RSA Blind Signatures

draft-irtf-cfrg-blind-signatures
Security Analysis of RSA-BSSA

- Security proof for the proposed scheme by Anna Lysyanskaya

- New definition of blindness to encompass privacy risks caused by adversarial signing key generation

- Raised concerns that FDH and deterministic variants do not satisfy blindness when the public key \((N,e)\) is chosen maliciously

- Not a concern for single-use high-entropy tokens but risks if such a construction were used for general purpose blind signatures
Proposed Resolution

• No downscoping of the draft
  • Continue standardizing blind signatures and not only a blind token scheme.

• Remove the deterministic variant from the draft
  • Given the concerns about such a construction with a maliciously generated signing key, we recommend to remove that variant of the draft

• Include a new message nonce
  • That nonce can be be omitted when signing high-entropy inputs only
WG Questions

• Does anyone have applications where deterministic signing is a requirement?
  • Adds a lot of complexity to support it, so without any concrete use case, we don’t think it’s worth furthering standardization efforts with that approach

• Opened pull request with the proposed changes
  • Please review and comment if you have feedback or concerns