Stateful HBS: how to handle

~~draft-wiggers-hbs-state~~
draft-ietf-pquip-hbs-state

Agenda

1. Status update
2. How to proceed
3. Overview open discussion items

I would rather run out of time than reach the end of my slides!

Changes since last IETF

- Adopted by WG 🎉
- Fixed a typo
- Converted some list discussion points to Github issues

Gemini: “the most glitzy imaginable "news" flashing text”

Path to WGLC

1. Write content
2. Identify/discuss any remaining gaps
3. ???
4. WGLC

Reversing the order

1. When are we declaring this work “complete enough” to proceed to WGLC
2. Identify gaps until we are at the above points
3. How are we going to fill identified gaps
4. Any comments on the existing guidance in the document—anything from meta to nitpicking comments could honestly be helpful.

When are we done?

IMHO, we have:

- A decent amount of exposition of “yes, it is hard” and “this is how things can break in a way you don’t have experience with yet from classic crypto”
- A decent amount of discussion of some solutions and approaches, including caveats
- We will never be able to be exhaustive

When are we going to call it?

Gaps?

Gap: NIST’s work in progress

- NIST is working on changes to SP800-208, but no news since meeting at beginning of the year
- May obsolete some of the contents, but changes could also result in additional need for guidance (changes will likely remove technical blockers for backups but trade for introducing procedural difficulties)

- NIST is also investigating *state-light* variants of SPHINCS$^+$ with limited numbers of allowed signatures.

Adressing the gaps

```
def process_gaps(list_of_gaps):
    for gap in list_of_gaps:
        match gap.kind():
            case "bugfix" | "author_review":
                yield "PRs welcome, but we'll try to follow up"
            case "new_use_case":
                yield "Come talk to us"
            case "contributor":
                yield "We don't bite"
            case "your fun pseudocode doesn't make sense" :
                yield "don't @ me"
            case _:    # default
                yield "Discuss on list?"
```

Open floor

- Any comments / praise / criticisms / gaps / points not brought up yet?

Open Github issues

https://github.com/hbs-guidance/draft-hbs-state

- #10: NIST’s stuff
- #11 Comments from Alicja Kario
- #14 Devices with degrading storage
- #16 Interval-based approaches
- #18 "Soft-fail" / Warnings when at a certain amount of signatures left