Recap:

- Hash-based signatures in X.509
  - LMS/HSS (RFC8554)
  - XMSS/XMSS\(^{MT}\) (RFC8391)
  - SPHINCS+ aka SLH-DSA (Draft FIPS 205)

- Use-cases:
  - Popular key format e.g. for code signing
  - Root-CA for trust centers

- Demand by agencies and industry
- Provide identifiers
- Alignment with other specifications
Available here:

Network Working Group
Internet-Draft
Intended status: Informational
Expires: 25 August 2024

Internet X.509 Public Key Infrastructure: Algorithm Identifiers for HSS and XMSS
draft-gazdag-x509-shbs-00

Abstract

This document specifies algorithm identifiers and ASN.1 encoding formats for the Stateful Hash-Based Signature Schemes (S-HBS), Hierarchical Signature System (HSS), extended Merkle Signature Scheme (XMSS), and XMSS\textsuperscript{MT}, a multi-tree variant of XMSS. This specification applies to the Internet X.509 Public Key Infrastructure (PKI) when those digital signatures are used in Internet X.509 certificates and certificate revocation lists.

https://datatracker.ietf.org/doc/draft-gazdag-x509-shbs/
https://datatracker.ietf.org/doc/draft-gazdag-x509-slhdss/
https://github.com/x509-hbs
Major change

Draft split into two as discussed at IETF 118

- draft-gazdag-x509-shbs
  Stateful schemes: LMS and XMSS
- draft-gazdag-x509-slhdsa
  Stateless scheme: SPHINCS+ aka SLH-DSA
Further changes

- Bugfix
- Proof-reading / sanity-check
- Tracked alignment to other documents

- Only minor issues left
Call for adoption started 8\textsuperscript{th} of March

We kindly ask for your support!
Questions?

Stefan-Lukas_Gazdag@genua.de

https://datatracker.ietf.org/doc/draft-gazdag-x509-shbs/

https://datatracker.ietf.org/doc/draft-gazdag-x509-slhdsa/

https://github.com/x509-hbs