# Results of the PAKE selection process

CFRG Chairs

CFRG
April 2020

# PAKE selection process: history

## IETF 103

- After receiving several PAKE proposals and seeing documents complete, the chairs want to announce PAKE selection process
- The aim is to select one or more ("zero or more") PAKEs to recommend to the wider IETF community
- Submissions to satisfy RFC 8125, Requirements for PAKE Schemes
- Both balanced (both sides store the same representation of password) and augmented (one side maintains a transform of the password and the other maintains the raw password) PAKEs are considered.
- Better to select one without a variety of options
- Involving Crypto Review Panel to come up with recommendations
- Support of the process at the CFRG session ("and please do it soon") and later at the TLS and IPSECME sessions

# Nominated PAKEs

- Balanced:
  - SPAKE2 (nominated by Watson Ladd and Ben Kaduk)
  - J-PAKE (nominated by Feng Hao)
  - SPEKE (nominated by Dan Harkins)
  - CPace (nominated by Björn Haase)
- Augmented:
  - OPAQUE (nominated by Hugo Krawczyk)
  - AuCPace (nominated by Björn Haase)
  - VTBPEKE (nominated by Guilin Wang)
  - BSPAKE (nominated by Steve Thomas)

# Results of Round 1

- The opinions of the reviewers were not unanimous; some new questions were raised during the final stages of Round 1, we moved to Round 2.
- 4 candidates were left for Round 2:
  - SPAKE2 (balanced) — nominated by Watson Ladd and Ben Kaduk
  - CPace (balanced) — nominated by Bjoern Haase
  - OPAQUE (augmented) — nominated by Hugo Krawczyk
  - AuCPace (augmented) — nominated by Björn Haase

## Balanced/augmented

- There was a reasonable amount of desire in reviews to have both a balanced PAKE and an augmented PAKE.
- So the intention of Round 2 was to select one (or zero) balanced PAKE and one (or zero) augmented PAKE, allocating two categories.

# Plan and timeline of Round 2 (1)

**Round 2, Stage 1, 21.11.2019-05.12.2019**

Additional questions for all four candidates were collected from CFRG participants (and Crypto Review Panel Members).

**Round 2, Stage 2, 10.12.2019-17.12.2019**

A list of new questions was published. The CFRG was asked if anything else should be added.

**Round 2, Stage 3, 25.12.2019-10.02.2020**

The authors of the candidates prepared their replies to the additional questions/requested clarifications.

**Round 2, Stage 4, 12.02.2020-10.03.2020**

Crypto Review Panel members prepared new overall reviews taking into account all information collected.

# Plan and timeline of Round 2 (2)

**Round 2, Stage 5, 12.03.2020-21.03.2020**

CFRG chairs to discuss the reviews and make recommendations.

**CFRG meeting**

- The chairs give a review of the progress.
- If everything is clear:
  - one (or zero) balanced PAKE is selected;
  - one (or zero) augmented PAKE is selected;
  - initiate a CFRG document „Recommendations for password-based authenticated key establishment in IETF protocols“, reflecting the results and practically important recommendations.

# Results of Stages 1, 2

**Stages 1, 2: 21.11.2019-17.12.2019**

Additional questions for all four candidates were collected from CFRG participants (and Crypto Review Panel members). The questions could be of one of possible types:

- Requests for clarifications for the candidate protocols or their proposed modifications.
- Questions to be taken into account in addition to ones collected at Stage 1 of Round 1.

## Stages 1, 2: Additional questions

The following additional questions for the authors were collected:

1. Can you propose a modification of SPAKE2 with a correspondingly updated security proof, addressing the issue of a single discrete log relationship necessary for the security of all sessions?
2. Can you propose a modification of CPace and AuCPace with a correspondingly updated security proof, addressing the issue of requiring the establishment of a session identifier (sid) during each call of the protocol for the cost of one additional message?
3. Can the nominators/developers of the protocols please re-evaluate possible IPR conflicts between their candidates protocols and own and foreign patents? Specifically, can you discuss the impact of U.S. Patent 7,047,408 on free use of SPAKE2 and the impact of EP1847062B1 on the free use of the RFC-drafts for OPAQUE?
4. Quantum annoyance of the PAKE?
5. Post-quantum preparedness of the PAKE?

