Use of the Hash-based Digital Signatures in COSE

draft-ietf-cose-hash-sig-01

Russ Housley

COSE WG at IETF 104

March 2019

HSS/LMS Digital Signatures

- 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 signing time computation
  - 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-cose-hash-sig

- Conventions for using hash-based digital signatures:
  - The 'kty' field MUST be present, and it MUST be 'HSS-LMS'
  - If the 'alg' field is present, and it MUST be 'HSS-LMS'
  - If the 'key_ops' field is present, it MUST include 'sign' when creating a HSS/LMS signature
  - If the 'key_ops' field is present, it MUST include 'verify’ when verifying a HSS/LMS signature
  - If the 'kid' field is present, it MAY be used to identify the top of the HSS tree. In RFC 8554, this identifier is called 'I', and it is the 16-byte identifier of the LMS public key for the tree

HSS/LMS Signatures for Software Update

- 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 SUIT WG is using COSE
- The SUIT WG is considering making HSS/LMS the mandatory to implement signature algorithm

Status and Way Forward

- Corrected small errors in -01 to align with most recent version of draft-mcgrew-hash-sigs (now RFC 8554), and addressed comments from Jim Schaad
- Jim Schaad did an implementation; next version will include examples from that code
- Once examples are added, ready for COSE WG Last Call