

Security Dispatch WG (SecDispatch)

Tuesday, November 6, 2018

IETF 103, Bangkok

Richard Barnes and Roman Danyliw

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)

Administrative Tasks

- Blue sheets
- Jabber scribes
- Note takers

Dispatch Process

Ground Rules

- SecDispatch recommends next steps for new work
- SecDispatch DOES NOT adopt drafts

Possible Outcomes

- Direction to an existing WG
- Propose a new, focused WG
- AD-sponsorship (assuming AD is willing)
- IETF should not work on this topic

Agenda

1. Logistics and introduction (chairs, 5 min)

2. Dispatch items (Each item is 10-15 minutes)

(2.1) Certificate Limitation Policy (Dmitry Belyavsky)

draft-belyavskiy-certificate-limitation-policy-06

(2.2) Algorithm Identifiers for HSS and XMSS for Use in the Internet X.509 Public Key Infrastructure (Daniel Van Geest)

draft-vangeest-x509-hash-sigs-01

(2.3) General Security Considerations for Crypto Assets Custodians
(Hirotaka Nakajima)

draft-vcgtf-crypto-assets-security-considerations-02

(2.4) Nimble out-of-band authentication for EAP (EAP-NOOB) (Tuomas Aura)

draft-aura-eap-noob-04

(2.5) Extended Security Considerations for the Automatic Certificate Management Environment (ESecACME) (Tobias Fiebig)

draft-fiebig-acme-esecacme-00

3. Closing (chairs, 5 min)