Secure Shell Maintenance (SSHM)

Chairs:
Job Snijders *job@bsd.nl*
Stephen Farrell *stephen.farrell@cs.tcd.ie*

IETF 124, Montreal, Canada

Agenda

- Scan bluesheet QR code!
- Resources
- Note Well
- Discussion on SSH-related Internet-Drafts

Resources

- mailarchive.ietf.org/arch/browse/ssh/
- zulip.ietf.org/#narrow/channel/401-sshm/topic/ietf-124

Note Well (1/2)

By participating in the IETF you agree to follow IETF processes and policies. This Note Well is a reminder of some of those policies.

- IETF participants are expected to behave in a professional manner and extend respect and courtesy to their colleagues at all times (see RFC 7154: IETF Guidelines for Conduct and IETF Anti-Harassment Policy). If you have any concerns about behavior, please contact the Ombudsteam who have a duty of confidentiality and extensive powers to act, as set out in RFC 7776: IETF Anti-Harassment Procedures.
- If you are aware that any IETF contribution (as defined in RFC 5378: Rights Contributors Provide to the IETF Trust) is covered by patents or patent applications that are owned or controlled by you, your employer or your sponsor, you must disclose that fact, or not participate in the discussion (see RFC 8179: Intellectual Property Rights in IETF Technology).

Note Well (2/2)

By participating in the IETF you agree to follow IETF processes and policies. This Note Well is a reminder of some of those policies.

- For detailed process information consult RFC 2026: Internet Standards Process and RFC 2418: IETF Working Group Guidelines and Procedures and updates to those.
- The IETF routinely makes public written, audio, video, and photographic records of IETF activities, including your personal information as set out in the IETF Privacy Statement.

For advice, please talk to Working Group chairs or Area Directors.

Welcome to Montreal!

Active with the IESG Internet-Drafts

- draft-ietf-sshm-ssh-agent-10
  SSH Agent Protocol
- draft-ietf-sshm-ntruprime-ssh-06
  Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512

Active Internet-Drafts

- draft-ietf-sshm-mlkem-hybrid-kex-03
  PQ/T Hybrid Key Exchange with ML-KEM in SSH
- draft-ietf-sshm-chacha20-poly1305-02
  Secure Shell (SSH) authenticated encryption cipher: chacha20-poly1305
- draft-ietf-sshm-strict-kex-00
  SSH Strict KEX extension

Related Internet-Drafts (1/3)

- draft-miller-sshm-hostkey-update-02
  Host key update mechanism for SSH
- draft-miller-ssh-cert-05
  SSH Certificate Format
- draft-gutmann-ssh-preauth-04
  A Pre-Authentication Mechanism for SSH
- draft-spaghetti-sshm-filexfer-00
  SSH File Transfer Protocol

Related Internet-Drafts (2/3)

- draft-josefsson-ssh-mceliece-02
  Secure Shell Key Exchange Method Using Chempat Hybrid of Classic McEliece and X25519 with SHA-512: mceliece6688128x25519-sha512
- draft-josefsson-ssh-sphincs-01
  Stateless Hash-Based Signatures for Secure Shell (SSH)
- draft-josefsson-ssh-ed25519mldsa65-01
  Hybrid Ed25519 with ML-DSA-65 for Secure Shell (SSH)

Related Internet-Drafts (3/3)

- draft-becker-cnsa2-ssh-profile-02
  Commercial National Security Algorithm (CNSA) Suite Profile for SSH
- draft-sfluhrer-ssh-mldsa-04
  SSH Support of ML-DSA
- draft-rpe-ssh-mldsa-02
  ML-DSA Public Key Algorithms for the Secure Shell (SSH) Protocol
- draft-sun-ssh-composite-sigs-01
  Composite ML-DSA Signatures for SSH
- draft-harrison-sshm-mlkem-00
  Module-Lattice Key Exchange in SSH