# Results of Stage 3

**Stage 3: 25.12.2019-10.02.2020**

The authors of the candidates prepared their replies to the additional questions/requested clarifications.

At the end of Stage 3 we had all replies from the authors (see https://github.com/cfrg/pake-selection).

# Results of Stage 4

**Stage 4, 12.02.2020-10.03.2020**

Crypto Review Panel members prepared new overall reviews (for 4 remaining PAKEs) taking into account both the reviews obtained on Round 1 and new information obtained during Round 2.

As a result of Round 2 we obtained four strong reviews:

- Bjoern Tackmann
- Russ Housley
- Julia Hesse
- Scott Fluhrer

All of them are available at https://github.com/cfrg/pake-selection.

## TL;DR's of the Crypto Review Panel reviews

1. Bjoern Tackmann:
   "I prefer CPace over SPAKE2. SPAKE2 seems an (almost) equally good alternative, and picking one of the two was difficult.
   I prefer OPAQUE over AUCPACE. The main arguments are OPAQUE's better compatibility with important application protocols through less protocol messages, and its flexibility."
2. Russ Housley:
   "RECOMMENDATION: CPace;
   RECOMMENDATION: OPAQUE."
3. Julia Hesse:
   "Security-wise I (conditionally) recommend SPAKE2 and OPAQUE."
4. Scott Fluhrer:
   "Balanced PAKE: CPace;
   Augmented PAKE: OPAQUE."

# The results

The PAKE selection process is finished.

We recommend the following two protocols to be selected as "recommended by the CFRG for usage in IETF protocols":

- one balanced PAKE: CPace;
- one augmented PAKE: OPAQUE.

# Acknowledgements


## The authors

Many thanks to all authors of the nominations:
Watson Ladd, Benjamin Kaduk, Feng Hao, Dan Harkins, Björn Haase, Hugo Krawczyk, Guilin Wang, Steve Thomas

## The reviewers at the Stage 1

Many thanks to all independent reviewers:
Yoav Nir, Valery Smyslov, Thyla van der Merwe, JC Jones, Martin Thomson, Kevin Jacobs, Karthik Bhargavan, Jonathan Hoyland, David Gotrik, Steve Thomas, Kevin Lewi, Brian Warner, Bill Cox, Bjoern Tackmann, Scott Fluhrer, Tibor Jager

## The Crypto Review Panel experts

Special thanks to the Crypto Review Panel experts:
Bjoern Tackmann, Russ Housley, Yaron Sheffer, Stanislav Smyshlyaev, Julia Hesse, Scott Fluhrer

# What now?

## Further actions

Now we initiate a CFRG document „Recommendations for password-based authenticated key establishment in IETF protocols“.

- A detailed description of the PAKE(s).
- Recommendations for generation of parameters.
- Mandated auxiliary primitives.
- Test vectors.
- Guidelines for integrating into protocols:
  - on which step to negotiate PAKE parameters
  - how cross-cipher suite security should be taken into account
  - supported identity fields and recommendations on their protection
  - whether and how „optional“ protocol exchanges can be eliminated
  - required additional key confirmation steps
  - handling the counters of failed attempts of authentication
  - ...

## Questions to CFRG

1. Do we need one or two documents?
   - Option 1: „Recommendations for password-based authenticated key establishment in IETF protocols" with both CPace and OPAQUE.
   - Option 2: „Recommendations for balanced password-based authenticated key establishment in IETF protocols" with CPace and „Recommendations for augmented password-based authenticated key establishment in IETF protocols" with OPAQUE.

   CFRG chairs will have the final say in case of absence of strong arguments for one way or another.
2. Editors? Authors?

Thank you for your attention!

Questions?

- crypto-panel@irtf.org
- cfrg-chairs@ietf.org