Public Comments on SP 800-106, Randomized Hashing for Digital Signatures

Comment period: January 13, 2022 – March 16, 2022

On January 13, 2022, NIST's Crypto Publication Review Board initiated a review of SP 800-106, *Randomized Hashing for Digital Signatures* (February 2009). This document includes the public comments received during the comment period from January 13, 2022, to March 16, 2022. While this comment period was directed toward SP 800-106, the feedback provided will be considered for the appropriate documents.

More details about this review are available from NIST's Crypto Publication Review Project site.

LIST OF COMMENTS

1. Comments from Roger Johnson, January 13, 2022

800-106 addresses using hashing in digital signatures. 800-132 addresses using hashing in password-based key derivation. There might be other application-specific guidance on hashing.

Perhaps there could be one SP on the use/application of hashing?

Part 1: Concepts: To address the concepts for hashing use (which currently seem to be repeated across SPs for different applications)—specifically of all of the parameters and choices which the crypto user must address, such as:

1. Initialization vector/ salt – its purpose, and the inclusion of some/all randomness in the IV for certain purposes.
2. Iteration count – ditto
3. Length of resultant hash – any security implications from various choices
4. …

Part 2: Applications: Additional chapters or appendices addressing specific applications and specific considerations/recommendations for each application of hashing, such as (probably need to address many/all of the PBKDF2 parameters and alternatives in each application, not just for passwords):

- Digital signatures:
  - IV: specific randomness, length, etc. recommendations/requirements
  - Pseudorandom function: if randomness required, recommended/required functions and parameters
  - Iteration count: The "digital signature" application of hashing has traditionally been "one" hash iteration (would higher iteration counts address any of the existing or anticipated problems with intentionally finding collisions to undermine a signature?)
  - Hashing Algorithms and Key Sizes: which hashing algorithms and key sizes are allowed/recommended
  - Length of resultant hash: recommendations for specific value or minimums/maximums (for security, practical interoperability, …)
- Passwords:
  - …

Part 1 might be fairly static, while Part 2 might change fairly rapidly over time. Something like 800-131A could be a good common place to put all dynamic "parameters" for all hashing ("Part

2") and other crypto (including algorithms and key lengths to be used in particular applications) in one place that can be easily referenced and frequently updated, while the underlying math and science in Part 1 remains static in other SPs without the dynamic Part 2 application information.

I suspect that "requirements and recommendations* for use/application of crypto" (e.g. current 800-131A and the hashing "Part 2" information) probably needs to be on a frequent review/update schedule (every one or two years), if not more frequent and/or event driven (with an update approach similar to what NIST is adopting for SP 800-53 to allow frequent/rapid updates to individual controls without updating/reviewing/approving republication of the entire SP).

The Part 2 approach might help address the implementation of your technical question – is 800-106 still needed? If was required in the past, might or might not be needed now with current algorithms, but perhaps might be needed again in the future (perhaps due to quantum computing, other advances, or aging of current algorithms). The theory/concepts in Part 1 should hold up over time, and the temporal requirements/ recommendations of different algorithms for different applications to address current threats / computing capabilities can then change more easily as needed over time.

*Requirements: minimum/maximum allowed. Recommendations: what is reasonably/ adequately secure for a particular use (best practice), not what is minimally allowed (e.g. for backward compatibility)

2. Comments from Canadian Centre for Cyber Security (CCCS), January 22, 2022

The randomized hashing specified in SP 800-106 was introduced as a way to improve the security of a signing protocol without a change in the underlying functions or algorithms. The introduction of this mode of operation was particularly important after early attacks on SHA-1 reduced its collision strength to below NIST requirements. Since then, the introduction of SHA-3 provided another alternative to SHA-2. Furthermore, other digital signatures, such as ECDSA, and specifically the newer EdDSA, already have randomization built into their design.

The Internet-Draft corresponding to SP 800-106 (https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-rhash-01) has not been formally adopted and has expired; we are not aware of any wide use of this technique that would warrant discussion.