



draft-irtf-cfrg-cspace

STATUS IETF | 17, JULY 2023

MICHEL ABDALLA, BJÖRN HAASE, JULIA HESSE



draft-irtf-cfrg-cspace

STATUS - I

Current version -08 is essentially unchanged since version -06.

Objectives of the last major rewrite for -06 were:

- Improve readability by focusing on implementers- and protocol-designer perspectives
- Cover the case of existing frameworks such as TLS coming with clear initiator and responder roles and with specified message encoding formats
- Provide an encoding format also for stand-alone constructions
- Explicitly cover both, use-cases where message-sequence ordering is enforced and not enforced (clear or no clear initiator and responder roles)
- Add comprehensive test vectors

draft-irtf-cfrg-cspace

STATUS - 2

- Some feedback has been obtained from implementers that contacted the editors, mostly not on the list.
 - Most actual implementer feedback came in the context of the Ristretto/Decaf cipher suites which indicates that there is interest in the Ristretto/Decaf suites.
 - Some feedback advocated for removing Ristretto/Decaf cipher suites from the draft for the sake of reduced complexity.
- The editors understand both perspectives. We would like to appreciate feedback on whether or not the Ristretto/Decaf cipher-suites should be kept in the draft and whether or not Ristretto/Decaf suites should be included in the list of **recommended** cipher suites.
- Current compromise: Test vectors for Ristretto/Decaf suites are included but the corresponding suites are not added to the list of **recommended** cipher suites.

draft-irtf-cfrg-cpace

NEXT STEPS

- Editorial review by a native speaker would be welcome.
- Official review by the crypto review panel board should be started.
- Upon request of some implementers, we plan to also produce JSON-encoded test vectors within the reference implementation code.
(<https://github.com/cfrg/draft-irtf-cfrg-cpace/>)