draft-irtf-cfrg-cpace-13

Michel Abdalla, Björn Haase, Julia Hesse

Status IETF 121, November 2024

- Integrated first round of 3 Reviews by Crypto Review Panel
- Considered all the feedback given on the list and off the list
- Updated security consideration with new insights from [BGHJ24]
- Integrated JSON version of test vectors

=> Draft now considered to be on a “release candidate” level

ID-Changes since last presentation

- Fully included feedback from Crypto Review Panel reviews.
- Reference to the “network representation” was removed. This simplified the draft considerably. (Main point in the feedback of Thomas Pornin)
- We added a guidance section with recommendations on how to best integrate CPace in higher-level protocols such as TLS.
- We added the new result of BGHJ24 that showed how a unique session id can be calculated alongside with CPace if no session id was available before starting CPace.
- We now have both, human-readable and embedded JSON test vectors.
- We added a link to the reference implementation used for generating the test vectors.

Incorporated crypto review panel feedback

We received very detailed and helpful feedback from Thomas Pornin, Khartik Bhargavan and Björn Tackmann.

Again a big “Thank you” to all of you, Thomas, Khartik and Björn!

We have considered all your comments. For the individual aspects and our respective responses see also:

https://github.com/cfrg/draft-irtf-cfrg-cpace/blob/master/TODO_review

Status update: Security analysis

New paper available online:

[BGHJ24] https://eprint.iacr.org/2024/234 M. Barbosa, K. Gellert, J. Hesse, S. Jarecki "Bare PAKE: Universally Composable Key Exchange from just Passwords"

Results in a nutshell

- CPace also ***UC*** secure without pre-established session id (sid)
- New UC analysis independently confirms the results regarding sid from Game-Based analysis in appendix B in https://eprint.iacr.org/2021/114
- We now have two independent studies confirming that CPace as specified in the draft is secure also without a preceeding message flow for pre-establishing a sid (now UC model *and* real-or-random game-based model covered)

- Resolves the main aspect brought up by Karthik

Recap: Work since the PAKE selection process

- Focused on the target reader group: protocol implementers, testers and integrators.

  Technical aspects of protocol proofs outsourced to [AHH21] with a direct correspondence of security paper to the recommended cipher suites in the ID

- Integrated insights from new security analysis in [BGHJ24] and [ES21]
- Collected feedback from implementers and during CFRG sessions regarding which cipher suites to recommend and for which to provide test vectors (3 suite families)
- Review by the crypto review panel members was initiated and review results were integrated in the draft.
- We link to a reference implementation used for generating test vectors.
- Collected and integrated feedback from CFRG list and from the Github repository

Summary

We consider draft-irtf-cfrg-cpace-13 now to be on a “release candidate” level and ready for a final approval round.