

Security Area Advisory Group

CodiMD for notes: <https://codimd.ietf.org/notes-ietf-112-saag>

Meetecho link:

<https://meetings.conf.meetecho.com/ietf112/?group=saag&short=&item=1>

Benjamin Kaduk

Roman Danyliw

IETF 112 -- Session III

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

Agenda

Tuesday, Session I

1. Welcome, Administrivia, and Agenda Bashing (5 mins)
2. Update on NIST PQC Project (45 min, Dustin Moody)
3. Open Mic (remaining time)

Thursday, Session III

4. Welcome, Administrivia, and Agenda Bashing (5 mins)
5. WG Reports (10 mins)
6. AD Report (5 mins)
7. "Recommended" guidance for TLS for other WG (20 min, TLS WG)
8. Open Mic (remaining time)

Working Group Summaries

ACE

Chairs

- Daniel Migault
- Loganaden Velvindron

Report

<https://mailarchive.ietf.org/arch/msg/saag/l6eQgA8CSpxeISBSw5JXZ8-wH8w/>

ACME

Chairs

- Deb Cooley
- Yoav Nir

Report

<https://mailarchive.ietf.org/arch/msg/saag/vmBHY18oGfP-4onfA4f17ApBIIU/>

COSE

Chairs

- Matthew Miller
- Ivaylo Petrov
- Mike Jones

Report

XXX

GNAP

Chairs

- Leif Johansson
- Yaron Sheffer

Report

<https://mailarchive.ietf.org/arch/msg/saag/C8m-v8qIP0bDCgc6SRZE6CRHTFc/>

IPSECME

Chairs

- Tero Kivinen
- Yoav Nir

Report

https://mailarchive.ietf.org/arch/msg/saag/P8MR9_T8666PZBCNaa7WBkhCPFg/

LAMPS

Chairs

- Russ Housley
- Tim Hollebeek

Report

<https://mailarchive.ietf.org/arch/msg/saag/dvaepQD5VYjJbz86SNhHrxulrYA/>

OHAI

Chairs

- Richard Barnes
- Shivan Sahib

Report

XXX

OPENPGP

Chairs

- Daniel Gillmor
- Stephen Farrell

Report

https://mailarchive.ietf.org/arch/msg/saag/Swr_3nUY6vJILMrrBSxybAWgekA/

RATS

Chairs

- Nancy Cam-Winget
- Ned Smith
- Kathleen Moriarty

Report

https://mailarchive.ietf.org/arch/msg/saag/3Gn_AsYvMc7D7zHmDRfYkpjaJVA/

SACM

Chairs

- Chris Inacio
- Karen O'Donoghue

Report

<https://mailarchive.ietf.org/arch/msg/saag/EqffAA7JTRPEeKMthOPRqABUI6s/>

SecDispatch

Chairs

- Richard Barnes
- Kathleen Moriarty
- Mohit Sethi

Report

https://mailarchive.ietf.org/arch/msg/saag/W8UZxFOYw3Gmo6jral7igta_Yts/

SUIT

Chairs

- Russ Housley
- Dave Thaler
- David Waltermire

Report

<https://mailarchive.ietf.org/arch/msg/saag/s6dyxxpjYpWzvv8sDyAyJbeyEUY/>

TLS

Chairs

- Joe Salowey
- Sean Turner
- Chris Wood

Report

https://mailarchive.ietf.org/arch/msg/saag/4_nnPazSHC4Wcvi8tAzT6RR-a78/

WGs meeting later in the week

- DANCE
- LAKE (https://mailarchive.ietf.org/arch/msg/saag/Jl98rI071VEaUmDulsUkWwu_uPc/)
- RATS (second session)
- TEEP (<https://mailarchive.ietf.org/arch/msg/saag/F7bnRATHMXltN68G14cnG0JimgA/>)

WGs not meeting at IETF 112 (1)

- **CURDLE** (<https://mailarchive.ietf.org/arch/msg/saag/aisSjyR5QVkmMYM-5Ex5bV22v4w8/>)
- **DOTS** (https://mailarchive.ietf.org/arch/msg/saag/f0sYjSfbtsNDK0Wnglab-Wsl_U/)
- **EMU**
- **I2NSF**
- **KITTEN**
- **MLS**
- **OAUTH**
- **PRIVACYPASS**

WGs not meeting at IETF 112 (2)

