draft-gazdag-x509-hash-sigs

Stefan-Lukas_Gazdag@genua.de

6th November 2023

genua.

Available here:

Workgroup:
LAMPS - Limited Additional Mechanisms for PKIX and SMIME
Internet-Draft: draft-gazdag-x509-hash-sigs-02
Published: 14 September 2023
Intended Status: Informational
Expires: 17 March 2024

K. Bashiri
BSI
S. Fluhrer
Cisco Systems
S. Gazdag
genua GmbH
D. Van Geest
S. Kousidis
BSI

Internet X.509 Public Key Infrastructure: Algorithm Identifiers for Hash-based Signatures

Abstract

This document specifies algorithm identifiers and ASN.1 encoding formats for the Hash-Based Signature (HBS) schemes Hierarchical Signature System (HSS), eXtended Merkle Signature Scheme (XMSS), and XMSS^MT, a multi-tree variant of XMSS, as well as SLH-DSA (formerly SPHINCS+), the latter being the only stateless scheme. 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-hash-sigs/

https://github.com/x509-hbs/draft-gazdag-x509-hash-sigs

genua.

Rationale

- 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

genua.

Changes for -02

Thanks for your comments via the mailing list!

- Clarified use-cases (e.g. no stateful HBS below Root cert)
- Extended security considerations
- Rationale to Backup and Restore Management
- Aligned encoding to other documents

genua.

Open issues

- Splitting document? Options:
  - Cumulative as is
  - Draft/RFC for each scheme
  - Two drafts/RFCs for stateful and stateless

genua.

We kindly ask for adoption

- We think it fit for practical use
- Except minor issues it’s ready to go
- Please let us know about any concerns

genua.

Questions?

Stefan-Lukas_Gazdag@genua.de

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

https://github.com/x509-hbs/draft-gazdag-x509-hash-sigs