

Hash-based Signatures: State and Backup Management

<https://datatracker.ietf.org/doc/draft-ietf-pquip-hbs-state/>

Status update



Changes made since IETF 124

- Comment from last meeting:
 - [Added comparison to MCGREW paper and ETSI TR 103 692 to introduction](#)
- Responded to comments by Scott Fluhrer
 - [Sharpened scope of sectorization](#)
 - [Additionally cite Scott's paper that explains a flaw in the BH16 analysis](#)
 - [Clarify that private key and state can be separated](#)
 - [Note implementation size separately in "when appropriate" but don't elaborate further](#)
- Responded to comments by Alicja Kario
 - [Added partial state transfer and ACID requirement](#)



New text

- Write about Interval-based state reservation
 - Reserve and commit an interval of, e.g., 100 keys, if you lose state just assume all were used
- Add warnings when reaching threshold
- Some text on parameter selection (suggested by Scott)



Scoping decisions

- Scott suggested that we could add (a lot of) text on parameter selection
 - Huge subject, XMSS/LMS are extremely tweakable
 - Authors settled on pointing out that there exist these trade-offs and name them, but not elaborating further.
- Scott suggested adding text on implementation tricks (and kindly volunteered)
 - We are leaning towards **not** adding this text, because it goes way beyond the scope of this document and its audience. <https://github.com/hbs-guidance/draft-hbs-state/issues/28>



NIST's changes to SP 800-208

- It is still looking like NIST has reduced bandwidth
- We have reached out via email and at the NIST PQC workshop, but have not gotten any response (yet?)
 - Circumstances have been difficult for NIST in the past weeks
- I don't believe any of our stuff is "in the way" of anything that they would do



WGLC soon?