Use of the Hash-based Digital Signatures in the Cryptographic Message Syntax (CMS)

draft-ietf-lamps-cms-hash-sig-02

Russ Housley
LAMPS WG at IETF 103
November 2018
Hash-based Digital Signatures

• CFRG has been working on specifications for hash-based digital signatures since 2013
• draft-mcgrew-hash-sigs-13 has completed RG Last Call
  – Describes the Leighton and Micali adaptation (1995) of the original work done by Lamport, Diffie, Winternitz, and Merkle
  – Small private and public keys
  – Fast signature generation
  – Fast signature verification using a small amount of code
  – LARGE signatures
  – Moderately slow key generation
• Hash-based signatures remain secure even if the attacker has a large-scale quantum computer
Conventions for using hash-based digital signatures with CMS

RFC 4108 uses CMS to protect firmware packages

Small verification code size is attractive in IoT environment

Deploy a quantum resistant signature now

Allows deployment of the next generation of cryptographic algorithms, even if current signature algorithms are broken or a large-scale quantum computer is invented in next decade or so
Status / The Ask

• LAMPS WG adopted the Internet-Draft
• Corrected small errors to align with draft-mcgrew-hash-sigs-13
  – Thanks Daniel for the very careful review

• Ready for WG Last Call as soon as draft-mcgrew-hash-sigs is in the RFC Editor queue
• Please review and comment on the mail list

• Tim will make all LAMPS WG consensus calls related to this document