

pq-dnssec side meeting at IETF 121

Welcome

- Chairs:
 - Caspar Schutijser <caspar.schutijser@sidn.nl>
 - Peter Thomassen <peter@desec.io>
- Note taker?
- Why are we here?

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 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)

IETF Code of Conduct Guidelines RFC7154

1. Treat colleagues with respect
2. Speak slowly and limit the use of slang
3. Dispute ideas by using reasoned argument
4. Use best engineering judgment
5. Find the best solution for the whole Internet
6. Contribute to the ongoing work of the group and the IETF

We take this very seriously. If you feel the Code has been violated,
please reach out to the chairs or the IETF ombuds team.

"We work as Individuals, let's remember to be nice to each other"

Agenda

- **15'+q** Joe Harvey (Verisign): PQ DNSSEC with MTL Mode
- **15'+q** Jason Goertzen (SandboxAQ): Field study on mitigating the costs of Post-Quantum DNSSEC with Merkle Trees
- **20'+q** Ralph Koning (SIDN Labs): A testbed to evaluate post-quantum cryptography in DNSSEC
- Open Discussion / AOB

Discussion

- Are you planning to bring your work to this group?
- Who else is working on PQ DNSSEC?
- Where do we want to stand in a year from now?
- What can the chairs do to facilitate that?
 - For example, organize meetings or workshops (here or elsewhere)?