CURDLE WG

IETF98

draft-ietf-curdle-pkix (1/2)

Abstract: OIDs and ASN.1 encoding format for signatures and keys using Curve25519 and Curve448.

Number of reviews: Multiple

Discussions:

1. OID arc assignment:
    - By IANA
2. Prehash versus non prehahs signature variant
    - Prehash variant is motivated for CRL, however CRL can be partitioned
    - Consensus is that only non-prehash variant is considered
3. Algorithm Identifier for prehash variant
    - Should we remove them ?

draft-ietf-curdle-pkix-03

Next Steps:

- New OID values
- Updated version

draft-ietf-curdle-cms-eddsa-signatures - R. Housley

Abstract: Align with draft-ietf-curdle-pkix once the decisions are made

Authors: R. Housley

Number of Reviews: 1 so far

Discussions: None needed

Next Steps: Ready for WG Last Call in the next few days

Draft-ietf-curdle-cms-ecdh-new-curves - R. Housley

Abstract: OID to be assigned in the S/MIME arc

Authors: R. Housley

Number of Reviews: 3 so far

Discussions: None needed

Next Steps: Ready for WG Last Call

Draft-ietf-curdle-rsa-sha2 - chair

Abstract: Specifies use of SHA-2 256 and SHA-2 512 signatures with existing RSA keys in SSH.

Authors: denis bider

Number of Reviews: 2 WG participants in CURDLE. Draft is a result of several iterations, based on feedback from multiple SSH implementers before CURDLE.

Discussions: The draft has incorporated feedback, and is implemented as specified in OpenSSH, Bitvise SSH Server/Client, and others.

Next Steps: Request exists to clarify Public Key Algorithm vs. Signature Algorithm.

Draft-ietf-curdle-ssh-ext-info - chair

Abstract: General extension mechanism for SSH, with a specific extension for servers to advertise support for RSA with SHA-2 signatures in user authentication.

Authors: denis bider

Number of Reviews: 2 WG participants in CURDLE. Draft is a result of several iterations, based on feedback from multiple SSH implementers before CURDLE.

Discussions: The EXT_INFO mechanism has incorporated feedback, and is implemented as specified in OpenSSH, Bitvise SSH Server/Client, and others.

Next Steps: Pending minor usage clarifications. Requests to re-add extensions (no-flow-control, elevation) ?

Draft-ietf-curdle-ssh-kex-sha2 - chairs

Abstract: Update the standards to deprecate weak Kex Algorithms. Augment the list with new MODP groups and Curves.

Authors: Mark Baushke

Number of Reviews: Multiple

Discussions: Depends on a few other IETF drafts to be approved. Including draft-ssorce-gss-keyex-sha2-00 which is not yet under Curdle.

Next Steps: Determine the best way for drafts like this one to update recommended the Kex Algorithms in the IANA tables then Last-Call.

Draft-ietf-curdle-ssh-curves - chairs

Abstract: Publish curve25519-sha256@libssh.org as “curve25519” also add similar “curve448” as key exchange algorithms.

Authors: Aris Adamantiadis and Simon Josefsson

Number of Reviews: Multiple

Discussions: Multiple implementations exist.

Next Steps: Republish expired draft. Last Call.

Draft-ietf-curdle-modp-dh-sha2 - chairs

Abstract: Add named DH group{14,15,16,17,18} with SHA2-256 and SHA2-512 hashes

Authors: Mark Baushke

Number of Reviews: 1 for this draft

Discussions:Multiple SSH client/server have interoperable patches implementing these new DH groups.

Next Steps: Delete errant extra paragraph. Last Call?

Thanks!