- SECEVENT

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

BoFs

- PRIV

Security Related IRTF

- CFRG
- PEARG

IAB Programs

- model-t

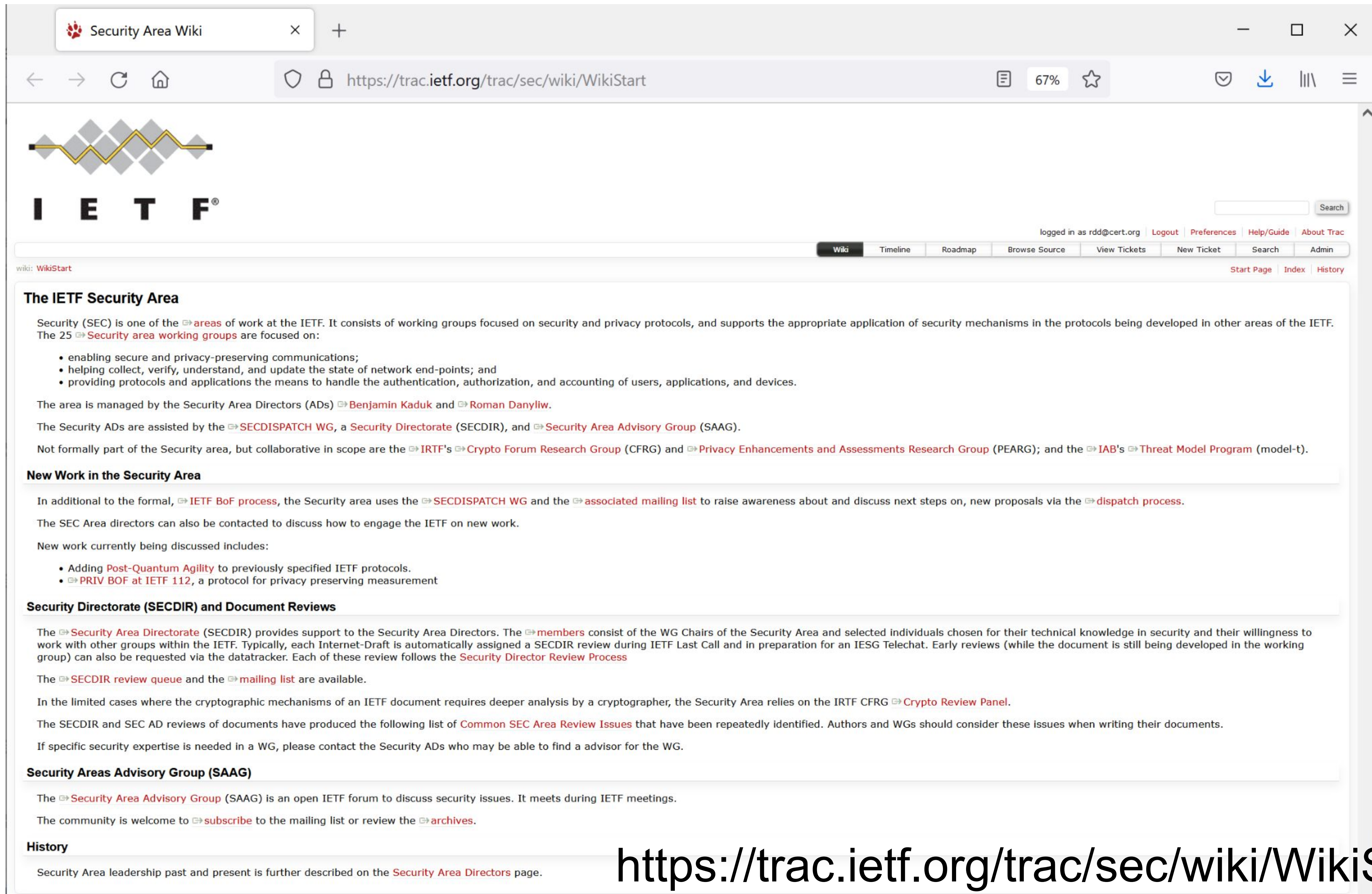
External related

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

AD Sponsored Drafts

Draft	Sponsor	Status
draft-foudil-securitytxt	Ben	RFC Editor
draft-gont-numeric-ids-sec-considerations	Ben	IESG::Waiting for Writeup
draft-housley-ers-asn1-modules	Roman	RFC Editor
draft-eastlake-rfc6931bis-xmlsec-uris	Roman	AD Review:: Revised I-D Needed

SEC Area Highlights



The screenshot shows a web browser window displaying the IETF Security Area Wiki page. The browser's address bar shows the URL <https://trac.ietf.org/trac/sec/wiki/WikiStart>. The page features the IETF logo at the top left and a search bar at the top right. The main content is organized into several sections:

- The IETF Security Area**: A paragraph explaining the scope of the Security Area and listing 25 working groups. A bulleted list includes: enabling secure and privacy-preserving communications; helping collect, verify, understand, and update the state of network end-points; and providing protocols and applications for authentication, authorization, and accounting.
- New Work in the Security Area**: A paragraph describing the IETF BoF process and the SECDISPATCH WG, followed by a bulleted list of current work items like Post-Quantum Agility and PRIV BOF at IETF 112.
- Security Directorate (SECDIR) and Document Reviews**: A paragraph detailing the SECDIR's role in reviewing Internet-Drafts and providing a review queue and mailing list.
- Security Areas Advisory Group (SAAG)**: A paragraph describing the SAAG as an open forum for discussing security issues.
- History**: A short paragraph mentioning the Security Area Directors page.

The URL <https://trac.ietf.org/trac/sec/wiki/WikiStart> is also displayed in large text at the bottom right of the screenshot.

SEC Area Highlights (2)

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/benjamin.kaduk>

Continued discussion about PQ agility

- Summary -- <https://trac.ietf.org/trac/sec/wiki/PQCAgility>
- SAAG ML --

<https://mailarchive.ietf.org/arch/msg/saag/5uV72m80X9PTGFWFyDY5VrNyK-c/>

WG Changes

New	DANCE OHAI SCIM*
Closed	TRANS
Rechartered	
Rechartering	SUIT

* re-opened; decided to stay in ART

Thanks to the SECDIR Reviewers since IETF 110

- Adam Montville
- Alan DeKok
- Alexey Melnikov
- Barry Leiba
- Catherine Meadows
- Charlie Kaufman
- Chris Lonvick
- Christian Huitema
- Christopher Wood
- Dan Harkins
- Daniel Migault
- David Mandelberg
- Derek Atkins

- Derrell Piper
- Donald Eastlake
- Joseph Salowey
- Kyle Rose
- Linda Dunbar
- Melinda Shore
- Nancy Cam-Winget
- Paul Wouters
- Robert Sparks
- Russ Housley
- Samuel Weiler
- Sean Turner
- Shawn Emery

- Steve Hanna
- Tero Kivinen
- Valery Smyslov
- Yaron Sheffer
- Yoav Nir

**"Recommended" guidance
for TLS for other WG**

Open Mic