SSHM Working Group

IETF 121, Dublin, Ireland

Note well

- 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.

https://www.ietf.org/about/note-well/

About SSHM

Secure Shell Maintenance (SSHM) working group set up to:

- update the RFCs documenting SSH to reflect what is implemented and deployed in practice. In particular, the working group will document the OpenSSH certificate structure, the SSH agent protocol, and SFTP, as they are currently implemented.
- update and maintain the list of cryptographic algorithms used by SSH.

Chairs: Job Snijders & Stephen Farrell

Area Director: Deb Cooley

Mailing list: ssh@ietf.org

Archive: https://mailarchive.ietf.org/arch/browse/ssh/

WG document updates

Adopted:

- draft-miller-ssh-agent
- draft-josefsson-ntruprime-ssh

Waiting for authors to submit new -00 versions with appropriate filename.

Next up for adoption?

- draft-miller-secsh-compression-delayed ?
- draft-ietf-secsh-filexfer-02 (this specific version?)
- PROTOCOL.certkeys (needs to be converted to internet-draft)
- draft-kampanakis-curdle-ssh-pq-ke ?

Anything else?

- Strict KEX?

Today’s agenda

- Chairs - Working Group Modus Operandi
- Damien Miller - SSH Agent Protocol
- Theo de Raadt - Deprecating ciphers
- Any Other Business?

Speaker attendance unconfirmed?

- ntruprime
- PQ-KE

And then we'll be done for today!

Working Group Modus Operandi

- IETF datatracker system is used to upload, publish, track states of internet-drafts, collect directorate reviews, etc: https://datatracker.ietf.org/
  - Authors are encouraged to create an IETF datatracker account
- Authors can choose their own tooling for editorial work
  - GitHub, Gitlab, private repositories, no repositories - all good
  - XML2RFC, Markdown, TXT - all good
  - Some authors like to use web-accessible issue trackers, some don’t
- Working group participants can send feedback on internet-drafts to ssh@ietf.org, or to the I-D authors directly, or via VCS (if applicable).
  - Feedback can be just natural language, unified diff, pull-requests - all good

Working Group Modus Operandi

From the charter: “This working group will strive for strong security, simplicity, and ease of implementation. In particular, proposals will only be adopted if there is evidence of significant existing deployment or broad interest in new implementation and deployment. Protocol documents should not be submitted to the IESG for publication before they have at least two demonstrably interoperable implementations.”

Reports on interoperability are incredibly valuable!

- “Implementation Status Section” https://www.rfc-editor.org/rfc/rfc7942.html
- https://ssh-comparison.quendi.de/comparison/cipher.html (third party)
- https://wiki.ietf.org/en/group/SSHM (free form submission)

Working Group Modus Operandi - discussion

Questions?

Requests from the room?

Suggestions?

Comments?

You can always email sshm-chairs@ietf.org if you have questions how to proceed or approach something!