

Security Area Advisory Group

Benjamin Kaduk

Roman Danyliw

IETF 104

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)

Agenda

1. WG/BoF Reports and Administrivia (10 mins)
2. Invited/Offered Talks
 1. Misbinding in Pairing Protocols (20 min)
Tuomas Aura
 2. SNOW-V Stream Cipher (10 min)
John Mattsson
3. Open Mic (remainder)

Working Group Summaries

ACE

Chairs

- Daniel Migault
- Jim Schaad

Report

<https://mailarchive.ietf.org/arch/msg/saag/Mn4OqigHZmd98VlPhzeanUdvKMM>

ACME

Chairs

- Rich Salz
- Yoav Nir

Report

<https://mailarchive.ietf.org/arch/msg/saag/mUt2w56ZZvw4FWbpL8j8LmJKIzE>

COSE

Chairs

- Matthew Miller
- Ivaylo Petrov

Report

<https://mailarchive.ietf.org/arch/msg/saag/EP4Yde6fyhPTBcAP6p3j6QBP-HQ>

CURDLE

Chairs

- Daniel Migault
- Rich Salz

Report

Did not meet

<https://mailarchive.ietf.org/arch/msg/saag/zbPft4sOuCvuiGW1P0X5NO2s5S4>

DOTS

Chairs

- Valery Smyslov
- Liang Xia (Frank)

Report

<https://mailarchive.ietf.org/arch/msg/saag/n--vf46xXOL69d167S2HLXwLROs>

EMU

Chairs

- Joe Salowey
- Mohit Sethi

Report

https://mailarchive.ietf.org/arch/msg/saag/S9cxAzMNSm_vMllimzRiQ1xIHh8

I2NSF

Chairs

- Linda Dunbar
- Yoav Nir

Report

https://mailarchive.ietf.org/arch/msg/saag/eDIHWPMbv3xyx67K9_hwjalbdSs

IPSECME

Chairs

- Tivo Kevinen
- David Waltermire

Report

<https://mailarchive.ietf.org/arch/msg/saag/0NCwjDA56EBVc9JDyBg-nda6pDg>

KITTEN

Chairs

- Matt Miller
- Robbie Harwood
- Roland Dowdeswell

Report

Not meeting

<https://mailarchive.ietf.org/arch/msg/saag/9tV5gdaNmycyVBdK0hUQydgraoo>

LAMPS

Chairs

- Russ Housley
- Tim Hollebeek

Report

<https://mailarchive.ietf.org/arch/msg/saag/MgBzmAB4swuR7rFbihCdClh3IX4>

MILE

Chairs

- Nancy Cam-Winget
- Takeshi Takahashi

Report

<https://mailarchive.ietf.org/arch/msg/saag/s468uFCCTNNTpyGpLqaJj-Br3H8>

MLS

Chairs

- Nick Sullivan
- Sean Turner

Report

<https://mailarchive.ietf.org/arch/msg/saag/svqygnsxMTyCoYVtr46AcKSbdAk>

OAUTH

Chairs

- Hannes Tschofenig
- Rifaat Shekh-Yusef

Report

RATS

Chairs

- Nancy Cam-Winget
- Ned Smith
- Kathleen Moriarty

Report

https://mailarchive.ietf.org/arch/msg/saag/6_DM6ipdsFrcH64wcl86_09E4F0

SACM

Chairs

- Chris Inacio
- Karen O' Donoghue

Report

<https://mailarchive.ietf.org/arch/msg/saag/8c-kV4EwqNETZs93m9CLrQ3O1o4>

SecDispatch

Chairs

- Richard Barnes
- Kathleen Moriarty

Report

<https://mailarchive.ietf.org/arch/msg/saag/v6Qlgdtcoylgl58eSCVB8d3fxMo>

SecEvent

Chairs

- Dick Hardt
- Yaron Sheffer

Report

https://mailarchive.ietf.org/arch/msg/saag/O0s_iUy9ufOcZPJMcf3wpr33fs

SUIT

Chairs

- Russ Housley
- Dave Thaler
- David Waltermire

Report

<https://mailarchive.ietf.org/arch/msg/saag/QDfTMPiDEkJ71g8RtFDnaiMP28s>

TEEP

Chairs

- Nancy Cam-Winget
- Dave Thaler

Report

<https://mailarchive.ietf.org/arch/msg/saag/idYNaxXXtQ4VH6W4hfd40VNsxqQ>

TLS

Chairs

- Joe Salowey
- Sean Turner
- Chris Wood

Report

https://mailarchive.ietf.org/arch/msg/saag/G6TBolKCYHs7OXowTGE0TMSG_yU

TOKBIND

Chairs

- John Bradley
- Leif Johansson

Report

Not meeting

https://mailarchive.ietf.org/arch/msg/saag/DVF4XO3d96viGE2-jvfY5C_YJTw

TRANS

Chairs

- Melinda Shore
- Paul Wouters

Report

Not meeting

Related Non-SEC Area WGs

Security Topics in Related WGs

- ANIMA
- DIME
- DISPATCH
- DMARC
- DPRIVE
- HTTPBIS
- QUIC
- NETCONF
- NTP
- PERC
- RADext
- SIDROPS
- TCPINC
- UTA

Security Related IRTF

- CFRG
- IRTFOpen
- PEARG

IAB Programs

- PrivSec
- SMART

External related

- W3C

—

BoF Summaries

CACAO

Chairs

- Chris Inacio
- Joe Salowey

Report

<https://mailarchive.ietf.org/arch/msg/saag/KAyD-wHw1pzRcxeb57PSjOLm-PM>

New Split of WGs across ADs

Ben

- ACE
- COSE
- CURDLE
- DOTS
- IPSECME
- KITTEN
- MLS
- SECEVENTS
- TEEP
- TLS

Roman

- ACME
- EMU
- I2NSF
- LAMPS
- OAUTH
- RATS
- SACM
- SECDISPATCH
- SUIT
- TOKBIND
- TRANS

Invited/Offered Talks

1. Misbinding in Pairing Protocols (20 min)
Tuomas Aura
2. SNOW-V Stream Cipher (10 min)
John Mattsson

Open Mic