

[REDACTED]

From: dig-comments@list.nist.gov on behalf of Wayne Pollock
Sent: [REDACTED]
To: dig-comments@nist.gov
Subject: [dig-comments] Comments on proposed sb800-63-4 (sp800-63b)

Regarding <<https://pages.nist.gov/800-63-4/sp800-63b.html#passwordver>>:

"If Unicode characters are accepted in passwords, the verifier SHOULD apply the normalization process for stabilized strings using either the NFKC or NFKD normalization defined in Sec. 12.1 of Unicode Normalization Forms [UAX15]."

Please note this contradicts RFC-8265, section 4.2.2
(<<https://www.rfc-editor.org/rfc/rfc8265#section-4.2.2>>):

"4. Normalization Rule: Unicode Normalization Form C (NFC) MUST be applied to all strings."

I think NIST should consider this issue and update sp800-63b, at least with a note explaining your choice if you don't change to match RFC-8265. (If your experts believe the RFC is wrong, please submit an errata to it.)

Additional reference: <<https://datatracker.ietf.org/doc/html/rfc7564>>

--
Wayne Pollock, Brandon Florida USA

--
To unsubscribe from this group, send email to dig-comments+unsubscribe@list.nist.gov

View this message at <https://list.nist.gov/dig-comments>
To unsubscribe from this group and stop receiving emails from it, send an email to DIG-Comments+unsubscribe@list.nist.gov.