Use of the Hash-based Digital Signatures
in the Cryptographic Message Syntax (CMS)
draft-housley-cms-mts-hash-sig-10

Russ Housley
LAMPS WG at IETF 102
July 2018
Hash-based Digital Signatures

• CFRG has been working on specifications for hash-based digital signatures since 2013
• draft-mcgrew-hash-sigs-11 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
Developed in parallel to draft-mcgrew-hash-sigs
Conventions for using these hash-based digital signatures with the 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
The Ask

- LAMPS WG adopt the Internet-Draft: draft-housley-cms-mts-hash-sig-10
- Review and comment on the Internet-Draft
- Tim will make all LAMPS WG consensus calls related to this document