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

draft-ietf-lamps-cms-hash-sig-07

Russ Housley
LAMPS WG at IETF 104
March 2019
CFRG has been working on specifications for hash-based digital signatures since 2013

draft-mcgrew-hash-sigs is now published: RFC 8554

Describes the Leighton and Micali adaptation (1995) of the original work done by Lamport, Diffie, Winternitz, and Merkle

- The number of signing operations depends upon size of tree
- Small public keys, and low computational cost
- Fast signature verification using a small amount of code
- SMALL private key if signer does additional computation at signing time
- BIGGER private key for faster signing time
- LARGE signatures
- Moderately slow key generation

HSS/LMS remains secure even if the attacker has a large-scale quantum computer
draft-ietf-lamps-cms-mts-hash-sig

• 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

• Corrected small errors to align with most recent version of draft-mcgrew-hash-sigs
  – Thanks Daniel for the very careful review

• If no signed attributes, HSS/LMS signs content
• If signed attributes, HSS/LMS signs hash of attributes
  – Thanks Jim for pushing approach that only uses same hash function as the HSS/LMS tree

• Completed LAMPS WG Last Call
• Waiting for Security AD review and then IETF Last Call