Hash-based Signatures: State and Backup Management

draft-wiggers-hbs-state-01

Thom Wiggers, 2025-03-17, IETF 122, Bangkok

Guidance for state management
(repeat from IETF120)

- Dealing with state is hard
- Dealing with state is scary
  - “*Thou MUST NOT use a key more than once*” — but how?
  - You SHOULD use ~~SPHINCS+~~ SLH-DSA if possible
- You SHOULD probably use an HSM
- How do you reliably deploy S-HBS schemes?
- And what about backups?

“I’ll just divide signatures into epochs! That’ll be easy!

Fun content such as

5.8. Time-based State Management

[…]
Any time-based approach has a very strict reliance on accurate time-keeping and synchronization of clocks. In particular, we identify that at least the following engineering-related challenges need to be considered:

[16 BCP14 keywords follow]

CHANGELOG

Versus -00

- Added text about when stateful HBS are appropriate
- Minor editorial changes

NIST SP800-208 review meeting

Online, 2025-02-12

- NIST is responding to industry noises that current SP800-208 too restrictive
- Recently organized meeting to discuss allowing key export and provisioning of sHBS key blocks
- Lots of discussion about how to protect users technically but also procedurally

NIST’s changes will put more responsibility on those running stateful HBS, let’s give them some pointers.

Adopt?