05
Late
In time

Push And Pull Based Security Event Token (SET) Delivery

- draft-tulshibagwale-saag-pushpull-delivery presentation

“Pushpull” delivery of SETs

Atul Tulshibagwale
LinkedIn, GitHub: @tulshi

SGNL

Aaron Parecki
LinkedIn: @aaronparecki
GitHub: @aaronpk

Okta

Apoorva Deshpande
LinkedIn, GitHub: @appsdesh

Okta

Background

The secevent WG was active from Sep 2016 through June 2023

RFC 9493	**Subject Identifiers for Security Event Tokens**	18 pages Errata	2023-12
RFC 8935	**Push-Based Security Event Token (SET) Delivery Using HTTP**	15 pages	2020-11
RFC 8936	**Poll-Based Security Event Token (SET) Delivery Using HTTP**	16 pages	2020-11
RFC 8417	**Security Event Token (SET)**	28 pages Errata	2018-07

Push Delivery (RFC 8935)

Sender delivers a single event

```
POST /Events HTTP/1.1
Host: notify.rp.example.com
Accept: application/json
Content-Type: application/secevent+jwt

eyJ0eXAiOiJzZWNldmVudCtqd3QiLCJhbGciOiJIUzI1NiJ9Cg.
eyJpc3MiOiJodHRwczovL2lkcC5leGFtcGxlLmNvbS8iLCJqdGkiOiI3NTZFNjk
3MTc1NjUyMDY5NjQ2NTZFNzQ2OTY2Njk2NTcyIiwiaWF0IjoxNTA4MTg0ODQ1LC
JhdWQiOiI2MzZDNjk2NTZFNzQ1RjY5NjQiLCJldmVudHMiOnsiaHR0cHM6Ly9zY
2hlbWFzLm9wZW5pZC5uZXQvc2VjZXZlbnQvcmlzYy9ldmVudC10eXBlL2FjY291
bnQtZGlzYWJsZWQiOnsic3ViamVjdCI6eyJzdWJqZWN0X3R5cGUiOiJpc3Mtc3V
iIiwiaXNzIjoiaHR0cHM6Ly9pZHAuZXhhbXBsZS5jb20vIiwic3ViIjoiNzM3NT
YyNkE2NTYzNzQifSwicmVhc29uIjoiaGlqYWNraW5nIn19fQ.
Y4rXxMD406P2edv00cr9Wf3_XwNtLjB9n-jTqN1_lLc
```

Poll Delivery (RFC 8936)

```
POST /Events HTTP/1.1
Host: notify.idp.example.com
Content-Type: application/json

{
   "returnImmediately": true,
   "ack": ["3d0c3cf797584bd193bd0fb1bd4e7d30"]
}
```

Receiver asks for events and acknowledges previously received event

```
HTTP/1.1 200 OK
Content-Type: application/json

{
 "sets":
  {
   "eyJqdGkiOiI0ZDM1NTllYzY3NTA0YWFiYTY1ZDQwYjAzNjNmYWFkOCIsImlhdC
    L3NjaW0uZXhhbXBsZS5jb20vVXNlcnMvNDRmNjE0MmRmOTZiZDZhYjYxZTc1Mj
    FkOSIsImF0dHJpYnV0ZXMiOlsiaWQiLCJuYW1lIiwidXNlck5hbWUiLCJwYXN",
   "eyJqdGkiOiIzZDBjM2NmNzk3NTg0YmQxOTNiZDBmYjFiZDRlN2QzMCIsImlhdC
    I6MTQ1ODQ5NjAyNSwiaXNzIjoiaHR0cHM6Ly9zY2ltLmV4YW1wbGUuY29tIiwi
    dvcmRSZXNldCI6eyJpZCI6IjQ0ZjYxNDJkZjk2YmQ2YWI2MWU3NTIxZDkifSwi
    aHR0cHM6Ly9leGFtcGxlLmNvbS9zY2ltL2V2ZW50L3Bhc3N3b3JkUmVzZXRFeH
    QiOnsicmVzZXRBdHRlbXB0cyI6NX19fQ."
  }
}
```

Sender delivers new event in HTTP response

Pushpull Delivery: Communication Object

- Common JSON object that contains (all optional):
  - Multiple SETs to transfer to the recipient
  - An array of previous SETs to be acknowledged
  - Multiple error objects

- Similar to a HTTP Response in “Delivery Poll” (RFC8936)

```
{
  "sets": {
    "4d3559ec67504aaba65d40b0363faad8":
          "eyJ … d29yZCYWlscyJdfX19.",
    "3d0c3cf797584bd193bd0fb1bd4e7d30":
          "eyJ … QiOnsicmVzZXRBdl."
  },
  "ack": [
    "f52901c4-3996-11ef-9454-0242ac120002",
    "0636e274-3987-a1c3-3149-0215ac132142",
    "d563c724-79a0-4ff0-ba41-657fa5e2cb11"
  ],
  "setErrs": {
    "5c436b19-0958-4367-b408-2dd542606d3b" : {
      "err": "invalid subject",
      "description": "subject format not
supported"
    }
  }
}
```

Pushpull Delivery: Transport options

- Always a Communication Object
- HTTP Request Response binding
  - Requests can have an additional “maxResponseEvents” field
- WebSocket binding
  - WebSocket Subprotocol: `pushpull`
  - Communication Object is the Payload data
- Any initiator can request upgrade to WebSocket, and they must use WebSocket if handshake succeeds

Developments since IETF 122

- Combined “Pushpull” with “Multi-SET Push Delivery” - new draft is still called “Pushpull”
- Feedback received on:
  - Multi-SET Push
  - Pushpull
- Feedback response provided

Feedback Points

- Multi-SET Push
  - “Incremental work without significant engineering advantages”
  - Creates interoperability disadvantage

- Pushpull
  - Idea is not new. Another proposal here: “Symmetric SET Transfer Protocol” (expired 2018)
    - Some differences, but largely the same
  - Incremental work without significant engineering advantages
  - Creates interoperability disadvantage

Feedback response

- SSTP - merge authors
  - Pushpull seems to be a superset of SSTP

- “Incremental work” response:
  - No async acknowledgement of pushed events
  - No way to detect “zombie streams”
  - Efficiency improvement

- Interoperability disadvantage
  - Nascent adoption of these specs at this time - SSF is the biggest adopter

Efficiency improvement requirement

- Requirement: Implement cloud ITDR
  - Send CAEP “session established” and “session presented” events periodically for each active user.
  - Millions of active users at each app, tens of apps, assume period is 1 minute.
  - Push is convenient for lightweight Transmitters - no HTTP server required.
  - Single push per connection would be too expensive

- Single bidirectional stream instead of two unidirectional streams reduces overhead, simplifies architecture.

- Vision: SSF becomes the HTTP of asynchronous communication

RFC 4086 - Randomness Requirements for Security

- Published in 2005
- Information is very outdated
  - Predates Operating Systems providing mostly only secure random
  - Predates improved application libraries providing secure random
- We want drafts to reference something in Security Considerations
  - But not RFC 4086
  - An existing Standards document ? NIST SP 800-90 ?
- Update with a bis document ?
  - with inline content?
  - with mostly normative references to non-ietf documenst?
- Do not update, but make RFC 4086 Historic ?

IETF

Any other Business / Open Mic

IETF

The end: Safe travels home